Novell NetWare® 6.5

www.novell.com

NOVELL NATIVE FILE ACCESS PROTOCOLS INSTALLATION AND ADMINISTRATION GUIDE

Novell®

Legal Notices

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

www.novell.com

Novell Native File Access Protocols Installation and Administration Guide
April 2003

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.

Contents

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 11 describes the benefits of Novell Native File Access Protocols software.
- Chapter 2, "Installing Novell Native File Access Protocols on a NetWare 6.5 Server," on page 13 describes how to install the software on a NetWare server.
- Chapter 3, "Working with Macintosh Computers," on page 15 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 21 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 27 explains Novell Cluster Services™ and how to configure the Novell Native File Access software for Macintosh and Windows computers in a clustered environment.
- Chapter 6, "Working with UNIX Machines," on page 31 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

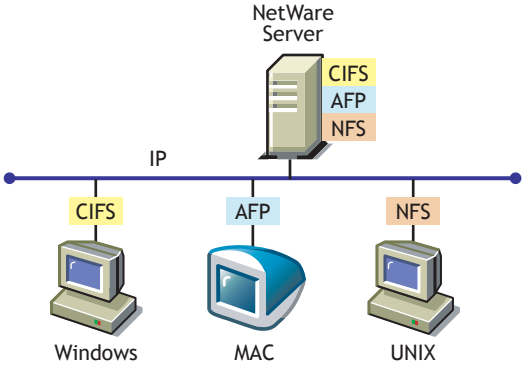
In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

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 or configuration is required.

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



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

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

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

Native File Access Protocols and the Universal Password

The simple password that was required for Native File Access Protocols in previous releases is no longer necessary. A new Universal Password is included in NetWare 6.5 that eliminates the need

for Simple Passwords and removes problems that previously existed with password synchronization. To learn more about Universal passwords, go to Universal PasswordNetWare 6.5 Security Overview guide.

What's Next

Novell Native File Access Protocols are installed by default with NetWare 6.5. To get started, continue with Chapter 2, "Installing Novell Native File Access Protocols on a NetWare 6.5 Server," on page 13.

2 Installing Novell Native File Access Protocols on a NetWare 6.5 Server

The Native File Access Protocols are currently installed and configured automatically when you install your NetWare 6.5 server.

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

1. Set up an Administrator Workstation.

   See "Administrator Workstation Prerequisites" on page 13.

2. 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 14.

3. "Starting and Stopping AFP and CIFS Protocols Service" on page 14

Administrator Workstation Prerequisites

Changing the default configuration settings and managing Novell Native File Access services must be done from a Windows-based Administrator Workstation. Make sure that the workstation meets the following system requirements.

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

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

- ❑ Client NICI 1.5.7 (or later) for Windows (Strong Encryption) installed

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

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

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

Client Computer Prerequisites

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

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

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

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

To set up and manage Macintosh users, see Chapter 3, "Working with Macintosh Computers," on page 15.

To set up and manage Windows users, see Chapter 4, "Working with Windows Computers," on page 21.

To set up and manage UNIX users, see Chapter 6, "Working with UNIX Machines," on page 31.

3 Working with Macintosh Computers

This chapter contains the following information:

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:

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

HINT: 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 eDirectory 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 a 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 eDirectory context of the Guest object to the context search file as described in "Editing the Context Search File" on page 15.
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 17).
- Logging In to the Network as Guest (page 17).
- Changing Passwords from a Macintosh Computer (page 17).
- Assigning Rights and Sharing Files from a Macintosh Computer (page 18).

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 16, 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.

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.

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

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.

HINT: 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) 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 eDirectory name).

HINT: 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 remove 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 21)
- Windows End User Tasks (page 24)

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:

- Specifying Contexts in the Context Search File (page 21)
- "Managing Network Access with ConsoleOne" on page 22
- Providing Network Access to Domain Users (page 22)
- Customizing the Network Environment for CIFS (page 22)
- Viewing Configuration Details (page 24)

Specifying Contexts in the Context Search File

An eDirectory search context is created automatically during the NetWare installation for Windows users who require access to the network. These contexts are saved in the context search file. When Windows users 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 eDirectory 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.

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 13.

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 eDirectory.

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

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

2 Run NetWare Remote Manager.

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

See NetWare Remote Manager Administration Guide in the NetWare 6.5 documentation.

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

4 Browse to the 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 ConsoleOne.

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 13.

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* means Unicode or international character support. Unicode characters are used in double-byte languages. Unicode is enabled by default for this NetWare 6.5 Beta release. It currently cannot be disabled. Checking or unchecking the check box has no effect.
- *OpLocks* (Opportunistic Locking) improves file access performance and is enabled by default for this NetWare 6.5 Beta release. It currently cannot be disabled. Checking or unchecking the check box has no effect.
- *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 intergchangeably.
- *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.

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 24)
- Mapping Drives from a Windows Computer (page 25)

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, XP 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.

HINT: 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.

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

NetWare® 6.5, 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 6.5 clustered environment so that Macintosh and Windows computers can use Novell Native File Access Protocols to access files on the network.

NOTE: For information on setting up UNIX computers to use Novell Native File Access Protocols in a clustered NetWare 6.5 environment, see Chapter 6, "Working with UNIX Machines," on page 31.

Prerequisites

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

- ❑ Novell Cluster Services 1.7 installed on NetWare 6.5 servers

  For information on configuring Novell Cluster Services, see the Novell Cluster Services Overview and Installation.

- ❑ NetWare 6.5 configured as described in "Installing Novell Native File Access Protocols on a NetWare 6.5 Server" on page 13

- ❑ Administrator workstation configured as described in "Administrator Workstation Prerequisites" on page 13

- ❑ Novell Native File Access Protocols installed on each server in the cluster that you want users to access.

  Follow the instructions in "Installing Novell Native File Access Protocols on a NetWare 6.5 Server" on page 13.

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 NetWare 6.5 installation.

2. Cluster enable the shared-disk pools or volumes by following the procedures described in Create Shared Disk Partitions.

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 16.

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 cluster by entering the IP address or virtual server name of the cluster-enabled volume.

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

Setting Up for Windows

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

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

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

1 Ensure the CIFSSTRT.NCF command is in the AUTOEXEC.NCF file of each server in the cluster that will run CIFS.

2 Create and cluster enable pools by following the instructions in the 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 29.

3 (Conditional) To make pools that have already been cluster enabled (virtual servers) accessible to CIFS clients, you must manually add an NFAP auxillary 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 /overridetype=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 Novell Native File Access Protocols on a NetWare 6.5 Server" on page 13 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 6.5 cluster configured with Novell Native File Access Protocols, Macintosh and Windows users can receive the benefits of a clustered environment—without needing additional client software.

For an explanation of how Macintosh users access network files and for more information on managing Macintosh workstations, see Chapter 3, "Working with Macintosh Computers," on page 15.

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 21.

6 Working with UNIX Machines

Native File Access for UNIX* provides an NFS* Server that lets UNIX users access and store files on NetWare® servers. It is an implementation of the Network File System (NFS) protocol. The required software components are installed and run only on the NetWare servers; no additional software is required on the UNIX workstations. UNIX users attach to NetWare storage using NFS over the TCP/IP protocol. They can mount the exported network storage and use it as their own file system.

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

What's New

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

  NFS Server has been tested with 300 clients simultaneously performing basic file operations using a script over NFS Version 2 and 3 with combinations using both UDP and TCP as transport. Over TCP the number of connections was scaled up to 600 using 2 IP Addresses on the server and establishing 2 NFS connections per client.

  Performance of NFS over TCP has improved almost five imes over previous NFS releases and is now almost equivalent to UDP performance. Operations that used to take up to 25 minutes on an average, are now complete within 5 minutes.

- The NetWare and independent modes of file access are supported to maintain file and directory access security.

  For details, refer to "File Access Modes" on page 34.

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

  For details, refer to "NFS Server File Lock Manager" on page 39.

- The NFS Server is now MP enabled.

- The NFS Export filename and format have been modified to make it more user friendly.

  For details, refer to "Export Options" on page 57 and the comments in the sys:/etc/exports file.

- You can now administer NFS Server using the Web-based administration utility provided by NPS Gadgets.

For details, refer to “Managing NFS Server Using NPS Gadgets” on page 60.

- Only NSS-type volumes can be exported using NFAU. The new design of NFS Server does not support the NetWare traditional file system.

Features of Native File Access for UNIX

- NFS Server

  Network File System (NFS) Server 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 access NetWare files using the NFS Server.

  See “NFS Server” on page 33.

- Web-Based Administration for NFS Server

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

  See “Managing NFS Server Using NPS Gadgets” on page 60.

- 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 40.

- UNIX User Management

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

  See “UNIX User Management Using eDirectory” on page 43.

- ConsoleOne-Based Administration for Network Information Services

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

  See “ConsoleOne-Based Administration” on page 44.

Overview of Native File Access for UNIX

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

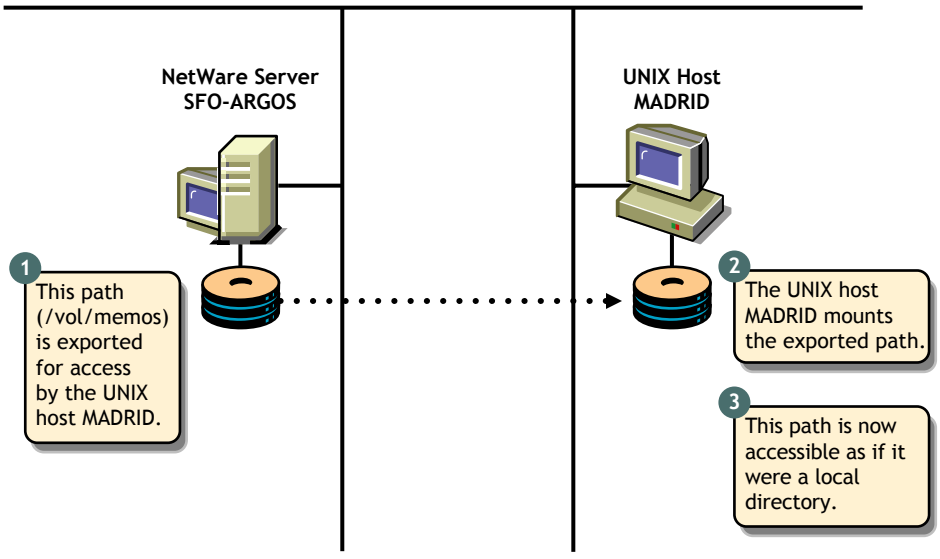
- “NFS Server” on page 33.
- “Network Information Service” on page 40.
- “User and Group Information” on page 43.
- “ConsoleOne-Based Administration” on page 44.
- “Administration Utilities” on page 45.
- “Upgrade Utility” on page 46.

NFS Server

Network File System (NFS) Server 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 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, make it 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 hosts, export the directory as Read-only.

Accessing the NetWare File System from UNIX NFS Clients

After exporting the NetWare file system from a NetWare server, mount the exported file system on the UNIX workstation for normal access. 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 that you create. This directory becomes the access point for the NetWare file system. When you select an existing directory as a mount point, the contents of the existing directory are not accessible until you unmount the remote file system.

- Mounting the NetWare directory

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

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

File Access Modes

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

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

- "Independent Mode" on page 34
- "NetWare Mode" on page 36

In this section, the term *mapped user* refers to the user who creates a connection to a drive on the network. After mapping to the drive, the user can use it like a local hard disk, based on the rights assigned to the user on the drive. You can map to a specific folder on the drive or to the root of the drive.

The term *unmapped user* refers to user accessing a file or directory without access mapping.

Independent Mode

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

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

Independent Mode Functionality

This mode functions as follows:

- NetWare trustees are not assigned.
- No mapping of permissions RWX to SRWCEMFA and vice versa is done.
- No NetWare attribute mapping is done.
- IRM is set to the default (SRWCEMFA).
- NetWare OwnerID is mapped to UNIX user on the NFS side.
- UNIX UID, GID, and UNIX permissions do not affect NetWare rights or attributes in any way.
- Changing Group and Fmode does not affect DOS side.

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

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

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

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

NetWare Mode

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

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

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

To get the UNIX permissions, map the user with the required effective rights on the NetWare side.

Export Option for NetWare Mode

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

For example:

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

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

NetWare Mode Functionality

This mode functions as follows:

- Trustees are not assigned and attributes are not mapped. [r-w-x] is not mapped to [SRWCEMFA].
- By default, IRM is set to SRWCEMFA.
- The default permissions for files created by UNIX users are based on the effective rights of the mapped NetWare user account.
- NetWare ownership of a file is determined by the mappings between NetWare and UNIX global objects. The OwnerID (NetWare files) is mapped to the UNIX owner of the file.
- Files created from DOS by unmapped users have UID set to 0.
- The chown and chgrp commands are unsuccessful.
- Touch command functionality is normal. It initiates a recomputation of permissions or owner change as required.
- The chmod, chown, and chgrp commands have no effect on the NetWare rights and attributes of the file and they fail silently.
- Executing a chmod command would reflect changes on the UNIX side only when the _x (execute permission) for file is involved.

  The chmod commands allows setUID, setGID, and sticky bits to be set for a file or a directory and to be retained persistently between NetWare owner changes or permission recomputations.

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

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

Rights Mapping

The following table outlines the rights mapping for file/directory/folder.

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

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

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

IMPORTANT: To ensure that Others in UNIX receive sufficient permissions, create a Novell eDirectory Group object and set the UNIX profile GID of the Group object to 65535. Make this object a trustee to the exported path with sufficient rights.

Refresh of Permissions

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

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

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

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

  ```
  touch *
  ```

  ```
  touch filename|directory_name
  ```

  ```
  touch .
  ```

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

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

  For example, if the World had no permissions for a directory, and Others receives r-x for, by giving Read and FileScan rights for the World object.

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

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

General Behavior

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

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

NFS Server File Lock Manager

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

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

NetWare NFS Lock Manager file locking functions similarly to NetWare file locking by setting mandatory (physical) locks that automatically prevent simultaneous file access by users. File locks are provided only when an application contacts the NetWare NFS lock manager. If an NFS user or process attempts to access a file through an application that does not contact the lock manager, no lock is issued. For example, if a UNIX user accesses a NetWare file using the vi editor, which does not contact the lock manager, no file lock is issued. If another UNIX user attempts to simultaneously access the same file, access is permitted and inconsistencies can occur.

The NetWare NFS Server synchronizes file locking by using both the NetWare and NFS lock managers. Synchronized file locking provides the NFS client with mandatory locking, provided lock manager software is running on the NetWare NFS Server and the remote application contacts the lock manager.

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

Network Information Service

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

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

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

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

A typical UNIX system stores user account information in the /etc/passwd file and group information in the /etc/group file. The migration utility lets you migrate the user/group information to eDirectory. For more information on the migration utility, see “Migrating NIS Maps” on page 50.

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

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

1. Right-click the NISSERV_*servername* object > Click Properties.

2 Click the Memberships tab to display the list of NIS Domains served by this NIS Server object.

3 Click the Others tab to view the IP address associated to *NISSERV_servername* object.

NIS Information on eDirectory

NIS Domain

The NIS services organizes nodes into administrative segments called *domains*. The NIS domain exists only in the local environment and usually covers a single network. 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, prefer relating the NIS domain name to their DNS domain name, but this is not necessary.

NIS Maps

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

The NIS Server supports both standard and custom maps.

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

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

- **Ethers Map**—A source of information about the Ethernet addresses (48-bit) of hosts on the Internet. The Ether objects (ieee802Device) store information about the Ethernet address and hostname.
- **Bootparams Map—**A source of information for various boot parameters. The Boot objects store information about the boot parameters of the various devices that are running. To migrate the Bootparams text filename from the ConsoleOne, name the text file to *bootp*.
- **Hosts Map—**Contains one entry for each IP address of each host. If a host has more than one IP address, it has an entry for each IP address. The Hosts objects store the IP address and hostname as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Netgroup Map—**A source of information about Net Group parameters. It provides the abstraction of net groups.
- **Networks Map**—Contains a single object for each network. The Network objects store network names as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Protocols Map—**Contains one object for each protocol. The Protocols objects store protocol names as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **RPC Map—**Contains one object for each Remote Procedure Call (RPC) program name. The RPC objects store RPC program names as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.

- **Services Map—**Contains an object for each service. The Services objects store service names, ports, and protocols as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Passwd Map—**Maintains the details of the users such as UID, Username, home directory.
- **Group Map—**Maintains the details of the groups present such as GID, Group name, and Group members.
- **Ypservers Map—**Maintains a list of NIS slave servers which can serve the NIS domain.

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

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

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

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

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

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

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

Janice_SmithMS 881-1456

Bob_RodriguezMS 235-6777

Eric_Mueller MS 769-8909
```

Various NIS Configurations

NIS can be configured in the following ways:

- “NIS Master Server” on page 42
- “NIS Slave Server” on page 43
- “NIS Client” on page 43

NIS Master Server

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

NIS Slave Server

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

After the slave server is set up, you do not need to manage the update process manually. The slave servers periodically query the master and request an update when the slave detects a more recent time stamp on the master.You can get an immediate update of the slave servers, through ConsoleOne 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 be used for load distribution in the network. A master NIS server for one domain can function as a slave NIS server for another domain.

NIS Client

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

For more information on setting up and managing NIS, see "Managing NIS Server" on page 64.

UNIX User Management Using eDirectory

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

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

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

When a set of users/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 does not exist, a new eDirectory User or Group object is created with default NetWare rights. If the User or Group object exists, the user or group's UNIX-related information is updated by default during the migration.

User and Group Information

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

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

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 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.

For information about UNIX user management, see “Migrating NIS Maps” on page 50.

ConsoleOne-Based Administration

You can use ConsoleOne to perform the following tasks:

- Configure the server's global parameters
- Configure and manage NIS services

- Configure error reporting
- Configure user and group UNIX information

For more information, see “ConsoleOne-Based Configuration” on page 47.

Administration Utilities

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

SCHINST

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

This utility does the following:

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

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

The syntax is:

```
schinst -n
```

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

NISINST

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

NIS Server uses this object to store the list of domain names 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.

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

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

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

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

Manually Executing Administrative Utilities

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

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

To manually run the administrative utilities:

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

   `schinst -n`

   SCHINST takes the administrator's FDN and password as input for extending the schema.
3. Run **`nisinst`**
4. Execute **`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 select Native File Access for UNIX while upgrading the operating system from NetWare 4.*x* or NetWare 5.*x* to NetWare 6.

When invoked during installation, the upgrade utility retains the existing configuration into the new configuration files, nfs.cfg, nis.cfg, and located in sys:\etc.

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

IMPORTANT: For this release, upgrade for NFS Server is not supported. Export the NFS shares again.

Configuring and Managing

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

- “Configuration Methods” on page 47
- “Configuring Server General Parameters” on page 48
- “Migrating NIS Maps” on page 50
- “Managing NFS Server” on page 56

- “Managing NIS Server” on page 64

Configuration Methods

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

ConsoleOne-Based Configuration

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

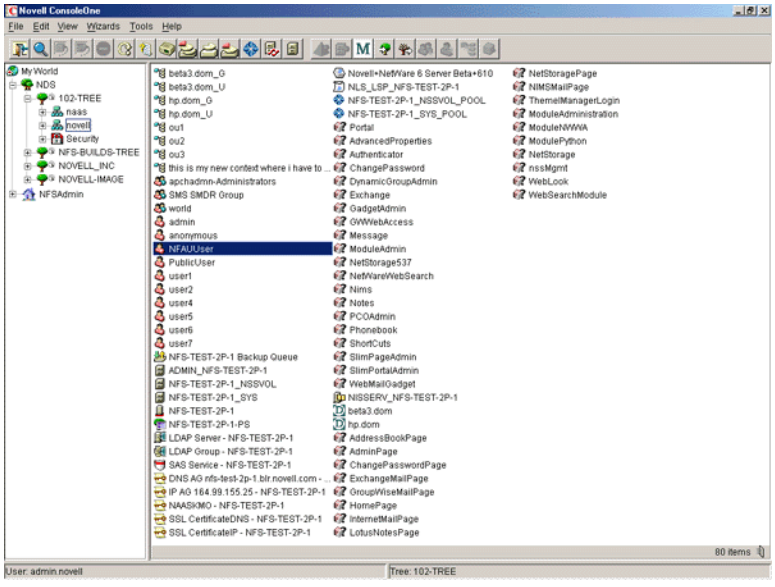
To start ConsoleOne from the client:

IMPORTANT: Before starting ConsoleOne, ensure to 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. Administration of NetWare NFS Services 3.0 on NetWare 5.1 from ConsoleOne on NetWare 6 is not supported.

Figure 2 Native File Access for UNIX Objects



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

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, change the required parameter value in the corresponding .cfg file and restart the module.

Configuring Server General Parameters

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

File-Based Configuration of Server General Parameters

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

Table 1 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 starts from the default (first) bindery and then in the server's default context.

ConsoleOne-Based Configuration of Server General Parameters

This section explains the following tasks:

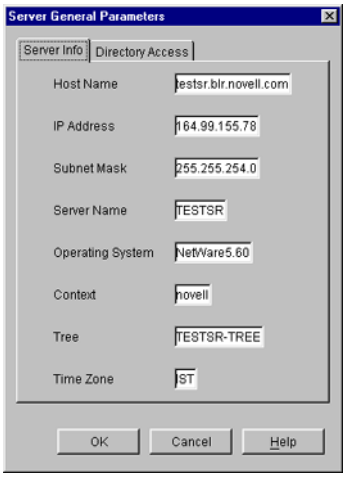
- “Viewing the Server General Parameters” on page 49
- “Configuring the Server General Parameters” on page 49

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.

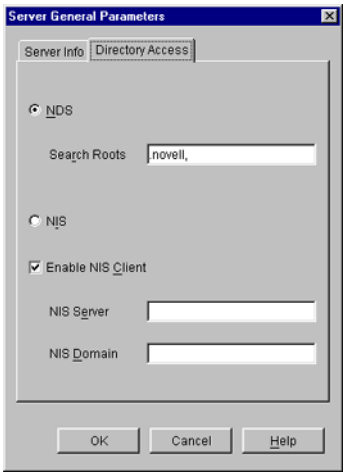
Time Zone—The world time zone reference for your area. The time zone is used for time stamps and to set time synchronization. The time zone reference is set during the NetWare installation.

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.

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

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

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

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

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

For more information on UNIX user management, see "UNIX User Management Using eDirectory" on page 43.

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: Use all options only in the specified order.

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

  `makenis -d domainname`

  The *domainname parameter* is mandatory.

- To capture the results of the migration, use the following format:

  `makenis -r resultfilename -d domainname`

- To remove the existing domain data and then migrate, use the following format:

  `makenis -rd domainname`

- To specify the context where you want to create your Domain object and data, 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 you do not specify anything, all the files in the makefile are migrated.

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

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

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

- To migrate specific maps, use the following format:

  `makenis -d domainname mapname1, mapname2`

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

  `makenis -d domainname mapname -lp lineoffset`

  Or

  `makenis -d domainname mapname, -bp byteoffset`

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

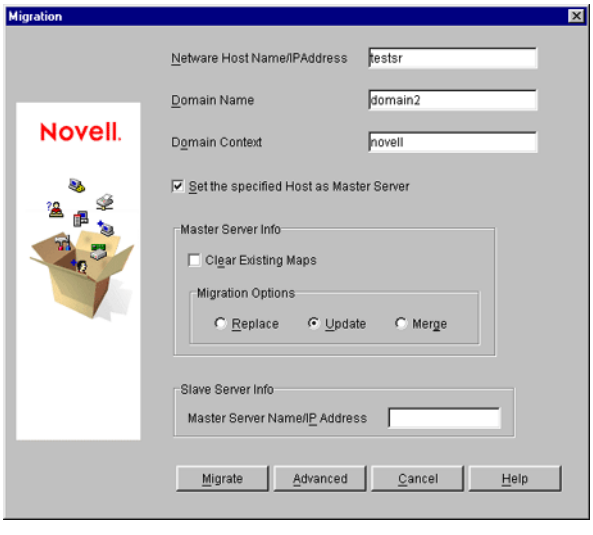
  Makenis adds users to the Members attribute, gives the user the rights equivalent to that of the group, and updates its Group Membership attribute.

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:

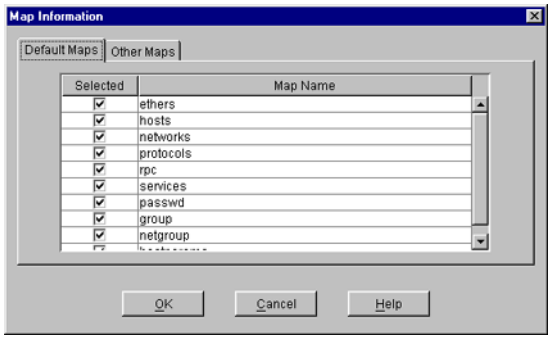
Figure 5 Migration Panel



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

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

Figure 6 Map Information Panel

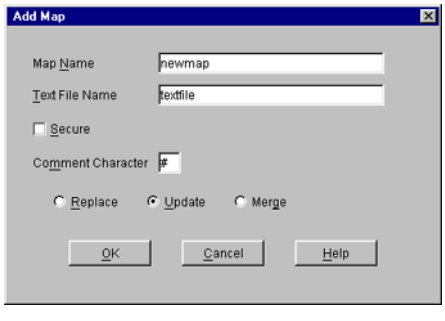


10a. Click either Default Maps or Other Maps.

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. (Conditional) Click Secure, if you want to enable secure access to the map.

11c In the Comment Character box, enter the comment character present in the specified text file and click OK.

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

12 Click Migrate.

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

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, select the tree and log in to it.

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

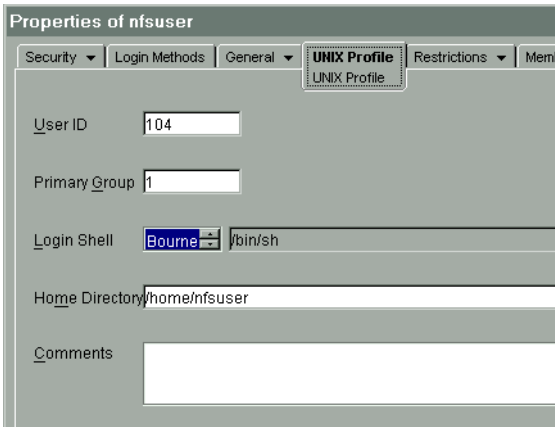
The User objects under this particular container are displayed.

3 Right-click the User object whose properties you want to change 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 Click UNIX Profile to modify the UNIX user profile, and specify the information in the following fields:

User ID—The users' UNIX UID.

Primary Group—The group ID (GID) of the group this user belongs to. To 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.

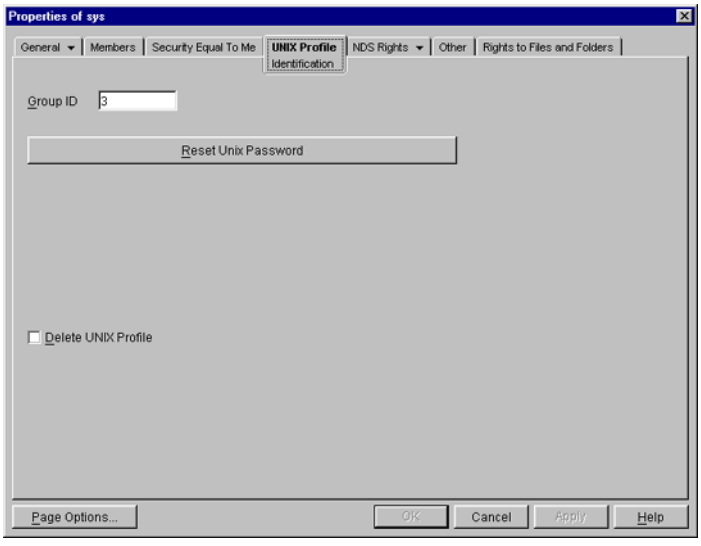
The groups under this particular container are displayed.

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

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

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

Figure 9 UNIX Profile Tab of Group Properties Panel



4 Click the UNIX Profile tab and specify the information in the following field, to modify the UNIX group profile:

Group ID—The group's UNIX GID.

5 Click Apply > OK.

Adding a New User or Group

To add a new user:

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:

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

Managing Migration Utility Log Files

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

- The containers added such as domainname container, domainname_U (for users), 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.

Managing NFS Server

This section discusses the following topics:

Starting and Stopping NFS Server

To start NFS Server at the system console, enter

```
load xnfs
```

To stop NFS Server at the system console, enter

```
unload xnfs
```

Export Options

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

The syntax for exporting a pathname is

```
/pathname [-ro|-rw][-root][-anon][-nwmode]
```

Pathname	Usage
/pathname	When you give a pathname, make sure of the following: ◆ Always prefix the pathname with a slash (/). For example /nssvol. ◆ When exporting a path, the volume name is not case sensitive. However, any directory names in the path should exactly match the directory names that exists in the NFS (UNIX) name space. To view the name as it displays in the NFS (UNIX) name space, use NWADMN32, browse to the volume, and then to the folder and select Details. You can view the name of the folder as it exists in every name space in the details.

When you do not specify any option, by default the root, anon and read-write access is denied for all the clients and the read-only access is enabled for all NFS hosts.

For more information on using the export options, see “Export Option Examples” on page 59, and “Export Options Usage Guidelines” on page 59.

Trusted Hostname

The following formats are supported for the access list entries:

- Trust individual hosts based on complete or short DNS name or IP address.
  - The IP address. For example, aaa.bbb.ccc.ddd.
  - Complete or short DNS name. For example, xyz or xyz.us.acme.com.
- Trust a complete DNS Domain, or a Subnet based on network number.
  - DNS Domain.suffix distinguished from hostnames and netgroups by a prefixed dot (.). For example, .us.acme.com trusts all the hosts in the us.acme.com DNS Domain
  - The network or subnet component is prefixed by an at-sign (@). For example, @129.144.255 trusts all hosts in the 129.144.255 network.

If the network prefixes are not byte-aligned, the syntax allows a mask length to be specified explicitly following a slash (/) delimiter.

For example, rw=@129.144.132/17 where the mask is the number of leftmost contiguous significant bits in the corresponding IP address.

Updating Exports List

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

```
xnfs mount refresh
```

Alternately, unload and reload xnfs.nlm.

The following table explains the various export options:

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

Export Option	Description
-ro	Exports the pathname with read-only rights to all the clients.
-ro = host[:host]	Exports the pathname with read-only rights *only* to the listed clients.The listed clients do not have root access.
-ro = host, root[:host,root]	Exports the pathname with read-only rights *only* to the listed clients.The listed clients have root access.
-rw	Exports the pathname with the read-write rights to all the clients.
-rw = host[:host]...	Exports the pathname with read-write rights *only* to the listed clients.The listed clients do not have root access.
-rw = host, root[:host,root]...	Exports the pathname with read-write rights *only* to the listed clients.The listed clients have root access.
-root	Exports the pathname with root access rights to all the clients.
-root = host[:host]...	Exports the pathname with root access rights *only* to the listed clients. No other clients have root access unless you specify the corresponding -ro or -rw options.
-anon	Exports the pathname with rights for anonymous user access to the file system, based on Others' permissions. **WARNING:** Do not use this option when root access is given to all the clients.

Export Option	Description
-anon= host[:host]...	Exports the pathname with rights for anonymous user access *only* for the listed clients.
-nwmode	Indicates if a particular path is exported in NetWare mode or not. If -nwmode is specified, the path is treated as being exported in NetWare mode. If it is not specified, it is treated as an Independent mode export.

Export Option Examples

Here are a few examples of using the export options:

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

  ```
  /nssvol/dir1
  ```

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

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

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

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

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

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

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

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

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

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

Export Options Usage Guidelines

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

  For example: `- ro` is incorrect, but `-ro` is correct.

- Do not use double quotes (" ") to separate the options.

- Use the colon (:) to separate multiple hosts when specifying the same option for the hosts.

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

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

  The following is incorrect:

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

- Append `,root` to hosts in `-ro` and `-rw` options to indicate root access.

For example, to give read-write root access to host3, use the following format:

```
/nssvol/dir2 -rw=host3,root
```

- Do not specify the same option globally as well as for a client.

  For example, the following syntax is incorrect:

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

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

  For example, in

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

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

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

  host1 has read-only access even though other clients continue to have the global permissions of read-write.

- When you repeat the same entries with multiple options, then the later option overrides the previous option.

  For example, in

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

  host1 has read-write access.

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

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

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

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

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

For more information on NFS Server, see “NFS Server” on page 33.

Managing NFS Server Using NPS Gadgets

You can perform the following administrative tasks using the NFS Administration Gadget.

- “Starting/Stopping NFS Services” on page 61
- “Updating the Umask Value” on page 61
- “Managing the Exported Paths” on page 61
- “Exporting a New Path” on page 62
- “Editing Exported Path Properties” on page 63

Meet the following requirements for NFS Server Admin gadget to get installed in iManager

- ❑ Apcahe Web Server is selected during NetWare 6.5 install.

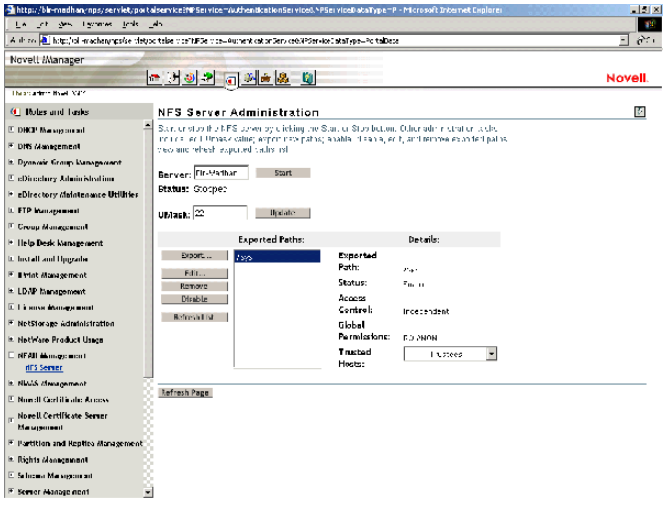
- ❑ iManager 2.0 is selected during the NetWare 6.5 install.

  For more information about installing iManager 2.0 refer to Installing Novell iManager section in the *Novell iManager 2.0 Administration Guide* available with this release.

Administering NFS Server

The NFS Server Administration screen displays the *Servername* that is being administered.

Figure 10 NFS Server Administration Screen



Starting/Stopping NFS Services

Click Stop or Start as required.

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

Updating the Umask Value

Enter the Umask value and click Update. Enter octal digits in the value range: 000 to 777. Default value = 022. Umask refers to the File mode creation mask for default UNIX permissions.

Managing the Exported Paths

1. In the Exported Paths table of the NFS Server Administration screen, view the list of exported paths.
2. Select a path in the Exported Paths table to view path details such as the Exported path, Access Control Mode, Global Permissions, and Trusted hosts.
3. Select a path in the Exported Paths list to manage the exported paths.

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

Exporting a New Path

Click Export to launch the Export Options screen where you can export a new path. For details, refer “Exporting a New Path” on page 62.

Editing Path Properties

Click Edit to launch the Export Options screen where you can view or modify the properties of an exported path. For details, refer, “Editing Exported Path Properties” on page 63.

Removing a Path

Click Remove to remove the exported path.

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

Refreshing a Path

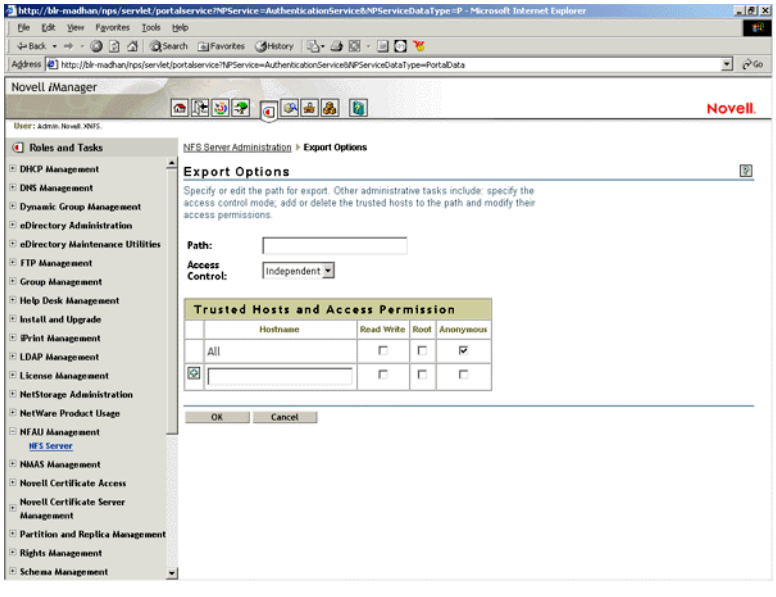
Click Refresh List to refresh the list of exported paths.

This updates the Exported Paths table based on the exports file on the server side. If a path is manually deleted in the exports file on the server side, refresh for the updates to get reflected.

Exporting a New Path

1 In the NFS Server Administration screen, click Export New Path to launch the Export Options screen.

Figure 11 Export Options Screen to Export a New Path



2 In the Path field, enter the pathname that you want to export. The format for exporting a path is /*pathname*

For example,

```
/nssvol
```

Prefix the pathname with a slash (/). The pathname can have up to 256 characters. It cannot have null, or special characters.

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

   Default mode = Independent.

4. In the Trustee List Hostname Textbox in the Trustee List table, enter the hostname that you want to make a trusted host for the exported path.

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

5. Assign the required access permissions to the trusted host.

   The All row indicates the default permissions given to all trusted hostnames. The default permissions are checked in the checkboxes; by default, read/write and root access are denied, and anonymous (anon) and read access are enabled, for all clients.

   - Check Read/Write to give read/write access to the hostname. This access is denied by default.
   - Check Root access to Check this to give root access to the hostname. This access is denied by default.
   - Check Anon access to give anonymous access to the hostname. This access is given by default.

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

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

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

7. Click OK to save the modifications and return to the NFS Server Administration screen, or click Cancel to cancel the modifications and return to the NFS Server Administration screen.

Editing Exported Path Properties

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

   This launches the Exports Options screen where you can view or modify the properties of the exported path.

2. Update the access control mode. You can do this by selecting NetWare or Independent as required from the Access Control Mode drop-down list.

3. Add the trusted hosts. For information on adding trusted hosts, refer Step 4 on page 63.

4. Update access permissions for the trusted hosts. For information on assigning access permissions, refer Step 5 on page 63.

5. Click the Add symbol (+) besides the text box to add the host to the trusted host list.

6. Click the Delete symbol (X) besides the text box to delete the trusted host.

7. Click OK to save the modifications and return to the NFS Server Administration screen, or click Cancel to cancel the modifications and return to the NFS Server Administration screen.

Managing NIS Server

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

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

For more information about NIS, see "Network Information Service" on page 40.

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 is referenced. By default the NISINST utility creates an object named NISSERV_*ServerName*.
INTERDOMAIN_RESOLUTION	0	Specifies whether interdomain resolution is allowed or not. If allowed, DNS is contacted for hostname resolution even if NIS is not running. This is used for host maps only.
FILEMARK_LOG_FREQ	100	Puts the file in the log after parsing the specified number of records. This is used by the migration utility when the administrator wants to migrate maps 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:etc\nis	The path in the NetWare server where you want to write the log file for migration.
MAX_LOG_MSG	5000	Upper limit of number of log messages that can be logged. The information is specific to each log file. By default the last 5000 messages are displayed. If the number of log messages is set to *n*, the last *n* messages are retained.

Parameter	Default Value	Description
NIS_LOG_LEVEL	7	The log level indicates the types of messages to be logged. You can either select one of these or a combination of these. To get the combination, add two or more log levels. For example, to get Error and Information Messages, set the Log level to, 5= (1+4). By default, you get all the messages.
MAP_REFRESH_DEFAULT	24:00:00	Specifies the default time interval for refreshing the maps by synchronizing the maps in the slave server with the master.
NIS_ADMIN_OBJECT_ CONTEXT		The context where the NIS Admin object is created.

Setting Up a NetWare Server as a NIS Master

1. Copy the NIS related text files required for the domain from the UNIX machine (which are available in /etc in UNIX) into sys:\etc\nis.
2. (Conditional) Set up other NIS server as slave to this NIS server:
   - **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 51.
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 need 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*
4. Ensure that 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
   ```

Setting Password from NIS

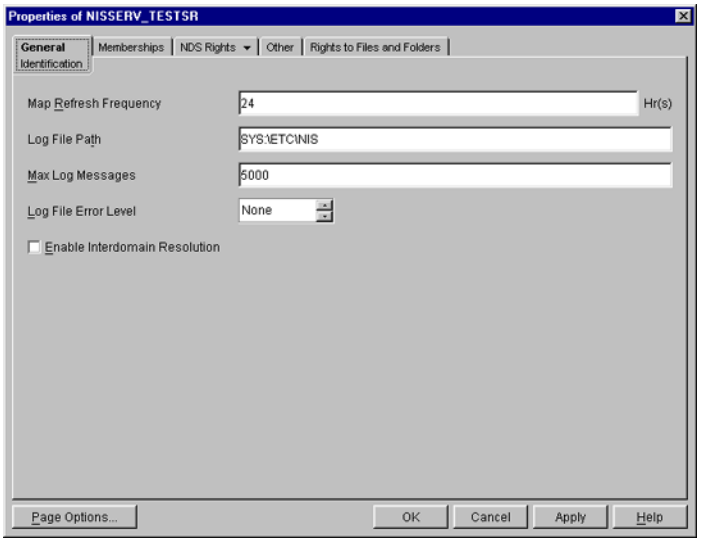
To log in or set the password for a user from a UNIX NIS client, set the default domain in the NetWare server using ypset.

ConsoleOne- Based Management for NIS Server

NIS Server Configuration Parameters

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

Figure 12 NIS 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 to the NetWare Server where you want to write the NIS log files.

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

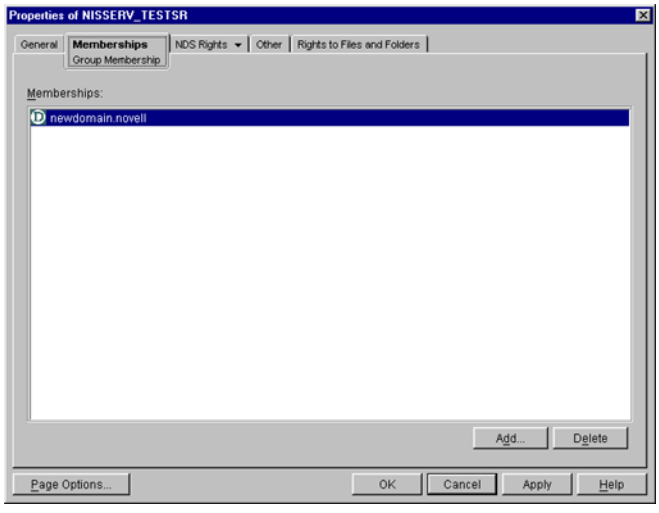
Log File Error Level—The level of error messages written to the audit.log file. Select an error level from the drop-down list.

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

Viewing Domains Served by NIS Server

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

Figure 13 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) to sys:\etc\nis.
2. (Conditional) Set up other NIS server as slave to this NIS server.
   - **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
     ```

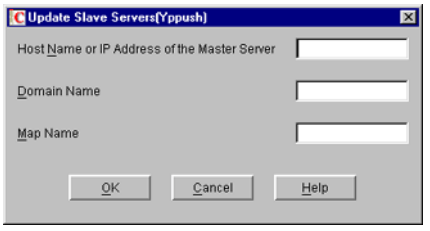
     NOTE: The first field should not be IP Address.
   - **2b** Enter the YPSERVERS map entry in sys:\etc\nis\nismake with its path in the following format:

     ```
     YPSERVERS sys:\etc\nis\ypserv
     ```
3. Migrate the domain. For migration information, see “ConsoleOne-Based Migration” on page 52.
4. Start NISSERV.
5. (Conditional) Use the YPPUSH utility to update the Slave NIS Server.

The YPPUSH utility copies a new version of the named NIS map from the master NIS server to the slave NIS servers. The YPPUSH utility is normally run only on the master NIS server after the master databases are changed and the changes need to be updated in the NIS slave servers immediately. The YPPUSH utility first constructs a list of NIS slave server hosts by reading the NIS map Ypservers within the same domain. Then a transfer map request is sent to the NIS server on each host.

Right-click NISSERV_*servername* and then click Update Slave Server. A panel similar to the following appears:

Figure 14 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. Enter the NetWare hostname/IP address, slave domain name, and context where the Domain object is to be created, to migrate a domain.
6. Uncheck Set the Specified Host As Master Server to set the NIS Server as slave for this specified domain.
7. Enter the Master server's name /IP address in the Slave server information.
8. Click Migrate to migrate the domain.

Configuring eDirectory Objects to be Served by NIS Server

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

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

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

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

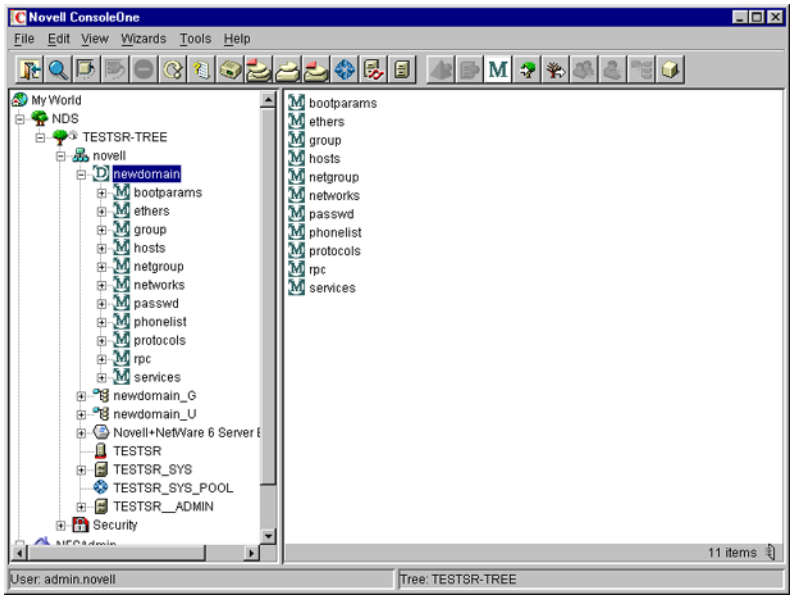
You can create new NIS maps and NIS map records under NIS domain object as you create normal eDirectory objects.

NOTE: No objects are 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 are available as objects under the migrated NIS domain object.

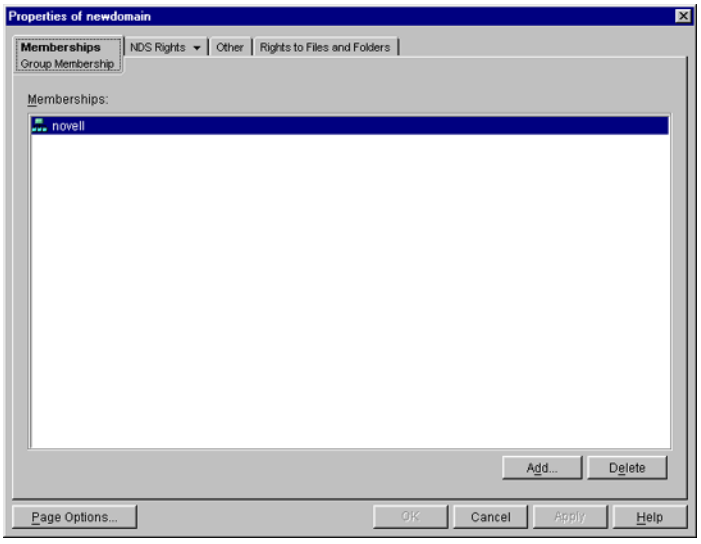
Figure 15 Maps under the Migrated Domain



When a client call is made to this domain, the NIS Server lists the data present under the corresponding Domain object. However, for user/group details, it looks for users and groups belonging to the domain under the contexts specified by an attribute of the Domain object.

To view the list of contexts where the users and groups are located, right-click Domain object and then click Properties > Membership. A panel similar to the following appears.

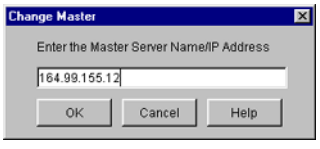
Figure 16 Domain Properties Panel



If the NetWare NIS Server is a slave for a domain and the master NIS server for that domain is changed to some other server, to get the updates from the new master, you need to change the NIS master server name for the Domain object present in the NetWare NIS slave server.

Right-click Domain Object and then click Change Master. A panel similar to the following appears:

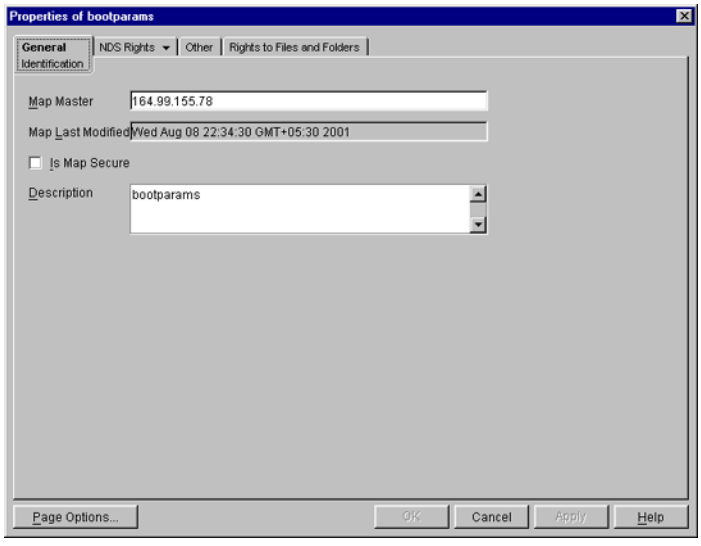
Figure 17 Change Master Panel



Enter the IP address of the new NIS master server. The NIS slave server now contacts the new master server for updates on all the maps under this domain.

You can view the properties for each map. Right-click Map Object > click Properties. A panel similar to the following appears:

Figure 18 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.

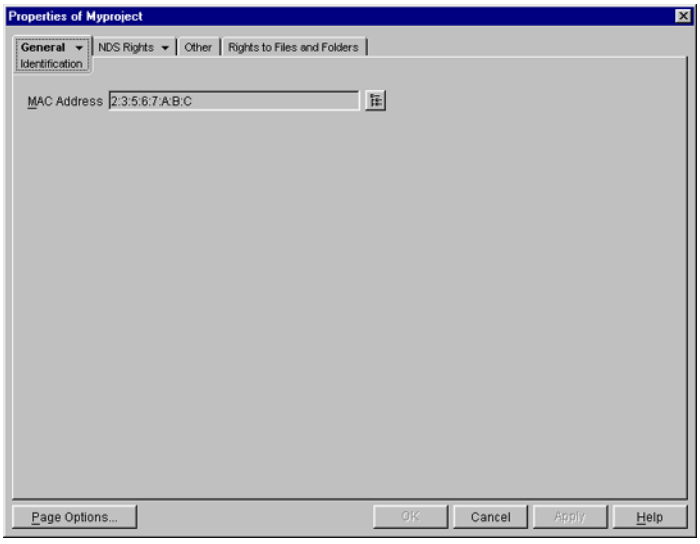
To add an object to a map, right-click the map in the left panel, click New, select the object, and then specify the details of the object in the dialog box.

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 19 Ethers Map Records Properties Panel

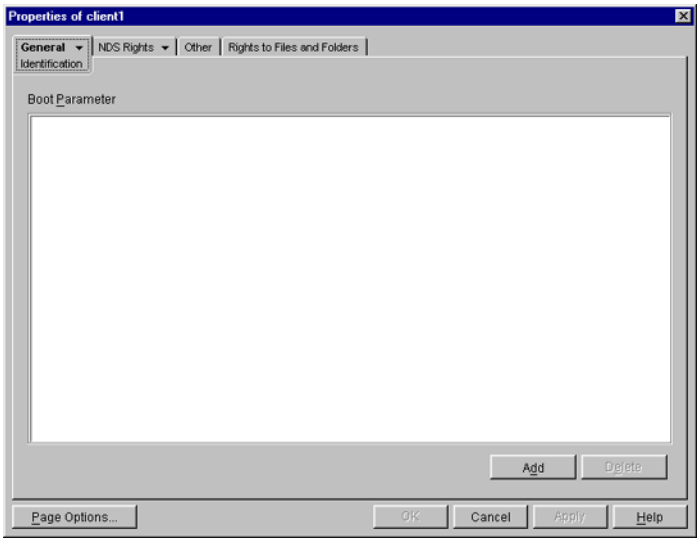


This panel shows the Ethernet address of the host.

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

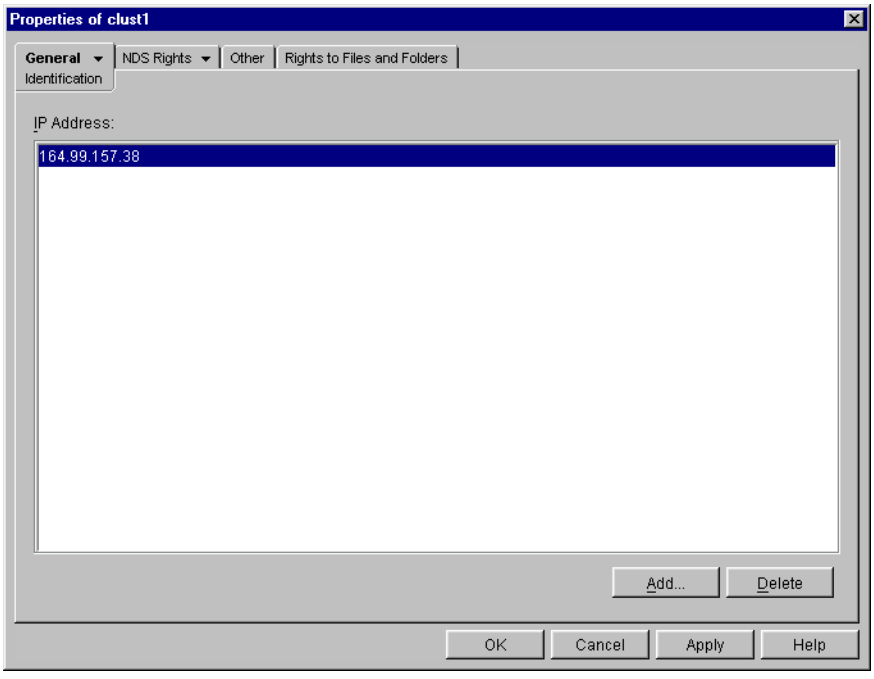
Click the icon to enter the Ethernet address of the host, and then click Apply > OK.

Figure 20 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 21 Host Map Records Properties Panel

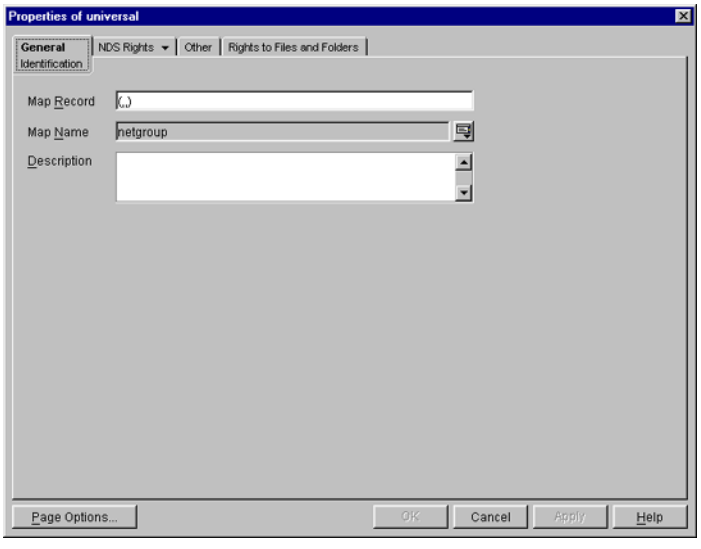


1. To add the host address, click Add, enter the IP address of the host, and then click Apply > OK.

   The network addresses are written in the conventional decimal dot notation.

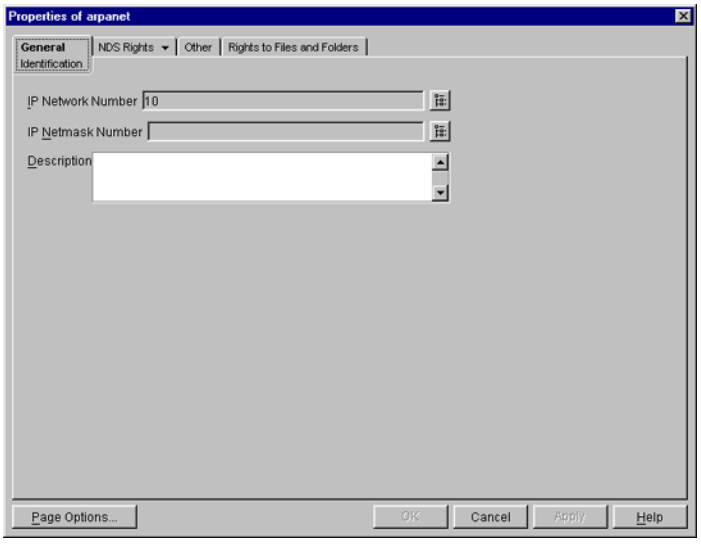
2. To delete the host address, select the host's IP address from the IP Address field, and then click Delete > Apply > OK.

Figure 22 Netgroup Map Records Properties Panel



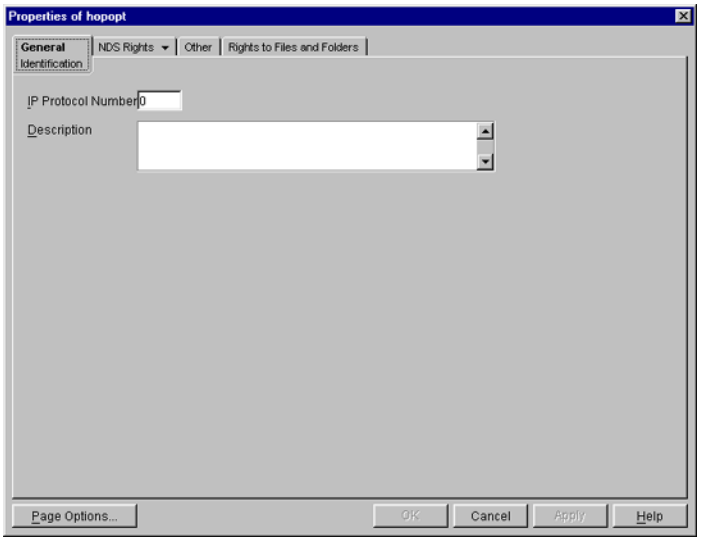
To add a netgroup address, enter the name of the Map Record, browse for the Map Name, enter the description of the map, and then click Apply > OK.

Figure 23 Network Map Records Properties Panel



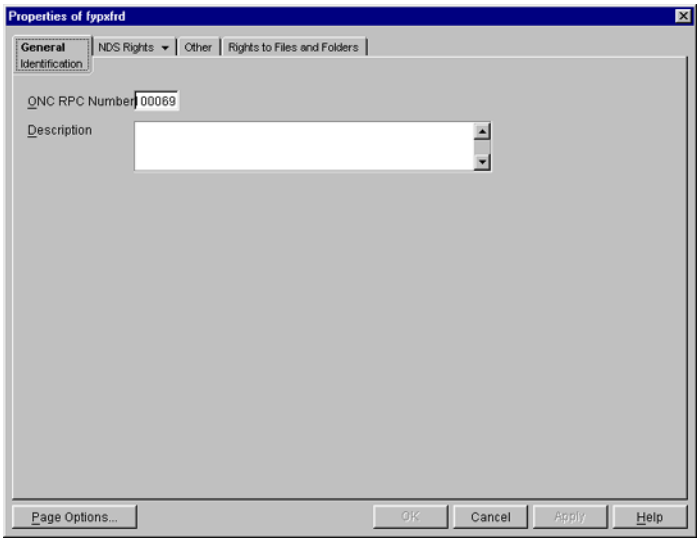
1. To enter the IP network number, click Browse, enter the network number, and click OK.
2. To enter the IP netmask number, click Browse, enter the netmask number, click OK, enter the description of the record, and then click Apply > OK.

Figure 24 Protocols Map Records Properties Panel



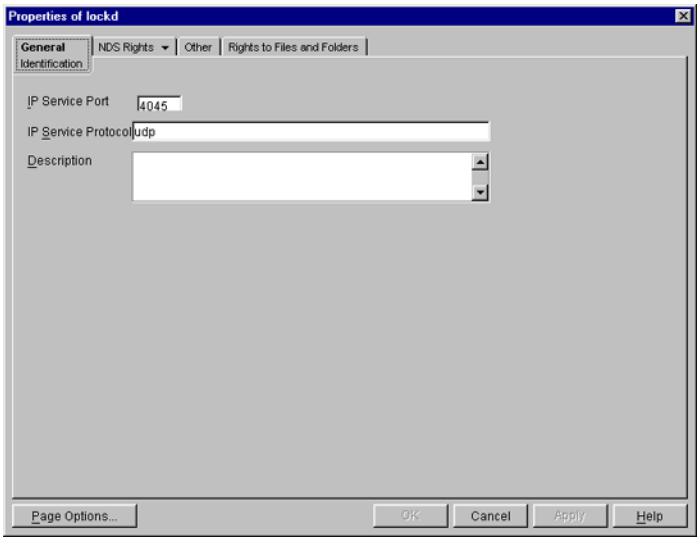
1. Enter the protocol number and a brief description of the record.
2. Click Apply > OK.

Figure 25 RPC Map Records Properties Panel



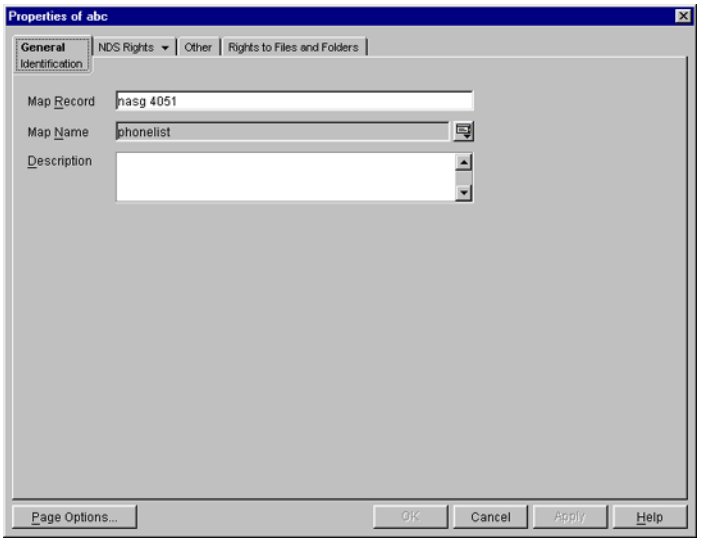
1. In the ONC RPC Number field, enter the RPC number of the program.
2. Enter a brief description of the record.
3. Click Apply > OK.

Figure 26 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 27 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* and then click Start/Stop Services.

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

Setting Up with Novell Cluster Services

To get the full benefit of using Native File Access for UNIX with Novell Cluster Services™, you need to install and configure the software to work in a cluster environment.

This section describes the following:

- "Prerequisites" on page 76.
- "Setting Up" on page 77.
- "Configuring Cluster Resource Properties" on page 78.
- "Component-Specific Configuration" on page 80.
- "Starting and Stopping Native File Access for UNIX with Cluster Services" on page 80.

Prerequisites

Before installing Native File Access for UNIX with cluster support, create a shared volume and a Cluster Volume object.

1. Create the sys:\nfsback directory.
2. Make a backup of the configuration files.
   - When cluster enabling for the first time, copy the nfs.cfg, nis.cfg, and the exports file from sys:\etc to sys:\nfsback.
   - When upgrading from a previously cluster enabled setup, copy the nfs.cfg, nis.cfg, and the exports file 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.
5. Create logical volumes in the pool.
6. Modify or view cluster resource object properties.
   - **6a** Cluster object (console view) > Cluster Resource Object > Right- click Properties.
   - **6b** Set the Start, Failover, and Failback modes.
   - **6c** Verify the order of the servers in the nodes list.
   - **6d** Save the changes to the Cluster Volume object, and then click OK.

Setting Up

1. (Conditional) If the NFS Services are running on any of the nodes, run **`nfsstop`** on those nodes.
2. Remove **`nfsstart`** from autoexec.ncf on all nodes.
3. Edit nfsstop.ncf and uncomment unloading of nfsadmin, pkernel and rpcbstub.
4. Delete all the NISSERV_servername NDS objects pertaining to the servers in this cluster.
5. Use the spinst utility to cluster enable and upgrade the configuration.
   - **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 shared_vol_name: -n res_name -i res_ipaddress`
   - **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 shared_vol_name: -n res_name -i res_ipaddress`

   IMPORTANT: When using spinst, make sure to include the colon (:) after typing the shared_vol_name.

Command Parameter	Description
-v	Shared volume name
-n	Resource name.
-i	Resource IP address.

6. Copy the necessary files to *shared_vol_name:\etc*.

6a Copy the configuration files, nfs.cfg, nis.cfg to *shared_vol_name:\etc*.

6b Copy the exports file from sys:\etc to the *shared_vol_name*:\etc.

Remove all local exports (paths exported from the local disk) and export the shared path by adding the shared path to the exports file at *shared_vol_name*:\etc.

6c Copy the nfsstart.ncf and nfsstop.ncf from sys:system to the *shared_vol_name*:\etc.

IMPORTANT: If you manually create \etc on shared volume, ensure to use all small case letters when creating the folder.

Configuring Cluster Resource Properties

Load and Unload Script

Customize your specific NetWare NFS Services configuration by editing the IP addresses and volume-specific commands in the load and unload scripts of the cluster volume object to which you are going to associate NFS Services.

Select and right-click the Cluster Volume object and then click Properties to find the Cluster Resource Load Script and Cluster Resource Unload Script.

Following are the formats for these scripts.

Load Script

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

nfsclust *AAA.BBB.CCC.DDD shared_vol_name shared_pool_server_name*

shared_vol_name:**\etc\nfsstart**

For example,

```
nfsclust 129.101.183.156 user USER_SERVER
user:\etc\nfsstart
```

IMPORTANT: When using nfsclust, make sure *not* to include the colon (:) after typing the shared_vol_name.

In this example,

- AAA.BBB.CCC.DDD=129.101.183
- shared_vol_name=user
- shared_pool_server_name=USER_SERVER

Unload Script

In the unload script, add the following at the beginning of the script:

shared_vol_name:**etc\nfsstop**

unload nfsclust

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
Failback	AUTO, MANUAL, DISABLE	AUTO allows Native File Access for to UNIX automatically move back to its preferred node when the preferred node is brought back online. 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. DISABLE causes Native File Access for UNIX to continue running in an online state on the node it has failed to. Default = DISABLE

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

Configuring the components of Native File Access for UNIX for cluster enabled set up is much the same as configuring the components without cluster services.

However, keep in mind the following points while configuring the following components:

- “NFS Server” on page 80
- “Network Information Service” on page 80

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 80.

NFS Server

While configuring the NFS Server:

- Export only the volumes in the shared pool.
- When mounting exported shared volumes from an NFS client, use the virtual IP address of the cluster volume object.

Network Information Service

While configuring the NIS clients:

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

Location of Configuration Files

Most configuration files are now located in the \etc directory of sharedvolume. 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	*shared_vol_name*:\etc
nis.cfg	sys:\etc	*shared_vol_name*:\etc
exports	sys:\etc	*shared_vol_name*:\etc
nismake	sys:\etc\nis	sys:\etc\nis
nfsstart.ncf	sys:\system	*shared_vol_name*:\etc
nfsstop.ncf	sys:\system	*shared_vol_name*:\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).

A System Messages

This section describes the system messages of the various components of Novell Native File Access for UNIX.

MakeNIS

Setting the log file

Possible Cause: The directory specified when creating the log file might be incorrect.

Action: Check for the validity of the directory path you specified.

Required parameters are missing

Explanation: The domain name is mandatory.

Possible Cause: The user has not specified the required parameters.

Action: Enter all the mandatory parameters.

Domain name is missing

Possible Cause: The user has not specified the domain name.

Action: Enter the domain name.

No make data for map

Possible Cause: There is no data corresponding to the map in the makefile.

Action: Enter the record corresponding to the map.

File is older than corresponding map

Possible Cause: The text file used for making this map is older than the map that exists on eDirectory.

Action: Change the time stamp on the text file by saving it again.

Object with same domain name already exists

Possible Cause: An eDirectory error occurred while adding the specified object.

Action: Check whether the object already exists.

Unable to add users to group objects

Explanation: Users are already present.

Unable to get the host name or IP address of the machine

Possible Cause: The configuration files containing the host data are not correct.

Action: Check the configuration file.

NIS Installation

Opening configuration file

Possible Cause: Either the file is not present in the specified location or the input is illegal.

Action: Check for the existence of the specified file or the validity of the input.

Reading configuration file

Possible Cause: It is not the correct configuration file.

Action: Check the configuration file.

Getting default host names

Possible Cause: Unable to get the DNS name of the current host.

Action: Check whether entries in relevant configuration files are correct.

Updating the configuration file

Possible Cause: Either the configuration file is not present or it is corrupted.

Action: Check the configuration file.

NIS Services

Internal error with refresh watchdog

Possible Cause: The refresh thread of the NIS Server is failing.

Action: Unload the NISSERV.NLM and load it again.

RPC error

Possible Cause: There was an error on the RPC client call to NIS Server.

Action: Unload the NISSERV.NLM and load it again.

Internal error

Possible Cause: Failure to allocate memory for the domain list of the NIS Server.

Action: Unload the NISSERV.NLM and load it again.

Resource failure

Possible Cause: An NIS Server internal error occurred while allocating memory for its internal structure.

Action: Unload the NISSERV.NLM and load it again.

Unable to allocate space for domain index list

Possible Cause: Failure to allocate memory for the domain list of NIS Server.

Action: Unload the NISSERV.NLM and load it again.

Unable to respond to RPC request

Possible Cause: Failure in sending the RPC response back to the client because of the PKERNAL.NLM.

Action: Repeat the client call.

B Native File Access for UNIX FAQs

NFS Server FAQs

This section has the following NFS Server FAQs:

What is the difference in the export options /pathname -ro,root and /pathname -ro -anon?

When you specify **/pathname -ro,root**, the path is exported as read-only with root access to all clients.

However, when you specify **/pathname -ro -anon**, the path is exported as read-only with anonymous access to all clients. If you do not specify the anon option, then on the client side root cannot do any operations on the mount point.Even executing a cd to the mount point is not allowed.

What is the result of specifying only -ro as the export option?

When you specify only **`-ro`** option for the pathname, it exports the path as read-only to all clients. Because by default, root-access and anonymous access are disabled, the root cannot perform any operations except mounting on the mount point.

Specifying this option equals giving no options as the read-only option to all clients is enabled by default.

What is the significance of the SEARCH_ROOT parameter in SYS:ETC\NFS.CFG file?

This parameter is a list of contexts under which NFS* modules search for users that have their UNIX* profiles populated.

There are some rules that need to be observed to add to this search list:

- The specified contexts should begin with a period (.)
- Contexts can be specified as .Ou1.Top or as .Ou=Ou1.O=Top
- Items in the list must be separated by commas (,) but no spaces.

How do I manually set the UNIX profile of a user?

After the product installation is complete and the schema has been extended to have UNIX attributes, appropriate ConsoleOne® snap-ins are now available to populate those attributes.

To populate the UNIX attributes, follow these steps:

1. In ConsoleOne, select an existing Group object or create a new Group object.
2. Right-click this Group object and then click Properties.
3. Go to the UNIX Profile tab and enter the desired GID Value.
4. Select/create a User object whose UNIX profile needs to be updated.
5. Right-click this User object and then click Properties.
6. Click the UNIX Profile tab and then enter the desired UID Value.

   For the Primary Group field, using the browse button, select the Group object used in Step 1 and then click on Apply/OK.

Now there is a user whose UNIX profile is populated; but to make this visible to NFS modules, this User's context or one of its parents' context needs to appear in the SEARCH_ROOT parameter in SYS:ETC\NFS.CFG. For this change to get reflected (if a fresh context was added to the SEARCH_ROOT list), do an nfsstop and nfsstart again.

How do I set a User's UNIX profile to the Root's profile ?

In Step 6 above, setting the UID Value to 0 in the User ID field attaches the root profile to that User object. Again, make sure that either this User's context or one of its parents' context is in the SEARCH_ROOT list.

I'm trying to export a traditional volume using NFS Server, but it fails to mount on an NFS Client even though showmount shows the export. Why ?

The new design of NFS Server does not support NetWare Traditional File system.

Could not authenticate ContextHandle. Load schinst and try again. Exiting...9601

Ensure that in the NFS.CFG, the NIS_ADMIN_OBJECT_CONTEXT is set to .NSC or .O=NSC and that SEARCH_ROOT also has the same context in the same format and is preceded by a dot (.).

Execute **nfsstop** and run SCHINST.NLM (get the SCHINST.LOG and NFS.CFG after this)

Delete the NFAUUser object, run SCHINST.NLM and capture the log and configuration files and see if it works.

When I execute nfsstart after reinstalling the directory services in the server or joining the server to an existing tree or deleting the NFAUUser object, messages such as "Error unloading, killed loaded module (ndsilib.nlm)", or "Unable to Login. : error -669 Could not authenticate ContextHandle. Load schinst and try again. Exiting...-669" display. What should I do?

You need to do the following:

1. Execute **nfsstop**.
2. Execute **schinst -n**.
   - **2a** (Conditional) When you reinstall the directory services in the server or join the server to an existing tree, run **nisinst**.
3. Execute **nfsstart**.

NIS Services FAQs

This section has the following NIS Services FAQs:

When is the NISSERV_*ServerName* object created and what is its role in NIS functionality?

The NISServ_*Servername* object holds the list of domains served by the NetWare NIS Server. It is created by the NISINST.NLM executed during the installation. For correct functionality of NIS Server, set the following parameters properly:

- The NIS_SERVER_CONTEXT parameter in SYS:ETC\NIS.CFG, indicates the NDS context where the NIS Server object exists.
- The NIS_SERVER_NAME parameter in SYS:ETC\NIS.CFG indicates the NIS Server object used to hold the NIS Domains that are being served by the NetWare NIS Server.

When I select the properties of the NISSERVER object, an error message displays. What should I do?

The schema might not be fully extended. This occurs when the NetWare 6 server is attached to a NetWare 5.1 tree.

Check ETC\SCHINST.LOG to view whether the schema is extended.

Nfsadmin might not be running.

Make sure that NFSADMIN is running.

I am unable to migrate or create a domain using makenis? What do I need to do?

Make sure that ndsilib is running.

Check ETC\NIS.CFG to view whether the NisServer context and name are set properly.

I am unable to change the password from a UNIX machine for a migrated domain. What do I need to do?

Ensure that the NetWare server is set as the default NIS server of the UNIX system

Use the UNIX command yppasswd for setting the NIS user password. The NISSWDD.NLM must be loaded on the NetWare server.

What is the 0_*2* user object automatically created when installing in to two servers which are joined one NDS tree?

When an object is created on e-Directory replica 1 and before it replicates to all replica servers, another object with the same name is created from another replica, the name of one of the objects changes.

This ensures that the two objects have unique names. The name will be in the format *number_n.*

For example, the object name could be 0_2 or 0_3 with the NFAUUser appended as a suffix.

On viewing such objects, delete them.