Novell Open Enterprise Server

www.novell.com

FILE SYSTEMS MANAGEMENT GUIDE

November 1, 2005

Novell®

Legal Notices

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

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

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc., in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare Core Protocol and NCP are trademarks of Novell, Inc.
NetWare Loadable Module and NLM are trademarks of Novell, Inc.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Client is a trademark of Novell, Inc.
Novell Cluster Services is a trademark of Novell, Inc.
Novell Storage Services is a trademark of Novell, Inc.
SUSE is a registered trademark of Novell, Inc., in the United States and other countries.
Transaction Tracking System and TTS are trademarks of Novell, Inc.

Third-Party Materials

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

Contents

About This Guide

This document describes how to create directories and files and secure access to them on a Novell® Open Enterprise Server. It discusses file system management issues, such as file system trustees, trustee rights, inherited rights filters, and directory and file attributes for the Novell Storage Services™ (NSS) File System on Linux* and NetWare® and for the NetWare Traditional File System. For information about managing traditional Linux file systems and POSIX* access control lists, see the *SUSE Linux Enterprise Server 9 Administration Guide* (http://www.novell.com/documentation/oes/sles_admin/data/front.html).

This guide is divided into the following sections:

Audience

This guide is intended for network administrators and users.

Feedback

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

Documentation Updates

For the most recent version of the *Novell Open Enterprise Server File Systems Management Guide*, see the latest Novell Open Enterprise Server documentation (http://www.novell.com/documentation/oes)

Additional Documentation

- *Novell Storage Services File System Administration Guide for OES*
- *SUSE Linux Enterprise Server 9 Administration Guide* (http://www.novell.com/documentation/oes/sles_admin/data/front.html)

- *NetWare Traditional File System Administration Guide for OES*
- *Novell iManager 2.5 Administration Guide* (http://www.novell.com/documentation/imanager25/imanager_admin_25/data/hk42s9ot.html)
- *OES NetStorage Administration Guide for Linux* (http://www.novell.com/documentation/oes/netstor_lx/data/h9izvdye.html)
- *OES NetStorage Administration Guide for NetWare* (http://www.novell.com/documentation/oes/netstor/data/h9izvdye.html)
- *Novell Remote Manager Administration Guide for Linux for OES*
- *Novell Remote Manager for NetWare Administration Guide for OES*
- *NCP Server for Linux Administration Guide*
- "Managing File Security and Passwords" (http://www.novell.com/documentation/noclienu/noclienu/data/h9nmmvwn.html) in the *Novell Client for Windows Installation and Administration Guide* (http://www.novell.com/documentation/noclienu/noclienu/data/h4rudg93.html)
- "Assigning Rights to Volumes, Files, and Directories" (http://www.novell.com/documentation/linux_client/linuxclientuser/data/bwfnnvo.html) in the *Novell Client 1.0 for Linux User Guide* (http://www.novell.com/documentation/linux_client/linuxclientuser/data/bwfuc85.html)

Documentation Conventions

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

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

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

File Systems Overview

1

This section introduces the file systems supported in Novell® Open Enterprise Server.

1.1 Novell Storage Services File System

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

NSS volumes are cross compatible between kernels. You can mount a non-encrypted NSS data volume on either kernel—Linux or NetWare—and move it between them. For information, see “Compatibility Issues for Using NSS Cross-Platform”in the *Novell Storage Services File System Administration Guide for OES*.

In a clustered SAN, NSS volumes can fail over between kernels, allowing for full data and file system feature preservation when migrating data to Linux. However, you cannot SAN boot cross-platform. For information, see the *OES Novell Cluster Services 1.8.2 Administration Guide for Linux*.

You can manage all storage management functions in the Web-based Novell iManager utility and NSS Management utility. NSS also supports third-party tools on both kernels for advanced data protection and management, virus scanning, and traditional archive and backup solutions.

For information, see the *Novell Storage Services File System Administration Guide for OES*

1.2 Linux Traditional File Systems

The OES Linux kernel supports a variety of Linux traditional file systems. It requires a Linux traditional file system for its system volume. The upper level of the kernel deals equally with these file systems through an abstract layer, the virtual file system (VFS). Some typical Linux traditional file systems are described in the following table:

Linux Traditional File System	Description
Second Extended File System (EXT2)	EXT2 is a legacy file system with a solid reputation. It uses less memory than other options and is sometimes faster. EXT2 does not maintain a journal so it is not desirable to use it for any server that needs high availability.

Linux Traditional File System	Description
Third Extended File System (EXT3)	EXT3 is a journaling file system that has the same data format and metadata format with its predecessor, EXT2. You can move from EXT2 to EXT3, and vice versa, without rebuilding your file system. It also offers options to coordinate its metadata journaling with data writes.
Reiser File System (ReiserFS)	ReiserFS supports metadata journaling, but does not include data journaling or ordered writes. Its disk space utilization, disk access performance, and crash recovery are better than EXT2.
Journaled File System (JFS)	JFS was developed by IBM* to support high throughput server environments where performance is the ultimate goal. Because it is a full 64-bit file system, JFS supports both large files and partitions. It supports group commit of log entries for multiple concurrent operations, which improves journaling performance. It supports different directory organization for small and large directories and uses space efficiently.
Extended File System (XFS)	XFS is a high-performance 64-bit journaling file system. It is good at manipulating large files and performs well on high-end hardware. XFS takes great care of metadata integrity. It supports independent allocation groups that can be addressed concurrently by the system kernel, which suits the needs of multiprocessor systems. It preallocates free space on the device to reduce file system fragmentation. However, delayed writes can result in data loss if the system crashes.

For information, see "File Systems in Linux" (http://www.novell.com/documentation/oes/sles_admin/data/cha-filesystems.html) in the *SUSE Linux Enterprise Server 9 Administration Guide* (http://www.novell.com/documentation/oes/sles_admin/data/front.html).

1.3 NetWare Traditional File System

The NetWare Traditional (Traditional) File System provides legacy storage and file system management for Novell Open Enterprise Server NetWare.

You can optionally use NetWare Traditional volumes in combination with NSS volumes on NetWare when you are using the NCP protocol. However, if you are planning to implement Apple* File Protocol (AFP), Network File System (NFS), or Common Internet File System (CIFS) for your NetWare server, you must use NSS for your system volume and for any data volumes that use any protocols other than NCP. For information, see the *OES Native File Access Protocols Guide*.

For information, see the *NetWare Traditional File System Administration Guide for OES*.

1.4 What's Next

Continue with Chapter 2, "Coexistence and Migration Issues," on page 13.

Coexistence and Migration Issues

2

This section discusses the issues involved in the coexistence and migration of file systems in Novell® Open Enterprise Server.

2.1 Comparison of NSS to Other File Systems in OES

The following table lists sections in the *Novell Storage Services File System Administration Guide for OES* that contain comparisons of the Novell Storage Services* File System to other file systems in OES:

Comparison	NSS on NetWare®	NSS on Linux	Linux Traditional File Systems	NetWare Traditional File System
“Comparison of NSS on NetWare and NSS on Linux”	X	X		
“Comparison of NSS for Linux and Linux Traditional File Systems”		X	X	
“Comparison of NSS on NetWare and the NetWare Traditional File System”	X			X

2.2 Compatibility Issues for File System Rights on Linux

This section discusses the following issues for controlling access to files on Linux:

2.2.1 Enforcing File System Rights on Linux

File and directory access rights are enforced on Linux systems in different ways, depending on the following:

- User identity, such as Novell eDirectory™ users or local-only users
- Access method, such as NCP™ Server, other protocols, or core Linux utilities.

  For information about core Linux utilities, see "Core Linux Utilities" on page 15.
- File system, such as NSS on Linux or traditional Linux file systems

Novell eDirectory Users

The following table describes how file system access rights are enforced on Linux systems for eDirectory users:

File System	Access via NCP Server for Linux	Access via Other Protocols (such as NFS or Samba)	Access via Core Linux Utilities
NSS on Linux	NCP enforces access. To preserve NetWare file ownership information when transferring NSS volumes cross-platform to Linux, eDirectory users must be Linux enabled. trustee rights are enforced regardless of file ownership. For security reasons, soft links are not supported by NCP Server. Soft links are not accessible from NCP clients; users cannot see or access them.	NSS enforces access.	NSS enforces access.
Traditional Linux	NCP enforces access. eDirectory users must be Linux-enabled to ensure support for all file systems features. For security reasons, soft links are not supported by NCP Server. Soft links are not accessible from NCP clients; users cannot see or access them.	Linux file systems enforce access. eDirectory users must be Linux-enabled to ensure support for all file systems features.	Linux file systems enforce access. eDirectory users must be Linux-enabled. Linux services need to be enabled for pluggable authentication modules (PAM) when you configure Linux User Management.

Local-Only Users

The following table describes how file system access rights are enforced on Linux systems for locally defined users:

File System	Access via NCP Server for Linux	Access via Other Protocols (such as NFS or Samba)	Access via Core Linux Utilities
NSS on Linux	Local users have no access to files via NCP.	Local users have no access to files via other protocols.	Access to NSS is restricted to the root user. Local users have no access to files on the NSS volume.
Traditional Linux	Local users have no access to files via NCP.	Local users have no access to files via other protocols.	Linux file systems enforce access.

Core Linux Utilities

Core Linux utilities are standard file services used to access files. They include the following:

- Shell login
- Samba server
- File transfer protocol (`ftp`)
- Secure shell (`ssh`)
- Substitute user (`su`), which opens runs a shell as root (or superuser)
- Remote shell (`rsh`)
- Remote login (`rlogin`)
- X display manager (`xdm`)
- Open Web-based enterprise management (`openwbem`)

2.2.2 Assigning File System Rights on Linux

The following table identifies the management tools to use to assign Novell trustee-based file system rights on Linux.

IMPORTANT: Only eDirectory users are eligible for file-system trustee rights. On Linux, the eDirectory users must also be Linux-enabled using Linux User Management.

Management Tool	NSS File System on Linux			Traditional Linux File Systems		
	NCP	NFS or Samba	Core Linux Utilities	NCP	NFS or Samba	Core Linux Utilities
NSS `rights` utility	Yes	Yes	Yes	Yes	Not applicable	Not applicable

Management Tool	NSS File System on Linux			Traditional Linux File Systems		
	NCP	NFS or Samba	Core Linux Utilities	NCP	NFS or Samba	Core Linux Utilities
Novell NetStorage	Yes	Yes	Yes, for NetStorage with SSH support	Not supported by NetStorage	Not applicable	Not applicable
Novell Client™ for Windows 2000/XP/2003	Yes	Not applicable	Not applicable	Yes	Not applicable	Not applicable
Novell Client for Linux	Yes	Not applicable	Not applicable	Yes	Not applicable	Not applicable
ConsoleOne®	Yes	No	No	Yes	Not applicable	Not applicable

2.2.3 Key Considerations

If you use core Linux utilities—with, or instead of, NCP Server for Linux—to control file access for eDirectory users on Linux:

- Make sure the core Linux utilities are PAM-enabled during Linux User Management (LUM) configuration.
- eDirectory users must be Linux-enabled to use the core Linux utilities. A Linux-enabled user is defined as a local user and as an eDirectory user. (Linux-enabled is also referred to as LUM-enabled.)

Although NCP and NSS keep file system rights information separately, the information should always be in sync.

2.3 NCP Server Directory and File-System Trustee Rights and Attributes

NCP Server for Linux provides the same file-system trustee rights for both NSS and traditional Linux file systems. These are the same rights that exist for NSS and NetWare Traditional file systems on NetWare. The trustee rights include:

- Read
- Write
- Create
- Erase
- Modify
- File Scan
- Access Control
- Supervisor

For information, see Section 6.2, “File-System Trustee Rights,” on page 40.

For the initial release of OES Linux, NCP Server supports only the following file and directory attributes for both NSS and Linux traditional file systems on Linux:

- Read Only
- Hidden

Other NSS file and directory attributes were not supported on OES Linux traditional file systems.

Beginning with OES SP1 Linux, NCP Server supports all NSS file system attributes. For information about attributes, see Section 6.6, "Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes," on page 47.

NCP volumes created on traditional Linux file systems (such as ReiserFS, JFS, EXT3) support only the Read Only, Hidden, and Shareable attributes.

2.4 Acquiring eDirectory Security Equivalence Vectors for NSS Users

The Security Equivalence Vector (SEV) is calculated for each NSS user based on information in the user's profile in Novell eDirectory. NSS validates the user's SEV against the trustee rights of the directory and file the user is attempting to access. In OES, SEVs are acquired differently for NSS on NetWare and NSS on Linux.

For NSS on NetWare, whenever a user connects to the NSS file system, NetWare retrieves the user's SEV from eDirectory and maintains it as part of the connection structure for the user's session. NSS automatically retrieves the user's SEV from the connection structure.

For NSS on Linux, whenever a user first connects to the NSS file system after reboot, NSS caches the SEV locally in the server memory, where it remains until the server is rebooted or unless the user is deleted from eDirectory. NSS polls eDirectory at a specified interval for updates to the SEVs that are in cache. Command line switches are available in the NSS Console utility (`nsscon`) to enable or disable the update, to set the update interval (5 minutes to 90 days), and to force an immediate update of security equivalence vectors. For information, see "Security Equivalence Vector Update Commands (Linux)" in the *Novell Storage Services File System Administration Guide for OES*.

2.5 Security Guidelines

To install applications on your NSS or NetWare Traditional file system, you must be logged in as a trustee with the Create right of the directory where you will be installing the application. The Supervisor user of the server automatically has the Create right.

2.6 Migrating NetWare Traditional Volumes to Linux

For the initial release of OES Linux, you can migrate a NetWare Traditional File System volume from your NetWare server to a Linux server by first upgrading it to an NSS volume on OES NetWare, then moving the volume cross-platform to OES Linux. However, for OES SP1 and later, NSS volumes on NetWare have a format that is not supported cross-platform. For information, see "Upgrading the Media Format for OES SP1 NetWare and NetWare 6.5 SP4" in the *Novell Storage Services File System Administration Guide for OES*.

To upgrade Traditional volumes for your OES NetWare server, see "Upgrading Legacy NSS Volumes and NetWare Traditional Volumes to NSS on NetWare Volumes" in the *Novell Storage Services File System Administration Guide for OES*.

For information about using NSS volumes cross-platform, see the following topics in the *Novell Storage Services File System Administration Guide for OES*:

- "Compatibility Issues for Using NSS Cross-Platform"
- "Moving Non-Clustered Devices From NetWare 6.5 or OES NetWare to OES Linux"
- "Moving Clustered Devices with NSS Volumes Cross-Platform"

3 Understanding NetWare Directory Structures

This section describes the following key concepts for the Novell® Storage Services™ (NSS) File System and the legacy NetWare® Traditional (Traditional) File System for Novell Open Enterprise Server NetWare:

3.1 Directory Structures

The NSS and Traditional file systems provide a uniform method of referring to directories and files and locating them on a variety of storage media. As with your office filing system, you must impose organization on data you store in a volume. Within each volume, you can group information in logical containers called folders or directories.

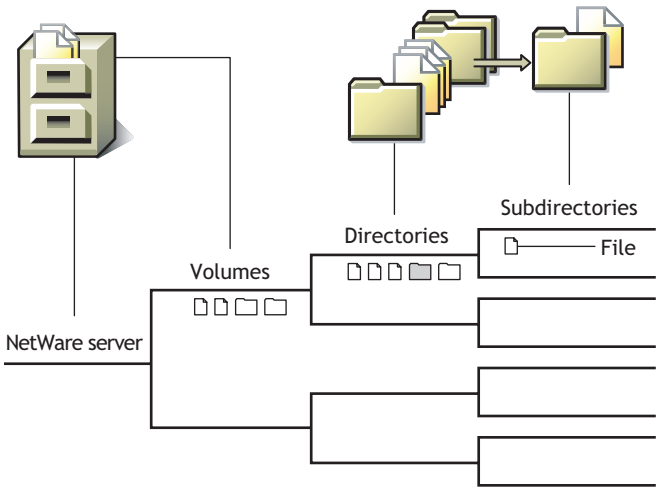
A directory is a logical separation within a volume where you store files and subordinate directories, called subdirectories. The directory is a special type of file that contains a list of its files and subdirectories. It can also contain metadata about the directory, such as who can access it and its attributes. For NetWare Traditional, the directory’s metadata is stored in a Directory Entry Table (DET), separate from the directory itself.

A file is the basic logical container for storing information, such as an image, a document, a program, text, or a database.

Within each volume, the directory structure is hierarchical. It is an inverted tree structure with a single root. The topmost directory in the hierarchy is called the root directory. A directory is called the parent directory of the subdirectories and files in it. A volume can contain any number of directories. A directory can contain any number of files and subdirectories.

The following figure illustrates how volumes are similar to drawers in an office filing cabinet that contain related information. For example, the `sys:` volume on NetWare contains the operating system and its extensions. Other volumes might contain applications, corporate data, or user home directories and files.

Figure 3-1 *Sample Directory Structure for NSS and Traditional File Systems on a NetWare Server*



There is no one best solution for organizing files with directories. You can use a combination of approaches, such as by geographic location, applications, business units, projects, or owners. For information, see "Planning Directory Structures for NetWare" on page 25.

To control who can access directories and files on your NSS and Traditional NetWare file systems, you must assign file system trustees, trustee rights, and inherited rights filters. For information, see Section 6.2, "File-System Trustee Rights," on page 40.

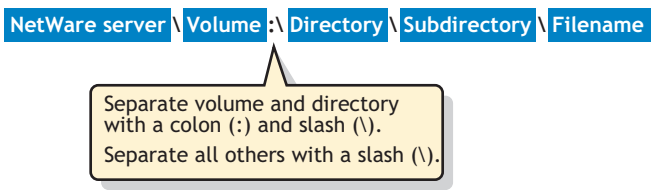
To control how authenticated users can use directories and files, you must set directory and file attributes. For information, see:

- Section 6.6, "Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes," on page 47
- Section 6.7, "Displaying Key NSS Directory and File Attributes as Linux POSIX Permissions," on page 48

3.2 Directory Path

A directory or file is located by its *path*, which states where the directory or file is logically located in a volume. A path includes the volume, directory, and any subdirectories leading to the file. The following figure shows how to specify a full path. Listing the server is optional. It is usually excluded when specifying a path relative to the server where you are logged in. The slash after the colon is required in some interfaces and optional in others. Refer to the interface's documentation to determine if a colon and slash combination (`:\`) is required to separate a volume and directory.

Figure 3-2 *Directory Path Conventions*



If your network uses multiple server or client operating systems or multiple file systems, keep in mind the conventions of the different file systems, such as delimiters, path length, and case

sensitivity. For example, the NSS and Traditional file systems on NetWare use backslashes as delimiters and are case insensitive, while file systems native to Linux and UNIX use forward slashes and are case sensitive. As another example, NetWare allows 255 characters in a directory path (counting the drive letter and delimiters), but DOS allows only 127 characters. For more information, check the application's documentation.

3.3 Root Directory

The root directory is the base directory in the volume. The root directory of a volume typically contains only directories.

Storing files at this level is possible, but it can be a security risk. Granting file-system trustee rights to files at the root of the volume necessitates granting rights to the entire volume. For information about trustee rights, see "Understanding File System Access Control for NSS and NetWare Traditional File Systems" on page 39.

To avoid this security risk, create Fake Roots for applications that want to write files to the root directory. For information, see Section 3.4, "Fake Root Directory," on page 21.

3.4 Fake Root Directory

A fake root is a directory in a volume that functions as a root directory for a specific software application.

Some applications require their executable files to be located in a root directory. However, for security, you should not grant users rights to files at the root of the volume.

NetWare allows you to map a directory as drive that serves as a fake root directory, using the `map root` command. This allows you to install an application in a directory and assign rights for it at that directory level. For information, see Section 5.4, "Creating a Fake Root Directory with the Map Root Command," on page 33.

Fake roots work with the NetWare DOS Requester, with NetWare shells, and with clients, including Windows* 98/ME and Windows 2000/XP/2003. Fake roots do not work for IBM* OS/2* clients. (Under OS/2, all mapped drives are roots, and search drives do not exist.)

For Windows NT*/2000/XP workstations that use Novell Client™ login scripts, a `map` command in the login script automatically enables a mapped NetWare subdirectory as a fake root directory. For information about disabling this behavior, see Section 5.5, "Disabling the Default Use of Map as Map Root in Login Scripts," on page 33.

3.5 Directory Map Objects

In Novell eDirectory™, the Directory Map object is a pointer to a path in the NetWare server file system that represents a particular directory in the file system. It allows you to make simpler references to directories by using a Directory Map object in your login scripts instead of the fixed path. Directory Map objects are available only for NetWare NSS and Traditional volumes.

For instructions, see Section 5.6, "Creating and Configuring a Directory Map Object," on page 34.

Using a Directory Map Object

Directory Map objects can be especially useful in Novell Client login scripts to point to directories that contain applications or other frequently used files. In Novell Client login scripts, you can map a drive to a Directory Map object instead of to the directory. If the application's location in the directory structure changes, you can update the path in the Directory Map object instead of changing the related drive maps in numerous login scripts. For information about `map` command options, see "Login Script Commands and Variables" (http://www.novell.com/documentation/linux_client/login/data/ak1lxuu.html) in the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).

For example, suppose a word processing application resides in a directory called `appsvol:wpapps\oo10`. You map a network-search drive to that directory in login scripts you create for users.

Later, you upgrade the word processing application and rename its directory from `appsvol:wpapps\oo10 to appsvol:wpapps\oo11`. You must modify the path in the network drive map in every login script where that network-search map appears.

If you map the directory path to a Directory Map object instead of a network-search drive, you can avoid tedious modifications of the login scripts. Use the eDirectory plug-in for Novell iManager to create a Directory Map object. For example, create a Directory Map object called *`default_wpapp`*, for `appsvol:wpapps\oo11`. Place a `map` command in your login scripts that map a search drive to the Directory Map object, rather than to the specific directory. For example:

```
map ins s2:=.default_wpapp.dept.domain_us
```

When users log in, their network-search drive is mapped to the `default_wpapp` Directory Map object, which, in turn, points to `appsvol:wpapps\oo11`.

Later, if you install a yet another default word processor and change the directory's name to *`appsvol:wpapps\superwp`*, you need to change only the directory path in the `default_wpapp` Directory Map object. You do not need to change the `map` command in the login script because the `map` command still indicates the correct Directory Map object.

Additional Information

For information, see "Object Classes and Properties" (http://www.novell.com/documentation/edir873/edir873/data/fbabihje.html) in the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a2iii88.html).

3.6 Drive Map

A drive map is a pointer to a location in your local or network file system. The map assigns a local drive letter to a directory path on a volume where you have access rights. The directory path includes the volume, directory, and any subdirectories leading to the file. The local drive letter can be used instead of the complete path name.

Drive maps can be permanent or temporary:

- **Permanent Map:** To map a drive so you can use it every time you log in, place a `map` command in your Novell Client login script, or use the mapping functionality of your client

operating system and enable it to reconnect at login. The network drive is remapped every time you log in.

- **Temporary Map:** To map a drive so you can use it only during your current session, use the *Novell Map Network Drive* option in the Novell Client, use the NetWare `map` command from a system prompt, or use the mapping functionality of your client operating system. The network drive map is valid only until you log out.

NetWare recognizes three types of drive mappings:

- Local Drive Maps
- Network Drive Maps
- Network-Search Drive Maps

For information about how to use the NetWare `map` command, see the following:

- "Map" (http://www.novell.com/documentation/oes/utlrfenu/data/h7onc376.html) in the *Utilities Reference for OES*
- "Login Script Commands and Variables" (http://www.novell.com/documentation/linux_client/login/data/ak1lxuu.html) in the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html)

3.6.1 Local Drive Maps

You create local drive maps to establish directory paths to local storage media such as your workstation disk drives, CD drives, Zip* drives, USB drives, and floppy disk drives.

Typically, the `lastdrive` command in your DOS configuration settings is set to end with drive `E:` (`lastdrive=e`), or with the last drive specification in use on your system. Typically, drives `C:` through `E:` are used for local drives, but you can assign more drive letters, if needed, by modifying the `lastdrive` command.

To change this default, use a text editor to add or modify the DOS `lastdrive` command in your workstation `config.sys` file. For example:

```
lastdrive=Z
```

3.6.2 Network Drive Maps

Network drive maps point to volumes and directories on the network where you have access rights. Typically, drives `F:` through `Z:` are used for network drive maps. Each user can map drive letters to different directories.

3.6.3 Network-Search Drive Maps

Network-search drive maps point to directories that contain frequently used files such as applications files. This map enables the system to locate an application file even if it is not located in the directory where you are working.

Network-search drive maps are numbered, although they also have drive letters. For example, a network-search drive `1` (or `s1`) can also be known as network drive `Z:`.

You can map up to 16 network-search drives, beginning with drive letter `Z:` (`s1`) and moving backwards through the alphabet to `K:` (`s16`). You cannot map a network-search drive and a regular network drive to the same drive letter.

If you request a file that the system cannot find in your current directory, the system looks in every directory where a network-search drive is mapped. The system searches, following the numerical order of the search drives, until the program file is found or cannot be located.

Network-search drive maps are not supported on IBM OS/2 workstations. The search functionality is provided with the OS/2 `path`, `libpath`, and `dpath` commands in the `config.sys` file.

4 Planning Directory Structures for NetWare

This section presents a simple example of directory structures to help you organize data in the Novell® Storage Services™ (NSS) File System and the legacy NetWare® Traditional (Traditional) File System for Novell Open Enterprise Server NetWare. Based on the example and the accompanying information, you can begin to design a directory hierarchy suitable to your own needs.

IMPORTANT: For file systems on NetWare, we recommend that you create separate volumes for applications and user data, reserving the `sys:` volume for the operating system and its extensions.

4.1 Organizing Directory Structures Based on Access Requirements

Security is one of the most important aspects of file system organization. File system trustees and trustee rights specify who can access different directories and files. File system directory and file attributes specify what authenticated users can do with the file, such as being able to merely read a file or to modify it.

Organizing the Directory Structure

Organize directories and files according to who needs access to them. In other words, use the directory structure to reflect access requirements.

For example, you can structure the hierarchy of directories in such a way as to take advantage of the inheritance aspect of rights. Associate file system trustees and trustee rights with volumes, directories, and files as a safeguard against deletion or modification by users. Specify directory and file attributes to control what users can do.

Grouping the User Community

Group the user community based on each user's access requirements.

Users grouped by role (relative to file access) can be assigned ownership of directories and files, and users whose roles vary can be assigned rights on the basis of equivalence.

Users needing a particular kind of access to certain directories and files can be grouped so that appropriate access belongs to the group (and consequently, to each member).

4.2 Managing Directory Structures for Network Applications

You can install various types of network applications, such as word processing or spreadsheet programs, to make them available to users. When installing applications, keep the following in mind:

- To install applications on your NSS or Traditional file system, you must be a Trustee with the Create right for the directory where you will be installing the application. The Supervisor user of the server automatically has this file-system trustee right.
- Follow the instructions in the application's documentation for installing the application onto a network. Make sure the application is designed for network (multiuser) use.
- When creating application directories, consider issues related to ease of distribution, installation, and operational control for network applications.
- If the application requires that it be installed at the root of a volume, but you would rather install it in a subdirectory for security reasons, you can map the directory to a fake root.

  For information, see Section 3.4, "Fake Root Directory," on page 21.
- After you install the application:
  - Designate Novell eDirectory organization, role, and user objects as file system Trustees for the application directory and its contents.
  - Assign access rights for each trustee.
  - Configure attributes for the directory and its files.

  For information, see "Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes" on page 53.
- To allow users to access network-based applications, map search drives to the directories that contain these applications. For information, see "Network-Search Drive Maps" on page 23.

  To make the mapped search drives permanent, place them in login scripts, which are executed when users log in. For information, see the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).
- You can create a Directory Map object that points to an application directory.

  Directory Map objects are useful in login scripts. Instead of mapping a drive to a specific directory path, you map a drive to a Directory Map object that points to a directory.

  If you change the directory path, you need to change only the Directory Map object's definition.
- If you install the application in the `sys:\public` directory, it is not necessary to make file system Trustee assignments or map a search drive. Because users generally have Read and File Scan rights in `sys:\public`, users can see and use all applications installed there. Use this directory structure only if you want all users to have access to all applications.

4.3 Designing Application Directory Structures

Application directories are storage areas where you install applications for convenient network access by groups, users, and other applications. You can install a variety of network applications, such as word processing or spreadsheet programs, and make them available to users.

For ease of management, create a separate volume for your applications and store applications in different directories. Mixing NetWare utilities with application program files complicates the file structure when you upgrade a network. An application file might have the same filename as a NetWare utility file or another application's program file. If filenames are the same, one file overwrites the other because two files with the same filename cannot coexist in a directory.

Keep program files separate from data files to simplify application management. For example, program files seldom change, but user data changes frequently. By creating a separate application volume and data volume, you can back up program files separately from a data files. Frequent network backup can then focus only on data directories, with application volumes being backed up as needed. Creating data directories for shared data files allows single-point backup and management of shared files.

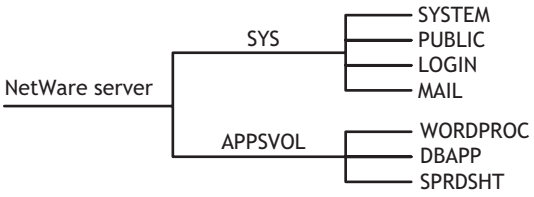
This section describes the following examples of application directory structures:

- Application Volume with Separate Application Directories Off Its Root
- Sys: Volume with a Parent Application Directory Off Its Root
- Sys: Volume with Separate Application Directories Off Its Root
- Sys:public Directory with a Parent Application Directory

4.3.1 Application Volume with Separate Application Directories Off Its Root

Create a separate volume for applications. Create a separate directory for each application off the root of the application volume, as shown in the following example.

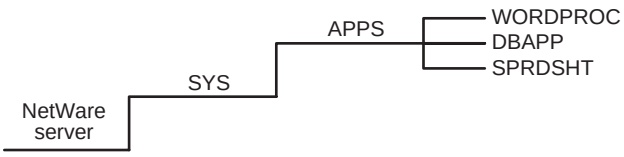
Figure 4-1 *Application Volume with Separate Application Directories Off Its Root*



4.3.2 Sys: Volume with a Parent Application Directory Off Its Root

In the `sys:` volume, create a parent application directory at the root. Create a separate directory for each application in the parent application directory, as shown in the following example.

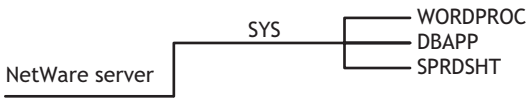
Figure 4-2 *Sys: Volume with a Parent Application Directory Off Its Root*



4.3.3 Sys: Volume with Separate Application Directories Off Its Root

In the `sys:` volume, create a separate directory for each application at the root of the volume, as shown in the following example.

Figure 4-3 *Sys: Volume with Separate Application Directories Off Its Root*

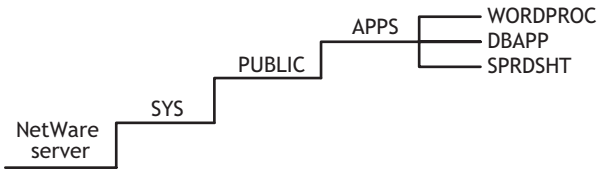


4.3.4 Sys:public Directory with a Parent Application Directory

Because users generally have Read and File Scan rights in `sys:\public`, users can see and use all applications installed in it. Use this directory structure only if you want all users to have access to all applications.

We do not recommend installing applications in the `sys:\public` directory. If you decide to use the `sys:\public` directory, create a parent directory for applications in `sys:\public`, as shown in the following example.

Figure 4-4 *Sys:public Directory with a Parent Application Directory*



4.4 Designing Data Directory Structures

Data directories are storage areas where groups and users store work files and databases. Data directories allow users to share data, create work directories, and make Trustee assignments for groups or users who need access to these directories. You can also create a directory to transfer files between directories on the network.

For ease of management, create a separate volume for your data and store different types of data in different directories.

4.5 Designing Home or User Directory Structures

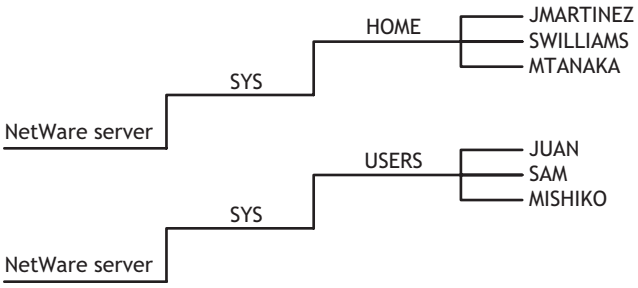
To provide personal workspace for users, create a separate home or user volume and create a subdirectory in it for each user. You can also create parent directories for groups of user directories. The data files a home or user directory contains are not available to other users, except network administrators or managers who have the necessary access rights.

For ease of management, create a separate volume for your home or user directories.

If you decide to use the `sys:` volume, create a parent directory in volume `sys:`, such as home or users. Within the parent directory, the name of each subdirectory should be the username.

Usernames can be up to 47 characters, but DOS displays only 8 characters in a one-level directory name.

Figure 4-5 *Home or User Directory Structure*



5 Configuring Directories for NetWare and NSS on Linux

This section discusses how to configure directories in the Novell® Storage Services™ (NSS) File System for Linux and NetWare® and the legacy NetWare Traditional (Traditional) File System.

5.1 Creating a Directory

You can create directories locally using the NetWare GUI console, and remotely using the following management tools:

Management Tool	NSS on Linux	NSS on NetWare	NetWare Traditional File System
Novell NetStorage	Yes	Yes	No NetStorage does not support Traditional volumes.
Novell Client™ for Windows 2000/XP	Yes	Yes	Yes
Novell Client for Linux	Yes	Yes	Yes
Novell Remote Manager for Linux	No	No	No
Novell Remote Manager for NetWare	No	Yes	Yes

To create a directory, you must have the Create right for the directory that you want to add the new directory to. When creating a root directory, select the Volume object instead of selecting a parent directory.

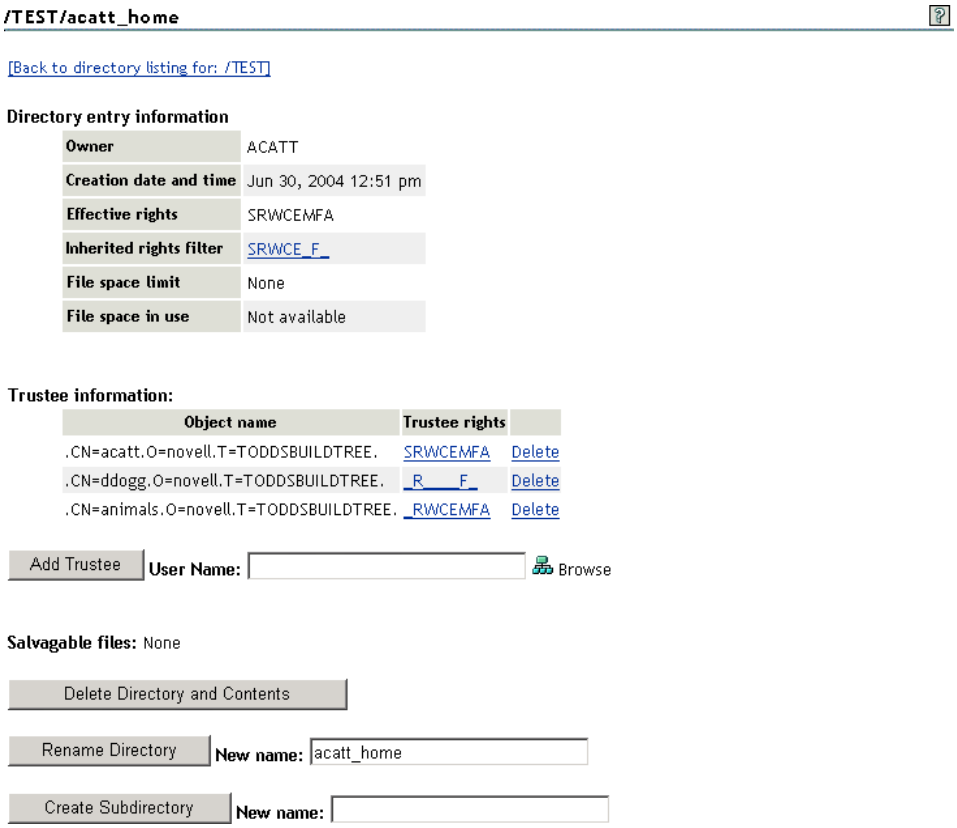
1. In your Web browser, log in to Novell Remote Manager on the NetWare server where you want to create a directory in an NSS volume. The general form of the URL is

   `http://192.168.1.1:8008`

   `https://192.168.1.1:8009`

   Replace *`192.168.1.1`* with the actual IP address or DNS name of your server.
2. Click *Manage Server* > *Volumes*.

3 Click the *Properties* icon next to the volume you want to manage.



4 Type the name of the subdirectory, then click *Create Subdirectory*.

5.2 Viewing Directory and File Information

You can see extended information about a directory or file with Novell NetStorage, Novell Remote Manager, and the Novell Client.

You can view directory information such as

- Owner and trustees
- Creation date and time
- Attributes, effective rights, and the IRF
- Disk space limitations

You can view file information such as

- Owner and trustees
- Attributes, effective rights, and the Inherited Rights and Filters (IRF)
- Name space
- File size
- Creation, access, archive, and modify dates

For information, see "Understanding File System Access Control for NSS and NetWare Traditional File Systems" on page 39.

5.3 Copying or Moving Directories and Files

You can copy or move a directory's subdirectories and files, if you have the necessary rights to do so. You cannot move the location of the directory itself, unless you also have the necessary rights for the parent directory of the target directory and for the destination directory.

To copy or move a directory's subdirectories and files, you must have File Scan rights to the source directory, and you must have the Create right to the destination directory.

To move a directory's subdirectories and files, you must also have the Erase right to the source directory, because moving files includes deleting them from the source directory. For instructions, see "Viewing Details about Files and Performing Actions on Them" in the *Novell Remote Manager for NetWare Administration Guide for OES*.

5.4 Creating a Fake Root Directory with the Map Root Command

If your application must be installed at the root, load the files in a directory, then use the `map root` command in the login script to designate the directory as a fake root directory. For information about using the `map` command in a login script, see "Login Script Commands and Variables" (http://www.novell.com/documentation/linux_client/login/data/ak1lxuu.html) in the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).

For example, suppose you want to install a word processing application, named *mywpapp*, on the `apps:` volume, and it requires a root directory installation. You do not want to put the application in the `apps:` volume's root directory for security reasons. Instead, you install the application in the *`apps:wpapps\mywpapp`* subdirectory. In the Novell Client login script for users of the application, you use the `map root` command to map the subdirectory to the `K:` drive as a fake root:

```
map root s16:=k:=apps:wpapps\mywpapp
```

To change the fake root back to the original root, remap the drive.

NOTE: You cannot use the DOS Change Directory (`cd`) command at the fake root to return to the original root.

5.5 Disabling the Default Use of Map as Map Root in Login Scripts

For Windows NT/2000/XP/2003 workstations that use Novell Client login scripts, a `map` command in the login script has the same effect as using an explicit `map root` command. It automatically enables a mapped NetWare subdirectory as a fake root directory. Applications installed in the subdirectory serving as the fake root cannot access directories above that subdirectory.

If necessary, you can disable the `map` command's automatic Map Root behavior on Windows by adding `SET MAPROOTOFF="1"` as the first line in the login script. To create a fake root when the `MapRootOff` parameter is enabled, the login script must explicitly use the `map root` command.

For more information, see the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).

5.6 Creating and Configuring a Directory Map Object

1 In your Web browser, log in to Novell iManager, then select the NetWare server where you want to create the Directory Map object. The general form of the URL is

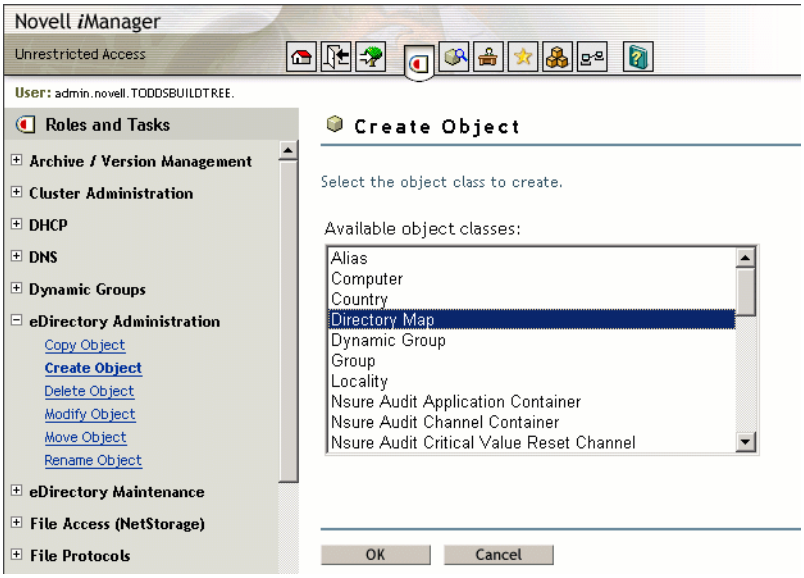
`https://192.168.1.1/nps/iManager.html`

Replace `192.168.1.1` with the actual IP address or DNS name of your iManager server.

The NetWare server must contain a NetWare NSS or Traditional volume.

To provide access from your tree to NetWare file systems in other trees, you can create NetWare Server and Volume objects in your tree that point to the NetWare servers and volumes in the other trees. The NetWare Server objects must be created before the Volume or Directory Map objects.

2 In *Roles and Tasks*, click *eDirectory Administration* > *Create Object* to open the Create Object page.



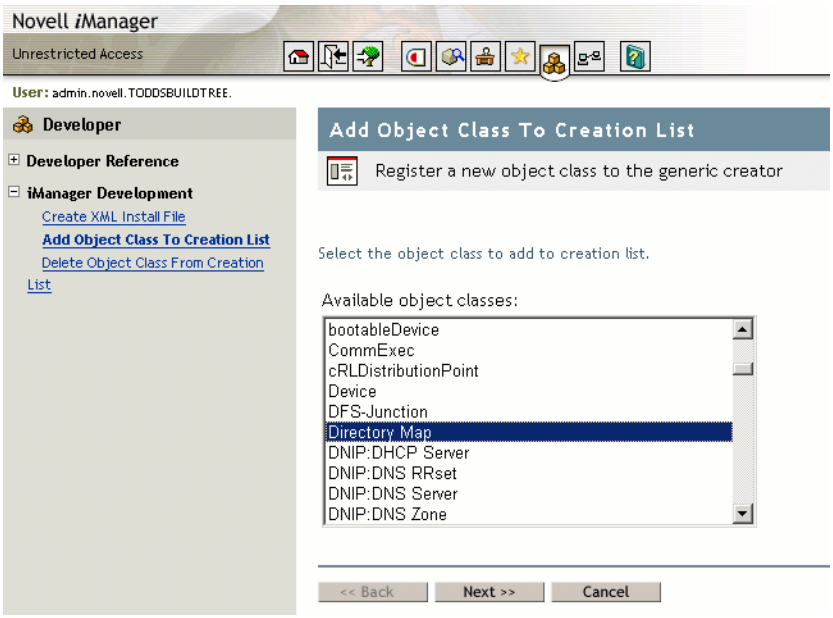
3 (Conditional) If Directory Map is not one of the Available Object Classes, you must add the Directory Map object class to the list.

When you select the *Create Object* task, it presents a list of available object classes. By default, it lists only the most commonly-used object classes in the list. You can add additional object classes to the list, which enables you to create corresponding objects using the *Create Object* option.

IMPORTANT: Role-Based Services must be configured before you can use the iManager Development role. For information, see "Setting Up Role-Based Services" (http://www.novell.com/documentation/imanager20/imanager20/data/bob1yft.html#bob1yft) in the *Novell iManager 2.5 Administration Guide* (http://www.novell.com/documentation/imanager25/imanager_admin_25/data/hk42s9ot.html).

3a In iManager, click the *Developer* icon.

3b Click *iManager Development* > *Add Object Class To Creation List*.



3c Select *Directory Map* from the *Available Object Classes* list, then click *Next*.

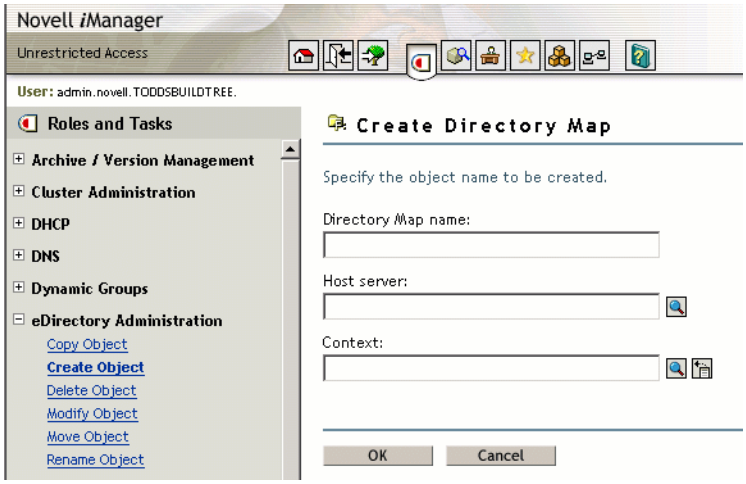
3d At the summary page, verify that the value of the *class-name* entry is `com.novell.emframe.fw.GenericCreator`, click *Finish*, then click *OK*.

3e Return to the Create Object task by clicking the *Roles and Tasks* icon, then clicking *eDirectory Administration* > *Create Object*.

3f Verify that the object classes you added are in the list of available object classes.

In case of errors during this process, the Web server might need to be restarted in order for the newly added object type to be available in the *Create Object* task.

4 In the *Available Object Classes* list, select *Directory Map*, then click *OK*.

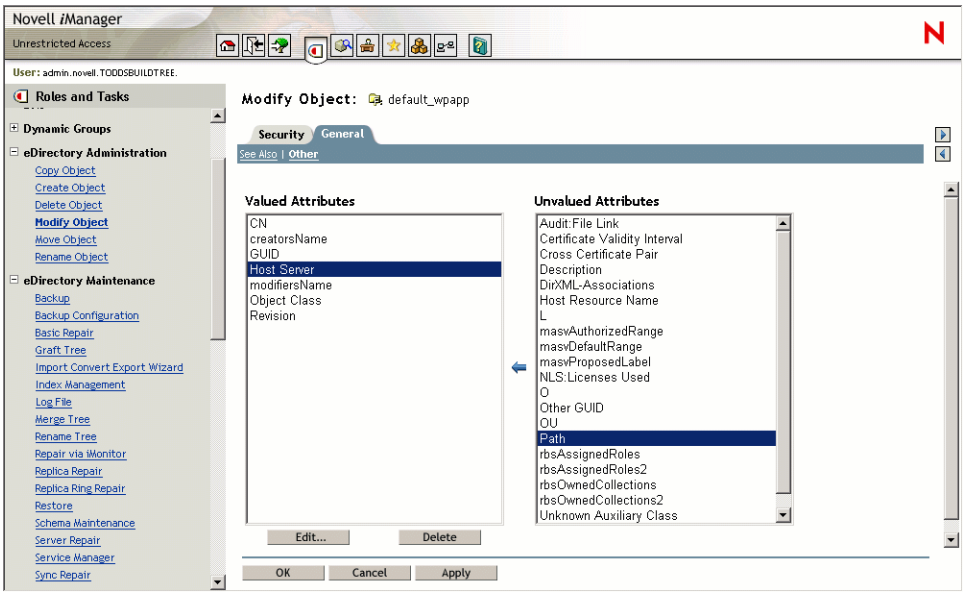


5 Specify the following information for the *Directory Map* object, then click *OK*.

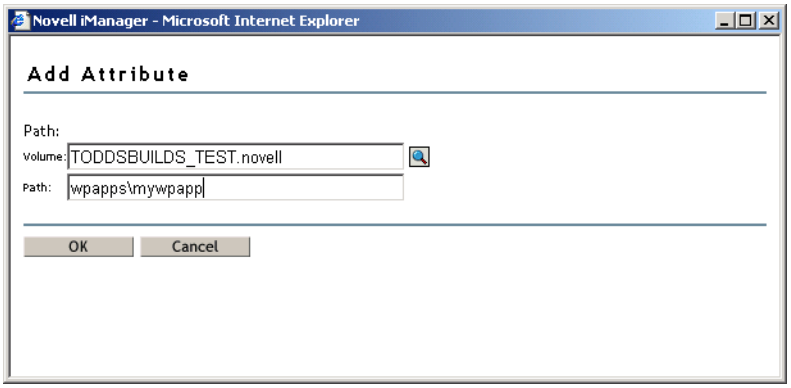
- **Directory Map Name:** Type the common name that represents this Directory Map object for use in `map` and `map root` commands.
- **Host Server:** Select the NetWare 6.5 or later server where the directory resides.

- **Context:** Select the context of the directory you plan to specify as the path this object represents.

6 Click *Modify* > *General* > *Other* to open the Modify Object page to the Directory Map's Attributes information.



7 In the *Unvalued Attributes* list, select *Path*, then click the *left-arrow* to add the attribute.



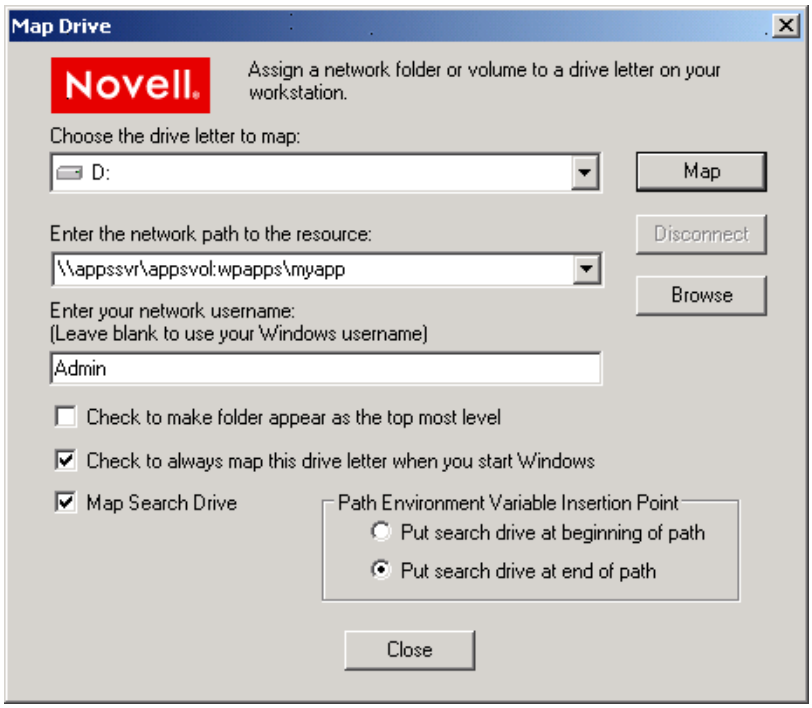
8 Specify the volume and path for the Directory Map object that the object represents, then click *OK*.

Novell iManager creates the Directory Map object with the specified volume and path, whether or not the specified path actually exists.

9 (Conditional) If the path you specified for the Directory Map object does not exist on the NetWare 6.5 or later server, create the specified path.

5.7 Mapping Network Drives

1 In the taskbar of your workstation, right-click the Novell Client icon, then select Novell Map Network Drive.



2 Specify a drive letter to map.

3 Type or browse to the path to the network resource where you want to map a drive.

4 Specify the login name to use for the map.

If none is provided, the client uses your Windows logon username. If necessary, the client later prompts you for the password that matches the server login username you provide.

5 (Optional) Select (enable) the *Check to Make Folder Appear as the Top-Most Level* option.

6 (Optional) Select (enable) the *Check to Always Map This Drive Letter When You Start Windows* option.

7 (Optional) Select (enable) the *Map Search Drive* option.

8 Under *Path Environment Variable Insertion Point*, specify whether to put the search drive at the beginning or end of the path.

9 Click *Map*.

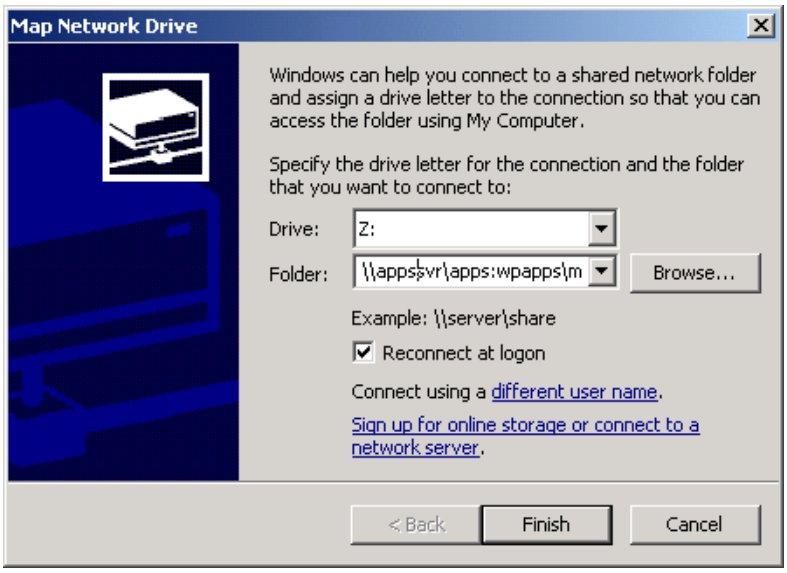
For more information, see the following:

- "Mapping Network Directories" (http://www.novell.com/documentation/linux_client/linuxclientuser/data/bvqayfv.html) in the *Novell Client 1.0 for Linux User Guide* (http://www.novell.com/documentation/linux_client/linuxclientuser/data/bwfuc85.html)
- *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).

Mapping Network Drives with Windows Explorer

You can also use native methods for mapping drives on your Windows client.

1. In Windows Explorer browser, click *Tools* > *Map Network Drive*.



2. Specify a drive letter to map.
3. Type or browse to specify the folder you want to map.
4. (Optional) To make the map automatically recur for subsequent logins to the network, select *Reconnect at Logon*.
5. Click *Finish*.

Mapping Network Drives on DOS Clients with the Map Command

You can also use native methods for mapping drives on your DOS client. Use the `map` command to map drives and search drives to network directories. For a general description of the `map` command, see "MAP" in the *Utilities Reference for OES*.

6 Understanding File System Access Control for NSS and NetWare Traditional File Systems

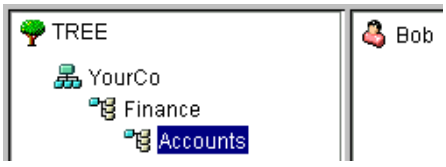
Security is one of the most important aspects of file system organization. The Novell® Storage Services™ File System and the NetWare® Traditional File System use the Novell trustee model to secure access to directories and files. Novell eDirectory™ objects, file-system trustee rights, and file system attributes for directories and files work together to allow you to determine who can access a directory or file and which actions are possible.

6.1 eDirectory Objects and Security Equivalence

In OES, administrators, users, and network resources are represented as objects in an eDirectory database. Use Novell iManager to create eDirectory objects, such as Organizational, Organizational Unit, Group, User, and Admin. For information, see the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a2iii88.html).

For example, in the following figure, The `TREE` container is configured and created when you install eDirectory. Later, you must populate the tree with container and leaf objects to represent the various resources in your company. `YourCo` is the main Organization (O) object in your TREE domain. In the `YourCo` container, you create `Finance` as an Organizational Unit (OU) object. In the `Finance` container, you create `Accounts` as an OU object that contains all accounting resources. Other OUs within `Finance` might represent Sales or Marketing organizations. In the `Accounts` container, `Bob` is a User object for a system user who is assigned to the Accounts Department.

Figure 6-1 *Example eDirectory Container and Objects*



Security equivalences help to simplify the task of assigning objects as file system trustees for your directories and files. Security equivalence is recorded in eDirectory as the value for the Security Equal To property of a User object. You can establish security equivalences explicitly, automatically, or implicitly.

- **Explicit:** By assignment. Trustees of a file or directory with the Supervisor or Access Control right can assign rights explicitly. An eDirectory Administrator can modify an object's Security Equal To property to explicitly assign it the same rights as those assigned to another object. For example, suppose you make a User object named `Joe` security equivalent to the Admin object. After you create the security equivalence, `Joe` has the same rights to the tree and file system as the `Admin` user.
- **Automatic:** By membership in a group or role. Whenever you assign an object to be a member in a Group object or Organizational Role object, the security equivalence is automatically added to the object's Security Equal To property.
- **Implied:** Equivalent to all parent containers and the [Public] trustee. Security equivalence for an object is implied by its parent container and by the Public container, which applies to all users.

Security equivalence is effective only for one step; it is not transferred by a subsequent security equivalence. For example, if you make a third user security equivalent to `Joe` in the example above, that user receives only `Joe`'s original security settings. The third user does not receive Admin rights or any other Security Equal To properties `Joe` might have.

Whenever a user attempts to access a network resource, eDirectory calculates the user's security equivalence and makes that information available to NetWare. NetWare compares the user's security equivalence information to the trustee assignments for the path and target directory or file to determine if the user can access the target resource and what action on it is permitted.

For more information about eDirectory objects and rights, "see eDirectory Rights" (http://www.novell.com/documentation/edir873/edir873/data/fbachifb.html) in the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a2iii88.html). For information about file-system trustee rights, see Section 6.2, "File-System Trustee Rights," on page 40.

6.2 File-System Trustee Rights

File-system trustee rights determine access and usage for directories and files on NSS volumes and Traditional volumes. A trustee is any eDirectory object, such as a User object, Group object, Organizational Role objects, or container object, that you grant one or more rights for a directory or file. trustee assignments allow you to assign ownership, set permissions, and monitor user access.

The file system stores each file system Trustee's ID and rights assignment as metadata with its directory or file in the NSS file system. In the NetWare Traditional file system, the file's security and attributes metadata is stored in the Directory Entry Table (DET) of its parent directory. For NSS, the files and directory properties contain this information.

File-system trustee rights granted at the directory level apply to all the files and subdirectories in that directory, unless the rights redefined at the file or subdirectory level override them.

File-system trustee rights assigned to files and subdirectories redefine the rights that users inherit from directory rights. Eight file-system trustee rights can be granted at either the directory or file level, as described in the table below:

File-System Trustee Right	Description
Supervisor	Grants the trustee all rights to the directory or file and any subordinate items. The Supervisor right cannot be blocked with an IRF (Inherited Rights Filter) and cannot be revoked. Users who have this right can also grant other users any rights to the directory or file and can change its Inherited Rights Filter. Default=Off
Create	Grants the trustee the ability to create directories and files and salvage deleted files. Default=Off
Erase	Grants the trustee the ability to delete directories and files. Default=Off
File Scan	Grants the trustee the ability to view directory and file names in the file system structure, including the directory structure from that file to the root directory. Default=On
Modify	Grants the trustee the ability to rename directories and files, and change file attributes. Does not allow the user to modify the contents of the file. Default=Off
Read	Grants the trustee the ability to open and read files, and open, read, and execute applications. Default=On
Write	Grants the trustee the ability to open and modify (write to) an existing file. Default=Off
Access Control	Grants the trustee the ability to add and remove trustees for directories and files and modify their trustee assignments and inherited rights filters. Default=Off

6.2.1 Inherited Rights Masks

In NetWare, trustee rights assignments made at a given directory level flow down to lower levels until they are either changed or masked out. This is referred to as *inheritance*. The mechanism provided for preventing inheritance is called the Inherited Rights Mask (IRM).

IRMs are taken into account when NSS builds what is referred to as the effective Access Control List (ACL) for a file or directory. The effective ACL is a list of all users who have rights to the directory and includes the rights they have. It is calculated by starting at the root of the volume and working down to the file.

At each level, the IRM is applied to all rights inherited from the parent directory. Only those rights allowed by the mask are inherited by the child object. Rights for the various trustees explicitly assigned to the child are then collected. When a trustee inherits rights from above, the new rights

replace the old ones (except the Supervisor right, which cannot be masked or removed by a new assignment to the same trustee).

By the time NSS reaches the target file or directory, it has a list of all trustees and the rights assigned and inherited for the requested file or directory. This list is then compared against the entries in the connection table structure. Every time there is a match in the connection table with an entry in the effective ACL, the rights are added to those that the owner of the connection has to the requested file or directory.

In reality, the rights are not calculated at every directory level. The actual algorithm NSS uses to calculate the rights for a particular file or directory is somewhat complicated because it ties in closely with the way the rights cache is implemented. The algorithm almost never needs to start at the root and work down.

In effect, when the effective rights of a user to an object are finally resolved, you have a list of all users who have rights to the file or directory (the effective ACL) and a list of all users in the connection table. These lists are seldom very large.

The one exception to this is a connection that has Admin-equivalent rights (not to be confused with having the Supervisor right from a trustee assignment). Admin-equivalent users have all rights to files, and they cannot be masked out by an IRM or explicit trustee assignment. The only way to keep an Admin-equivalent user from accessing files is to make a special trustee assignment that bars access to all but system connections. This assignment cannot be set through normal tools.

All rights other than Supervisor can be stripped away with an IRM at any level for nearly any user, except a user that has Supervisor right to the Server object itself (such as Admin and equivalents, which usually have rights resulting from an eDirectory rights inheritance). In this situation, the Admin user can see all files and folders regardless of IRMs because the access is not granted in the file system. Instead, a bit is set in the connection table to indicate that the user is an admin and as such has full access to the server and all volumes thereon.

6.2.2 Visibility Lists

The Visibility list is only used for making parent directories visible for navigation purposes. If a user has rights to a file, the NCP™ (via NCP Server for NetWare or NCP Server for Linux) makes all directories above the file visible to the user. This saves the administrator the task of assigning explicit rights to each directory above where the actual rights are assigned.

Visibility entries are stored in a manner similar to explicitly-assigned trustees. The first four entries are in the actual beast object; the rest are stored in overflow beast objects linked from the directory beast object.

Visibility lists only appear on directories. There is one entry for every trustee assigned anywhere in the subtree below the directory. Therefore, the further toward the root you go, the more GUIDs you see against that directory. At the root, the list has GUIDs for every trustee on the volume.

Each visibility entry has an eDirectory GUID and a count of the number of references to that GUID in the entries for the directory (not the subtree) where the Visibility list is assigned. This includes trustees that are explicitly assigned, as well as trustees in Visibility lists.

A Visibility list entry can be created in one of two ways:

- An immediate subordinate directory or file has a trustee that the parent does not.
- A visibility entry for a subordinate subdirectory is present.

Visibility counts do not consider trustees from directories or contents of directories that are not immediately subordinate to the considered directory.

The Visibility list is not affected by adding, deleting, or modifying IRMs. These operate in a transverse flow to the Visibility list. In other words, IRMs flow down the directory structure, while the Visibility list works up the structure.

For each request, GUID entries in the connection table are compared for the connection requesting against all GUIDs on the directory in question. If a match is found, the directory is made visible to the user in the Visibility list.

6.2.3 Supervisor Trustee Rights

A trustee of a Server object in eDirectory is automatically granted the Supervisor right [S] to the root directory of every NSS or NetWare Traditional volume attached to that server. You cannot override Supervisor rights with trustee rights applied at the subdirectory or file level, nor with Inherited Rights Filters. The Admin User object is automatically a trustee of the Server object.

The Supervisor user of the NSS or NetWare Traditional volume is automatically a trustee for all directories and files on the system and has all file-system trustee rights for them. The Supervisor right allows its trustee to assign other eDirectory objects as trustees and to specify any of the file-system trustee rights to them.

A trustee must have the Access Control right [A] to make trustee assignments in a directory or file.

Also, a trustee with the Write right to the File Server object is granted the Supervisor right to the file system.

6.2.4 Trustee Assignments for a Volume

If you grant a user privileges at the root directory of a volume, the user gains privileges to the entire volume unless those rights are specifically revoked at a lower level. You should be especially cautious about granting the Access Control right in a root directory. Users with the Access Control right can grant themselves all other rights in any subdirectory on the volume. You can improve network security by granting each user privileges only to the specific directories he or she uses.

6.2.5 Default Trustee Rights

In a trustee assignment for a directory, the default rights are File Scan and Read. Any trustee assignment, whether for a directory or a file, also includes the right to see the path leading from the root to that directory or file.

A new assignment of trustee rights at the file level can revoke rights assigned at the directory level, or it can allow additional rights.

6.2.6 Inherited Trustee Rights

Subdirectories and files can inherit rights from their parent directory. The directory's rights flow down through its structure to subdirectories and files, except for specific subdirectories or files with their own trustee assignments that supersede inherited rights. The trustee can exercise rights on subordinate directories and files without having explicit trustee assignments on each item.

When granting a trustee assignment to a subdirectory or file, the trustee assignment takes precedence over the inherited rights of its parent directory.

6.2.7 Public Trustee Rights

[Public] is a specialized trustee; it is not an eDirectory object. [Public] represents any network user, logged in or not, for rights assignment purposes. [Public] has Browse rights to the top of the tree, giving all users the right to view any object in the tree.

You can always specify [Public] as the trustee of a file, directory, or object. An unspecified authorized user who tries to access a file, directory, or object without any other rights is allowed the rights granted to the [Public] trustee.

6.2.8 Example of Rights Needed for Typical Access Tasks

The following table lists some common tasks and the rights required to do them.

Task	Trustee Assignment Needed
Read from a closed file	Read
See a filename	File Scan
Search a directory	File Scan
Write to a closed file	Write, Create, Erase, Modify
Create and write to a file	Create
Copy files into a directory	Create
Remove an empty subdirectory	Erase
Delete a file	Erase
Change directory or file attributes	Modify
Rename a file	Modify
Change the Inherited Rights Filter	Access Control
Change trustee assignments	Access Control
Modify a directory's disk space assignment for users	Access Control

6.3 Access Control for NSS on Linux

For an OES Linux server, you can control access to services locally or with eDirectory. If the server contains Novell Storage Systems (NSS) volumes, you can control access in only one of the two methods, not both, and not a combination. The access methods are referred to as Independent mode and NetWare mode.

Access Control	File System	Local Users	eDirectory Users	Access Mode
Local only	Linux traditional file systems	Yes	No	xNFS Independent

Access Control	File System	Local Users	eDirectory Users	Access Mode
NCP/eDirectory, except for Root user	Linux traditional file systems	No	Yes	xNFS Independent
Local and NCP/eDirectory	Linux traditional file systems	Yes	Yes, Linux-enabled local users	xNFS Independent
Local only	NSS	Root user only	No	xNFS Independent
NCP/eDirectory, except for Root user	NSS	Root user only	Yes	xNFS NetWare
Local and NCP/eDirectory	NSS	Root user only	Yes, Linux-enabled local users	xNFS NetWare

For more information about NSS, NCP Server, and Linux User Management, see the following:

- Section 2.2, "Compatibility Issues for File System Rights on Linux," on page 13
- "Access Control Issues for NSS on OES Linux" in the *Novell Storage Services File System Administration Guide for OES*

In NetWare mode, NCP calculates access control permissions for three entities:

- The eDirectory User object mapped to the directory or file User ID (UNIX User ID (UID))
- The eDirectory Group object mapped to the directory or file Group ID (UNIX Group ID (GID))
- The eDirectory Group object mapped to the directory or file Others ID (UNIX GID 65535)

These user entities are referred to as *mapped users*. All other users are called *unmapped users*.

For NSS volumes, the POSIX directory and file permissions are not used to determine access permission. NSS uses the permission fields to store Read Only, Read/Write, Execute, and Hidden attributes for directories and files. NSS does not allow the Linux system to set typical access control permissions in the POSIX fields. It interprets Linux `chmod` commands to apply the values as NetWare directory and file attributes, according to the way NSS maps them to the User, Group, and Other permission fields. For information, see Section 6.7, "Displaying Key NSS Directory and File Attributes as Linux POSIX Permissions," on page 48.

When the user connects to the system with a data request, NCP calculates the effective rights table for the user. As NCP accesses the data on an NSS volume, it compares the ID values to the user's effective rights to determine what access is allowed. It then interprets the directory or file attributes from the NSS metadata.

The NCP server ensures that trustee rights and directory and file attributes are enforced when users access their data. To ensure that the user's data is not less secure when accessed from the Linux environment or with other protocols, the NSS volume data tends to be less accessible when accessed locally on the Linux system or through other protocols. NCP users only have rights where they have been explicitly granted to them through trustee assignments on the volume or to the NCP server object in eDirectory so NCP does not create security back doors into other parts of the system.

NCP provides basic accessibility when the Linux-enabled authenticated user accesses the system locally or through another protocol. In order to accomplish this with file systems other than NSS, NCP sets the UID of files and directories to be that of the user who creates them. Using LUM (Linux

User Management), these IDs map to valid Linux UIDs. Additionally, a local user on the Linux system could use NCPFS (`ncpmount`) and establish an authenticated NCP session with the NCP server, allowing the user's local access rights to mirror the rights available remotely through NCP.

With NSS volumes, the trustee information is stored in NSS with the directory or file. NSS allows access to their file system to Linux user IDs based on what their trustee rights are in the NSS file system. If a user has an NCP-assigned trustee right to a subdirectory on an NSS volume, that same user could log in at the Linux console and have the same access locally that he or she has through NCP. Protocols such as NFS and Samba that access files with the remote client's UID should also work well with NSS.

6.4 The Connection Manager for NetWare

For NetWare, the Connection Manager module (`connmgr.nlm`) builds a connection table when a user connects to the file system. When a file is requested from either the NSS file system or the NetWare Traditional file system, the Connection Manager gathers information for the connection table from the eDirectory Services module (`ds.nlm`) in the form of a connection table comprised of the eDirectory EIDs for the object, for group memberships, and for security equivalences.

When the connection is established, the information in the connection table is relatively static unless the connected user is added to a new group or is given an explicit trustee assignment or security equivalence. In those situations, the connection manager updates the connection table and sends out an event that the table has changed. NSS uses this event to update its own connection table.

6.4.1 Connections to the NetWare Traditional File System

For the NetWare Traditional file system, the table of EIDs is all that is needed to proceed with authentication. After eDirectory provides the list of EIDs, the Connection Manager compares the list to the Directory Entry Table (DET) for the Traditional volume. It determines valid trustees by looking at the assigned trustees in the directory structure above (for trustee inheritance) and at the target file system object (for explicit trustee assignments). Inherited Rights Masks (IRMs) are also taken into consideration.

6.4.2 Connections to the NSS File System

For the NSS file system, the NSS connection table establishes an entry for a user when the regular connection table entry is created, rather than at the file system access time. Logically, the NSS connection table is part of the connection table with NSS-specific information, including the eDirectory object's GUID.

NSS uses GUIDs as the key for trustees. It keeps its own connection table with these GUIDs and compares it with the beast object entry to look for valid trustees. It finds valid trustees by looking at assigned trustees in the directory structure above (for trustee inheritance) and at the target file system object (for explicit trustee assignments), also taking IRMs into consideration.

If this fails to provide a method of access, NSS then checks the Visibility list to see if the requested object is a parent directory that requires visibility due to a rights assignment for a child directory. For information about the Visibility list, see Section 6.2.2, "Visibility Lists," on page 42.

When GUIDs are used instead of EIDs, it does not matter which server you are on, provided it is in the same tree, which is why Novell Cluster Services uses NSS pools and volumes.

NSS does not directly access the connection table. However, it does make calls to read information from it to form its own connection table with GUIDs and file-system trustee rights. For information about trustee rights, see Section 6.2, "File-System Trustee Rights," on page 40.

6.5 Novell Client

The Novell Client™ establishes an authenticated connection to the server through eDirectory. It does not perform periodic authentication checks, nor does it track rights. NCP Server and NSS work together to ensure that the Security Equivalence Vector is up-to-date, and that the entries in it are used to give correct access to the file system. The client does not control the rights process. To do so would introduce a security flaw into the client/server relationship in NetWare.

6.6 Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes

Directory and file attributes assign properties to individual directories or files. Some attributes are meaningful only when applied at the file level, but some apply to both the directory and the file levels.

File attributes apply universally to all users. For example, a file that has a read-only attribute is read-only for all users. The file attribute settings are like an on/off switch. Attributes can be set by any trustee with the Modify right to the directory or file, and attributes stay set until they are changed. Attributes do not change when you log out or when you down a file server.

IMPORTANT: Be careful when assigning a directory and file attribute. The attribute applies to all users.

For example, if a trustee with the Modify right enables the Delete Inhibit attribute for a file, no one, including the owner of the file or the network administrator, can delete the file. However, any trustee with the Modify right can disable the Delete Inhibit attribute to allow the file's deletion.

The table below describes directory and file attributes and whether they are apply to directories, files, or both.

Attribute Code	Description	Applies to
A	Archive Needed identifies files that have been modified since the last backup. This attribute is assigned automatically.	Files only
Ci	Copy Inhibit prevents users from copying a file. This attribute overrides the trustee Read right and File Scan right.	Files only
Dc	Do Not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Directories and files
Di	Delete Inhibit prevents users from deleting a directory or file. This attribute overrides the trustee Erase right. When it is enabled, no one, including the owner and network administrator, can delete the directory or file. A trustee with the Modify right must disable this right to allow the directory or file to be deleted.	Directories and files

Attribute Code	Description	Applies to
Dm	Do Not Migrate prevents directories and files from being migrated from the server's server disk to another storage medium.	Directories and files
Ds	Do Not Suballocate prevents data from being suballocated.	Files only
H	The Hidden attribute hides directories and files so they do not appear in a file manager or directory listing.	Directories and files
I	Index allows large files to be accessed quickly by indexing files with more than 64 File Allocation Table (FAT) entries. This attribute is set automatically.	Files only
Ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed.	Directories and files
N	Normal indicates the Read/Write attribute is assigned and the Shareable attribute is not. This is the default attribute assignment for all new files.	Directories and files
P	Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Directories and files
Ri	Rename Inhibit prevents the directory or file name from being modified.	Directories and files
Ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Files only
Rw	Read/Write allows you to write to a file. All files are created with this attribute.	Files only
Sh	Shareable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Files only
Sy	The System attribute hides the directory or file so it does not appear in a file manager or directory listing. System is normally used with operating system files, such as DOS system files.	Directories and files
T	Transactional allows a file to be tracked and protected by the Transaction Tracking System™ (TTS™).	Files only
X	The Execute attribute indicates program files such as .exe or .com.	Files only

6.7 Displaying Key NSS Directory and File Attributes as Linux POSIX Permissions

NSS displays its Read Only (Ro), Read/Write (Rw), Execute (X), and Hidden (H) attributes for directories and files in the Linux POSIX permission fields when the volume is mounted on Linux. However, NSS does not support the POSIX set-user-ID mode bit and set-group-ID mode bit. For information about Ro, Rw, X, and H attributes, see Section 6.6, "Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes," on page 47.

For NSS volumes on Linux, the POSIX permissions are not used conventionally to provide access control. Instead, they are merely a means of displaying NSS attributes in a familiar format to Linux users.

For NSS volumes on Linux, only the Root user can create files in a directory that is marked as Read Only. If the Read Only attribute is enabled for a directory, LUM-enabled users cannot create files in the directory even if they have the trustee Supervisor right assigned to them. For example, the POSIX fields for a Read Only directory might be

`dr-x r-x r-x` (for a directory with Read Only enabled and Hidden disabled)

`d--x --x --x` (for a directory with Read Only and Hidden enabled)

To enable LUM-enabled users to create files, you must disable Read Only for the directory, which is indicated in the POSIX rights field by enabling Write. For example, the POSIX fields when the Read Only attribute is disabled might be

`drwx rwx rwx` (for a directory with Read Only disabled and Hidden disabled)

`d-wx -wx -wx` (for a directory with Read Only disabled and Hidden enabled)

The following table describes how the NSS directory and file attributes are displayed in the Linux POSIX fields and how they handle conventional management commands such as `chmod`.

OES NetWare Directory and File Attributes	OES Linux Permissions (User, Group, Other)	Description
Read Only is enabled. Execute is disabled. Hidden is disabled.	`r-- r-- r--`	NSS enables the Read permission bit and disables the Write permission bit for the User, Group, and Other fields to indicate that the NetWare Read Only attribute is enabled and the Hidden attribute is disabled. The directory or file is visible in your file manager. The NetWare Read Only attribute is always set to On for files and directories. When the Hidden attribute is set to Off, the Read permission bit is set to On for the User, Group, or Other permission fields on Linux. Example: `chmod 400` has the same result as `chmod 444` `r-- r-- r--` The binary value for octal 4 is 100, which corresponds to Read=On, Write=Off, and Execute=Off.
Read Only is enabled. Execute is disabled. Hidden is enabled.	`--- --- ---`	NSS disables the Read and Write permission bits for the User, Group, and Other fields to indicate that the NetWare Read Only attribute is enabled and the Hidden attribute is enabled. The directory or file is not visible in your file manager, unless the file manager is set to view hidden files. The NetWare Read Only attribute is always set to On for files and directories. When the Hidden attribute is set to On, the Read permission bit is set to Off for the User, Group, or Other permission fields on Linux. Example: `chmod 044` or `chmod 040` has the same result as `chmod 000` `--- --- ---` The binary value for octal 0 is 000, which corresponds to Read=Off, Write=Off, and Execute=Off.

OES NetWare Directory and File Attributes	OES Linux Permissions (User, Group, Other)	Description

Read Only is disabled.
 	
Execute is disabled.
 	
Hidden is disabled.
	`rw- rw- rw-`	NSS enables the Write permission bit to indicate that Read Only is disabled. All users can read and modify the file or directory.
		
		If you set the Write permission bit for the User permission field, NSS sets the Write bit in all fields to the value in the User field.
		
		By default, NSS disables the Read Only attribute for files, so both the Read and Write permission bits are set to On in the Linux permissions.
		
		Example 1: `chmod 620` or `chmod 644` has the same result as `chmod 666`
		
		`rw- rw- rw-`
		
		The binary value for octal 6 is 110, which corresponds to Read=On, Write=On, and Execute=Off for the User field. The binary value for octal 2 is 010, which corresponds to Read=Off, Write=On, and Execute=Off for the Group field. NSS always sets the Read field to On. Because Write is set to On for the User field, it is also set to On for all fields. The NetWare Read Only attribute is disabled.
		
		Example 2: `chmod 420` or `chmod 466` has the same result as `chmod 444`
		
		`r-- r-- r--`
		
		NSS always sets the Read field to On. Because Write is set to Off for the User field, it is also set to Off for all. The NetWare Read Only attribute is enabled.

OES NetWare Directory and File Attributes	OES Linux Permissions (User, Group, Other)	Description

Read Only is enabled.
 	
Execute is enabled.
 	
Hidden is disabled.
	`r-x r-x r-x`	NSS enables the Execute permission bit to indicate that Execute is enabled. When the Execute permission is enabled, all users can list the contents of the directory and change to the directory.
		
		For files, if you set the Execute permission bit to On for any of the User, Group, or Other permission fields, NSS sets the Execute bit to On for all fields.
		
		For files, if you set the Execute permission bit to Off for all of the User, Group, or Other permission fields, NSS sets the Execute bit to Off for all fields.
		
		For directories, both the Read and Execute permission bits are always set to On.
		
		Example 1: `chmod 001`, `chmod 441`, or `chmod 401` has the same result as `chmod 555`
		
		`r-x r-x r-x`
		
		The binary value for octal 5 is 101, which corresponds to Read=On, Write=Off, and Execute=On. The binary value for octal 1 is 001, which corresponds to Read=Off, Write=Off, and Execute=On for the Other field. NSS always sets the Read field to On. Because the Execute bit is set to On for one of the fields, it is set to On for all of the fields.
		
		Example 2: `chmod 622`, `chmod 700`, or `chmod 766` has the same result as `chmod 777`
		
		`rwx rwx rwx`
		
		The binary value for octal 7 is 111, which corresponds to Read=On, Write=On, and Execute=On. NSS always sets the Read field to On. Because the Execute bit is set to On for one of the fields, it is set to On for all of the fields. Because Write is On for the User field, it is set to On for all fields.
		
		Example 3: for directories, `chmod 000`, `chmod 400`, and `chmod 022` have the same result as `chmod 555`
		
		`r-x r-x r-x`
		
		The binary value for octal 2 is 010, which corresponds to Read=Off, Write=On, and Execute=Off. NSS always sets the Read field to On. NSS always sets the Execute field to On for directories. The `chmod` command has no effect on the state of Read and Execute permission bits for directories. Because the Write bit is set to Off in the User field, it is set to Off for all fields.

OES NetWare Directory and File Attributes	OES Linux Permissions (User, Group, Other)	Description
Read Only is disabled. Execute is enabled. Hidden is disabled.	`rwx rwx rwx`	NSS enables the Read, Write, and Execute permission bits when Read Only is disabled and Execute is enabled. All users can read and modify the directory or file, and they can list the contents of the directory and change to the directory.

6.8 What's Next

Continue with "Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes" on page 53.

7 Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes

This section discusses how to configure Trustee Rights and Inherited Rights and Filters for directories and files on the Novell® Storage Services™ File System and NetWare® Traditional File System.

For an explanation of trustee rights, see “Understanding File System Access Control for NSS and NetWare Traditional File Systems” on page 39.

7.1 Tools for Managing File System Trustees and Attributes

7.1.1 Accessing Novell NetStorage

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

`http://192.168.1.1/oneNet/NetStorage`

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

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

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

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

NOTE: Viewing or changing directory and file attributes and rights using NetStorage is only possible using a browser. This functionality is not available using Microsoft Web Folders.

7.1.2 Accessing the Novell Client

In combination with NCP Server on your OES Linux or NetWare server, the Novell Client™ supports the following:

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

For information, see the following:

- *Novell Client for Windows Installation and Administration Guide* (http://www.novell.com/documentation/noclienu/noclienu/data/h4rudg93.html)
- *Novell Client 1.0 for Linux User Guide* (http://www.novell.com/documentation/linux_client/linuxclientuser/data/bwfuc85.html)

7.1.3 Accessing Novell Remote Manager for NetWare (NetWare)

1. In your Web browser, log in as administrator to Novell Remote Manager on the NetWare server where you want to create a directory. The general form of the URL is

   `http://192.168.1.1:8008`

   `https://192.168.1.1:8009`

   Replace `192.168.1.1` with the actual IP address or DNS name of your server.
2. Click *Manage Server* > *Volumes*.
3. Click the *Properties* icon  next to the volume you want to manage.

7.2 Generating a Server Security Report (NetWare)

For NetWare, you can generate the server Security report in Novell Remote Manager for NetWare to help track potential security risks. This report shows only the information that the logged-in user is allowed to view. To receive a report with the most helpful information, log in as the Admin user or as a user with eDirectory rights equivalent to Admin.

To generate the Security report for your NetWare server:

1. Open a Web browser to the Novell Remote Manager, then log in as administrator or equivalent.
2. In the left navigator, click *Reports/Log Files* to open the Reports/Log Files page.
3. Click *View Security Report*.

From this report, you can track the following file system security information:

- Trustee assignments for each volume

  Granting a user privileges at the root directory of a volume gives that user privileges to the entire volume unless those rights are specifically revoked at a lower level. You should be especially cautious about granting the Access Control right in a root directory. Users with the Access Control right can grant themselves all other rights in any subdirectory on the volume. You can improve network security by granting each user privileges only to the specific directories he or she uses.

- Trustee assignments for each common folder on the `sys:` volume

  User, organization, role, or other eDirectory objects should have only limited access, such as Read and File Scan rights, to common directories on volume sys: such as `sys:\public` and `sys:\login`.

- A list of users that have security equivalence to user Admin

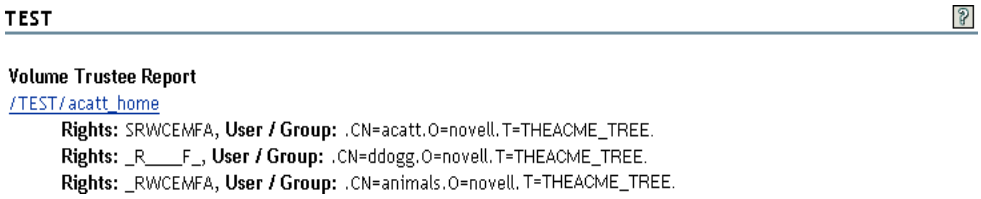
  As the number of users with rights equivalent to user Admin increases, your security risks multiply. Any time a user with rights equivalent to user Admin leaves a server unattended, anyone can gain access to the server.

For information, see "Security Report" in the *Novell Remote Manager for NetWare Administration Guide for OES*.

7.3 Viewing a File System Trustee Report for a Volume (NetWare)

For NetWare, administrators can view a Volume Trustee Report to see which users are trustees of which files and directories on a volume.

1. In Novell Remote Manager for NetWare, click *Manage Server* > *Volumes* to open the Volume Management page.
2. Click the *Information* icon ⓘ next to volume you are monitoring.
3. Scroll down the page, then click the *Volume Trustee Report* link.



7.4 Managing File System Trustees, Trustee Rights, and Inherited Rights Filters

Use the following methods to modify file system trustees for directories and files on NSS or NetWare Traditional file systems.

7.4.1 Using Novell NetStorage

1. Open your Web browser to NetStorage and log in.

   For information, see Section 7.1.1, "Accessing Novell NetStorage," on page 53.
2. Right-click the directory or file you want to manage, then select *Properties*.
3. Do one or more of the following:

   Although the option labels refer to NetWare, use the options for your NSS volumes on Linux or NetWare.

   - **Add Trustees:** Click the *NetWare Rights* tab, click the *eDirectory Object* viewer and brows to select the trustee you want to add, then click *Plus* (+).
   - **Remove Trustees:** Click the *NetWare Rights* tab, select the *Trustee* check box next to one or more trustees you want to remove, then click *Remove*.
   - **Modify File System Rights:** Click the *NetWare Rights* tab, in the *Rights* check boxes next to the trustee, select or deselect rights for the trustee, then click *Apply*.

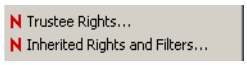
     For information, see Section 6.2, "File-System Trustee Rights," on page 40.
   - **Modify Inherited Rights Filter:** Click the *NetWare Rights* tab, select or deselect *Inherited Rights*, then click *Apply*.

     For information, see Section 6.2, "File-System Trustee Rights," on page 40.

7.4.2 Using the Novell Client to Manage Trustees and Trustee Rights

Administrators and users can manage file-system trustee rights for network directories and files, using the Novell Client on their workstations.

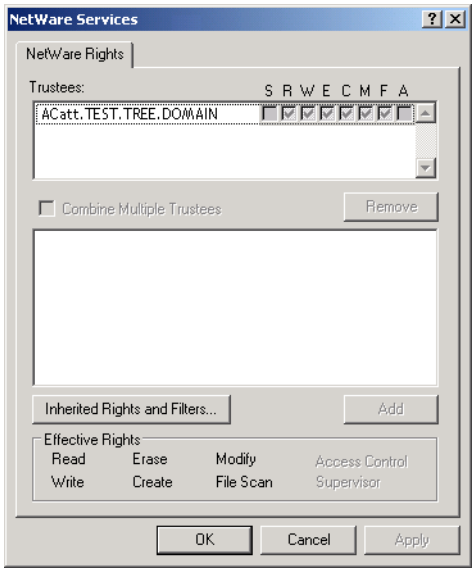
1. In a file manager, right-click the network directory or file, then select *Trustee Rights*.

2. In the *Trustees* area, click the username to display the user's trustee rights.

   Each trustee's rights are shown by a check mark under the letters of the associated rights. If there are no trustees listed, access for the selected directory or file is currently governed only by its Inherited Rights and Filters.

If you are viewing the properties of multiple directories or files, the trustees and rights shown are the combined trustees and rights for all the files.



3 In the *Effective Rights* area, view the actual rights of the selected user.

Explicit file-system trustee rights override inherited rights. If there are no trustees listed, the effective rights are the same as the inherited rights.

4 (Conditional) If you have the Supervisor right or the Access Control right for the selected network directory or file, you can configure trustee rights.

Do one or more of the following:

- **Add a Trustee:** Click *Add*, type the fully distinguished name (`username.context.tree.domain`) of the user you want to add, then click *OK*.
- **Modify Trustee Rights:** Select one or more trustees, select or deselect the check box for each trustee right you want to modify, then click *Apply*.
- **Delete a Trustee:** Select one or more trustees, then click *Remove*.
- **Combine Multiple Trustees:** This option is available only when viewing the file-system trustee rights for multiple directories or files. Additionally, at least one of the selected directories or files must have at least one trustee assignment.

  Select one or more trustees from the *Trustees* list, select *Combine Multiple Trustees*, then click *Apply*. The trustees' rights are combined and applied to all selected directories and files. All selected trustees become trustees of all selected directories and files.

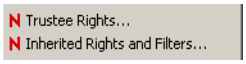
5 When you are done, click *OK* to apply your changes.

7.4.3 Using the Novell Client to Manage Inherited Rights and Filters

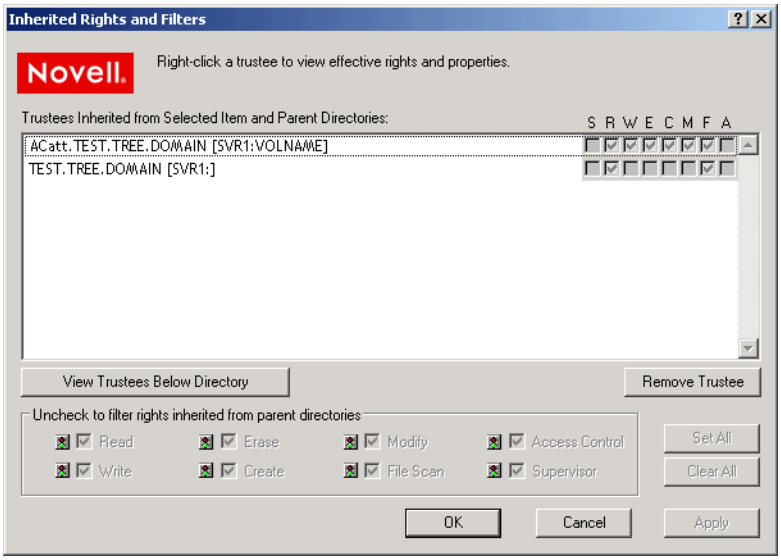
Administrators and users can manage file system inherited rights and filters for network directories and files, using the Novell Client on their workstations. For information about filtering inherited rights, see Section 6.2.6, "Inherited Trustee Rights," on page 43.

1 Use one of the following methods to access the Inherited Rights and Filters dialog box:

- In a file manager, right-click the network directory or file, then select *Inherited Rights and Filters*.



- In the file-system trustee rights window, click *Inherited Rights and Filters*.



2 (Conditional) If you have the Supervisor right or the Access Control right for the selected network directory or file, you can configure its inherited rights. Do one or more of the following:

- **Modify Trustee Rights:** Select the trustee you want to manage from the *Trustees Inherited from Selected Item and Parent Directories*. Select or deselect the check box of the file-system trustee right you want to modify, then click *Apply*.

  Changing the Inherited Rights and Filters does not grant rights; it removes rights previously assigned at a higher level in the path. Deselect the right to filter the right for a specific trustee or for all trustees of the selected directory or file.

- **Delete a Trustee:** Select the trustee you want to manage from the *Trustees Inherited from Selected Item and Parent Directories*, then click *Remove Trustee*.

3 (Conditional) If you selected a directory, click *View Trustees Below Directory* to view a list of trustees for files or directories in the selected directory.

4 When you are done, click *OK*.

7.4.4 Using Novell Remote Manager for NetWare (NetWare)

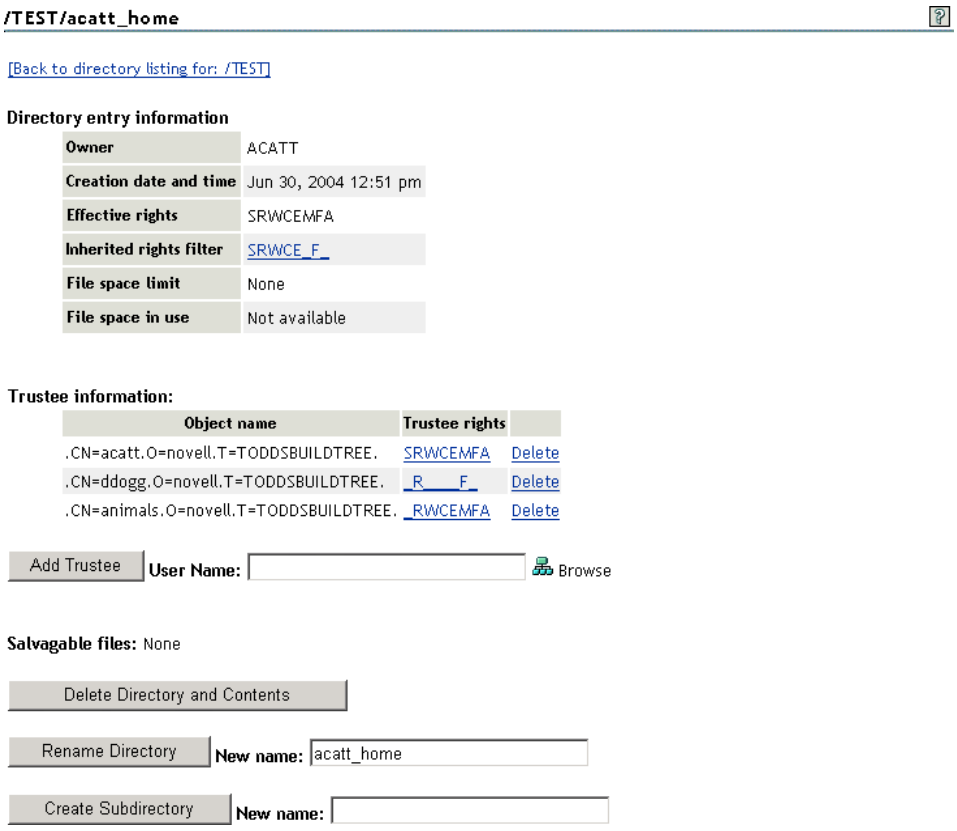
Administrators can also use Novell Remote Manager for NetWare to perform these tasks on NetWare.

1 In Novell Remote Manager, click *Manage Server* > *Volumes* to open the Volume Management page.

2 Click the *Volume* link of the volume you want to manage.

3 Browse to the directory or file you want to manage.

4 Click the *Properties* icon to the left of the directory or file you want to manage.



5 Do one or more of the following:

- **Add a Trustee:** Type the full distinguished name or bindery name of the User object you want to add in the *User Name* field of the *Trustee Information*, or browse to the User object and select it, then click *Add Trustee*.
- **Modify Trustee Rights:** Locate the User object name in the list of User objects under the *Trustee Information*, then click the *Trustee Rights* link next to the username. Select or deselect the check box for the trustee right you want to change, then click *OK*.
- **Delete a Trustee:** Locate the User object name in the list of User objects under the *Trustee Information*, then click the *Delete* link next to the username.
- **Modify the Inherited Rights Filter:** Click the *Inherited Rights Filter* link in the directory or file information table. Select or deselect the check box for the rights you want to modify, then click *OK*.

  Changing the Inherited Rights Filter does not grant rights; it only removes rights previously assigned at a higher level in the tree.

7.5 Managing Attributes for Directories and Files

Administrators can configure NetWare directory and file attributes using the following methods:

- Section 7.5.1, “Using Novell NetStorage,” on page 60
- Section 7.5.2, “Using the Novell Client,” on page 61
- Section 7.5.3, “Using Novell Remote Manager (NetWare),” on page 62
- Section 7.5.4, “Using the NetWare GUI (NetWare),” on page 63

For information about NetWare directory and file attributes and how to apply them, see Section 6.6, “Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes,” on page 47.

7.5.1 Using Novell NetStorage

1. Open your Web browser to NetStorage and log in.

   For information, see Section 7.1.1, “Accessing Novell NetStorage,” on page 53.
2. Right-click the directory or file you want to manage, then select *Properties*.
3. Click the *NetWare Info* tab, select or deselect attributes for the selected directory or file, then click *Apply*.

   Although the option label refers to NetWare, use the option for your Linux and NetWare NSS volumes.

   Select from the following attributes:

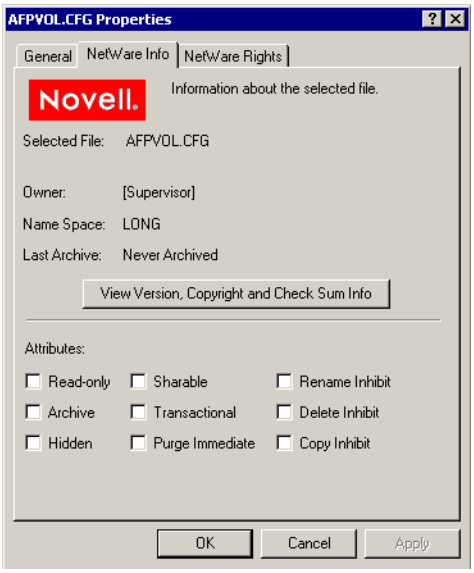
   - *Read only*
   - *Archive*
   - *Hidden*
   - *Shareable*
   - *Transactional*
   - *Purge immediate*
   - *Rename inhibit*
   - *Delete inhibit*
   - *Copy inhibit*

   For information, see Section 6.6, “Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes,” on page 47

7.5.2 Using the Novell Client

Administrators and users with trustee rights can specify some file system attributes for directories and files, using the Novell® Client™ on their workstations.

1 In a file manager, right-click the network directory or file, select *Properties*, then click *NetWare Info*.



2 In the *Attributes* area, select the attribute to enable it, then click *Apply*.

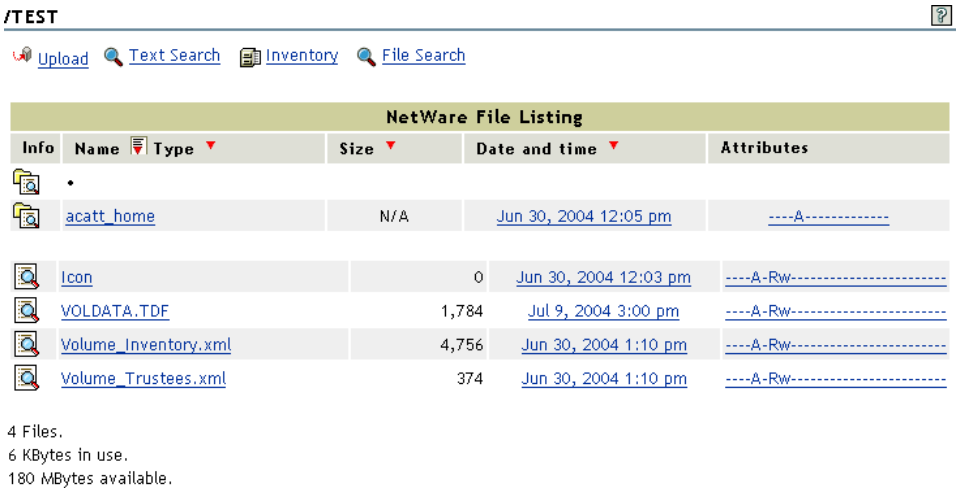
The attribute change is applied only if all the following conditions are met:

- The user has the correct trustee rights necessary to modify the selected attribute.
- The attribute must be a viable attribute for the underlying file system where the file resides. For example, some attributes apply only to NetWare Traditional volumes.
- The attribute must be enforceable by NCP or NSS in the current network configuration.

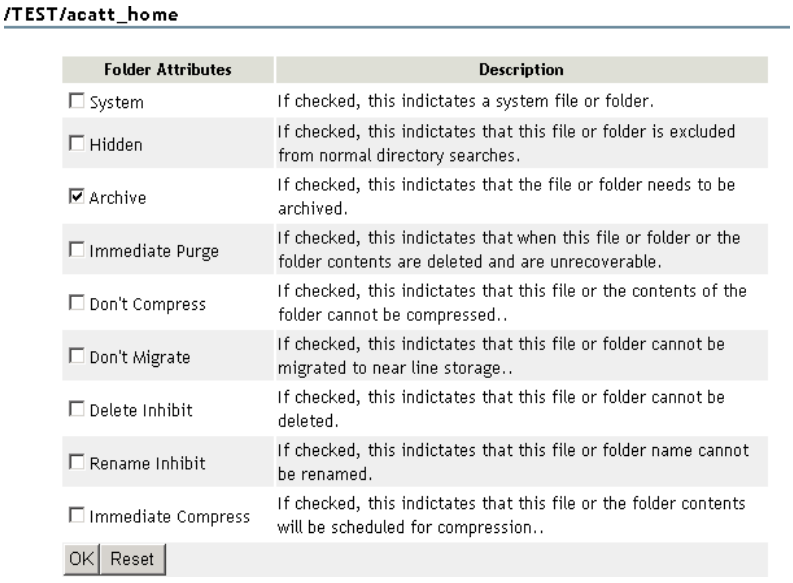
3 Click *OK*.

7.5.3 Using Novell Remote Manager (NetWare)

1. In Novell Remote Manager for NetWare, click *Manage Server* > *Volumes* to open the Volume Management page.
2. Click the *Volume* link of the volume you want to manage.
3. Browse to select the directory or file you want to manage.
4. View the resource's attributes in the *Attributes* column.



5. To modify the attributes, click the *Attributes* link.

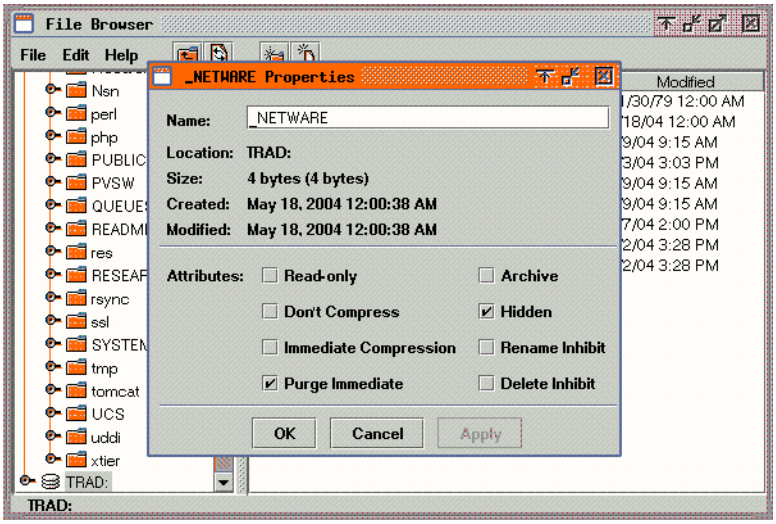


6. Select or deselect the check box for the attribute you want to set.
7. Click *OK*.

7.5.4 Using the NetWare GUI (NetWare)

1 In your NetWare GUI console, browse to the directory or file you want to view or change the attributes of.

2 Right-click the directory or file to open its Properties page.



3 View the attributes in the Attribute area.

4 Select or deselect the check box for the attribute you want to set.

5 Click *OK*.

7.6 Trustee Rights Utility for Linux

The Trustee Rights Utility for Linux allows you to specify trustee rights for directories and files in NSS volumes on OES Linux. This utility does not provide support for Trustees on Linux file systems. It is also not meant to be used to set trustees for NSS volumes on OES NetWare. The trustee information is saved in the file and directory metadata in the NSS volume and works seamlessly with OES NetWare if the volume is moved to OES NetWare.

7.6.1 Purpose

Use this utility at a workstation to

- View or modify user or group rights for files
- View or modify user or group rights for directories and volumes

7.6.2 Syntax

```
rights [OPTIONS]

rights [TOPTIONS] trustee USERNAME

rights [DOPTIONS] delete USERNAME

rights [IOPTIONS] irf
```

```
rights [EROPTIONS] effective USERNAME
rights [SOPTIONS] show
```

7.6.3 Actions

The first argument indicates the action to be taken.

`trustee`	Add or modify a trustee on a file or directory.
`delete`	Remove a trustee from a file or directory.
`irf`	Set the inherited rights filter on a directory.
`effective`	Display a user's effective rights.
`show`	Display the trustees and inherited rights filter.

7.6.4 Options

OPTIONS

`-v, --version`	Display the program version information.
`-h, --help`	Display the help screen.

TOPTIONS

`-r, --rights=MASK`	Specify the rights to be given to this trustee. For information, see MASK. If the No Rights (n) option is assigned, the trustee is removed. If rights are not specified, the default assignment is Read and File Scan rights.

`-f, --file=filename`	Specify the name of file or directory to assign trustees to. Filename is the path for the file or directory. For example:
	`-f /users/username/userfile.sxi`
	`--file=/designs/topsecret`
	If a file or directory is not specified, the current directory is used.

DOPTIONS

`-f, --file=filename`	The name of file or directory to delete trustees from. Filename is the path for the file or directory. If a file or directory is not specified, the current directory is used.

IOPTIONS

`-r, --rights=MASK`	Specify the rights to be passed through the filter. For information, see MASK. If rights are not specified, the default assignment is All Rights.
`-f, --file=filename`	Specify the name of the directory where the filter is to be applied. Filename is the path for the directory. If a directory is not specified, the current directory is used.

EROPTIONS

`-f, --file=filename`	The name of file or directory where effective right are to be calculated. Filename is the path for the file or directory. If a file or directory is not specified, the current directory is used.

SOPTIONS

`-f, --file=filename`	Specify the name of the file or directory to display a list of its trustees. If a file or directory is not specified, the current directory is used.

USERNAME

The username is the fully distinguished name of an eDirectory object, including the tree name. For example: `username.context.treename` or `joe.engineer.acme_tree`.

MASK

The mask is a string of characters, with each character representing a type of rights. The following table lists the rights, the letter to use for each right, and what the right is used for.

Right	Use to
`s` (Supervisor)	Grant all rights to the file or directory.
`r` (Read)	Open and read files in the directory.
`w` (Write)	Open and write to files in the directory.
`c` (Create)	Create files and subdirectories.
`e` (Erase)	Erase files and directories.
`m` (Modify)	Rename files and directories, and change file attributes.
`f` (File Scan)	View and search on file and directory names in the file system structure.
`a` (Access Control)	Add and remove trustees and change trustee rights to files and directories.
`n` (No Rights)	Remove all rights.
`all` (All Rights)	Add All rights except Supervisor.

7.6.5 Example

```
rights -f /designs/topsecret -r rwfc trustee joe.engineer.acme_tree
```

This command assigns Read, Write, File Scan, and Create rights to the `/designs/topsecret` directory for user joe in the engineer context of the `acme_tree` eDirectory tree.

7.7 Trustee Rights Utility for NetWare

The Trustee Rights Utility for NetWare allows you to specify trustee rights for directories and files in NSS volumes on OES NetWare.

7.7.1 Purpose

Use this utility at a workstation to

- View or modify user or group rights for files
- View or modify user or group rights for directories and volumes

7.7.2 Syntax

`RIGHTS` *`path`* `[[ + | - ]` *`rights`*`] [`*`/option`*`...] [/? | /VER]`

Parameter	Use to
`path`	Specify the path to the file, directory, or volume you want to modify or view rights to (you must always specify a path).
`+ | -`	Add or delete the specified rights. See “Using RIGHTS” on page 67.
`rights`	Specify one or more file or directory rights. See “File and Directory Rights” on page 67.
/option	Replace *option* with any available option. See “RIGHTS Options” on page 66.
`/?`	View online help. All other parameters are ignored when /? is used.
`/VER`	View the version number of the utility and the list of files it uses to execute. All other parameters are ignored when /VER is used.

RIGHTS Options

Option	Use to
`/C`	Scroll continuously through output.
`/F`	View the Inherited Rights Filter (IRF).
`/I`	View the trustee and group rights that created the inherited rights, and view where the inherited rights came from.
`/NAME=`*`username`*	View or modify rights for the user or group listed. Replace *username* with the name of the user or group whose rights you want to view or modify.

Option	Use to
/S	View or modify subdirectories below the current level.
/T	View trustee assignments in a directory.

File and Directory Rights

The following table lists the rights, the letter to use for each right, and what the right is used for.

Right	Use to
S (Supervisor)	Grant all rights to the file or directory.
R (Read)	Open and read files in the directory.
W (Write)	Open and write to files in the directory.
C (Create)	Create files and subdirectories.
E (Erase)	Erase files and directories.
M (Modify)	Rename files and directories, and change file attributes.
F (File Scan)	View and search on file and directory names in the file system structure.
A (Access Control)	Add and remove trustees and change trustee rights to files and directories.
N (No Rights)	Remove all rights.
REM (Remove)	Remove the user or group as a trustee of the specified file or directory.
ALL	Add All rights except Supervisor.

7.7.3 Using RIGHTS

- If you use + (plus) to add rights, the rights you list are added to the existing rights.
- If you use - (minus) to remove rights, the rights you list are deleted from the existing rights.
- If you add and delete rights in the same command, group all added rights together and all deleted rights together.
- If you list rights without using + or -, the rights you list replace the existing rights.
- You must always specify a path. You can use a period (.) to represent your current directory.
- You can use wildcard characters.

7.7.4 Examples

- To set the trustee rights in the current directory for user JANICE to Read, Write, and File Scan, enter

  ```
  RIGHTS . RWF /NAME=JANICE
  ```

- To remove user ERNESTO as a trustee of SYS:USERS, enter

  ```
  RIGHTS SYS:USERS REM /NAME=ERNESTO
  ```

- To see where user PATRICK's inherited rights came from for SYS:USERS\HOME, type

```
RIGHTS SYS:USERS\HOME /NAME=PATRICK /I
```

7.8 Attributes Utility for Linux

The Attributes (ATTRIB) Utility for Linux allows you to specify file system attributes for directories and files in NSS volumes on OES Linux.

IMPORTANT: This utility works only with directories and files in the NSS file system on Linux.

7.8.1 Purpose

Use at a workstation to

- View or modify file system attributes for files
- View or modify file system attributes for directories

7.8.2 Syntax

`attrib [OPTIONS] [`*`filename`*`]`

If both the set and clear options are selected, the clear option is done before the set option. If the filename is not specified, the operation is done on the current directory.

7.8.3 Options

OPTIONS

Option	Description
`-s, --set=ATTRIBUTES`	Sets the attributes on the file
`-c, --clear=[ATTRIBUTES | all]`	Clears the attributes on the file
`-l, --long`	Displays a long version of the file's attributes
`-q, --quiet`	Does not display any normal output
`-v, --version`	Displays the program version information
`-h, --help`	Displays the ATTRIB help screen

ATTRIBUTES

Multiple attributes are comma separated.

Code	Description	Applies to Files	Applies to Directories
aa	Attribute Archive identifies that a file's metadata has been modified since the last backup. This attribute is assigned automatically.	Yes	No

Code	Description	Applies to Files	Applies to Directories
all	All (used only for the Clear option) represents all attributes that can be modified.	Yes	Yes
ar	Archive identifies files that have modified content since the last backup. This attribute is assigned automatically.	Yes	No
cc	Cannot compress (status display only) displays if the file cannot be compressed because of limited space savings.	Yes	No
ci	Copy Inhibit prevents users from copying a file. This attribute overrides the trustee Read right and File Scan right.	Yes	No
cm	Compressed (status display only) displays whether the file is currently stored in compressed format.	Yes	No
dc	Do Not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Yes	No
di	Delete Inhibit prevents users from deleting a directory or file. This attribute overrides the trustee Erase right. When it is enabled, no one, including the owner and network administrator, can delete the directory or file. A trustee with the Modify right must disable this right to allow the directory or file to be deleted.	Yes	Yes
ex	Execute indicates program files such as .exe or .com.	Yes	No
hi	Hidden hides directories and files so they do not appear in a file manager or directory listing.	Yes	Yes
ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed. The files in the specified directory are compressed as soon as the operating system can perform the operation after the file is closed. This does not apply to the directory's subdirectories and the files in them.	Yes	Yes
ip	Immediate Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Yes	Yes
ln	Link (status display only) indicates a symbolic link (soft link).	Yes	No
mg	Migrated (status display only) displays if the file or directory is migrated to near-line media.	Yes	Yes
mi	Migrate Inhibit prevents directories and files from being migrated from the server's disk to a near-line storage medium.	Yes	Yes
ri	Rename Inhibit prevents the directory or file name from being modified.	Yes	Yes
ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Yes	No
sd	Subdirectory (status display only) indicates that the entry is a directory, not a file.	No	Yes

Code	Description	Applies to Files	Applies to Directories
sh	Sharable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Yes	No
sy	System hides the directory or file so it does not appear in a file manager or directory listing. System is normally used with operating system files, such as Linux or NetWare system files.	Yes	Yes
tr	Transactional allows a file to be tracked and protected by the Transaction Tracking System™ (TTS™).	Yes	No
vo	Volatile indicates that a file can change without being written to so that opportunistic locks cannot be set on it.	Yes	No

7.8.4 Example

```
attrib /designs/topsecret -c=all -s=ro,di
```

This command clears all attributes, then sets read-only and delete-inhibit on the `/designs/topsecret` file.

7.9 FLAG (NetWare)

For NetWare, you can use the FLAG utility to set directory and file attributes from the command line. For information, see "FLAG (NetWare)" in the *Novell Storage Services File System Administration Guide for OES*.

8 Understanding Directory Structures in Linux Traditional File Systems

This section discusses directory structures for Linux traditional file systems on your OES Linux server.

For information about OES Linux file systems, see the *SUSE Linux Enterprise Server 9 Administration Guide* (http://www.novell.com/documentation/oes/sles_admin/data/front.html).

8.1 Linux Filesystem Hierarchy

Linux recommends a standard file and directory placement. For information, see the *Linux Filesystem Hierarchy* (http://www.tldp.org/LDP/Linux-Filesystem-Hierarchy/html/index.html) at the Linux Documentation Project (http://www.tldp.org).

IMPORTANT: Refer to individual product documentation to understand where Novell applications store files within this hierarchy.

8.2 Default Directories

In Linux, all directories are attached to the root directory, which is identified by a forward slash (/). Directories that are only one level below the root directory are preceded by a slash, to indicate their position and prevent confusion with other directories that could have the same name. For example, the table below lists some common second-level directories:

Linux Directory	Description
`/bin`	System binaries, user programs with normal user permissions
`/sbin`	Executables that need root permission
`/data`	A user-defined directory
`/dev`	System device tree
`/etc`	System configuration
`/home`	Users’ home directories
`/home/username`	A user’s personal home directory
`/tmp`	System temporary files

Linux Directory	Description
/usr	Applications software
/usr/bin	Executable files for programs with user permission
/var	System variables
/lib	Libraries needed for installed programs to run

Every device and hard disk partition is represented in the Linux file system as a subdirectory of the root directory. For example, the floppy disk drive in Linux might be /etc/floppy. The root directory lives in the root partition, but other directories (and the devices they represent) can reside anywhere. Removable devices and hard disk partitions other than the root are mounted (attached) to subdirectories in the directory tree. This is done either at system initialization or in response to a `mount` command.

NOTE: There are no standards in Linux for which subdirectories are used for which devices.

All the file systems use directories and subdirectories. NetWare® separates directories with a backslash, and Linux uses a forward slash. NetWare filenames are case insensitive. Linux file names are case sensitive. For example "`abc`" and "`aBc`" are different files in Linux, but in NetWare, they refer to the same file.

8.3 Linux File Types

As with most file systems, Linux supports a variety of file types, as described in the following table:

File Type	First Character in File Listing	Description
Regular file	-	Normal files such as text, data, or executable files
Directory	d	Files that are lists of other files
Link	l	A shortcut that points to the location of the actual file
Special file	c	Mechanism used for input and output, such as files in /dev
Socket	s	A special file that provides inter-process networking protected by the file system's access control
Pipe	p	A special file that allows processes to communicate with each other without using network socket semantics

8.4 POSIX Access Control Lists

For information, see "Access Control Lists in Linux" (http://www.novell.com/documentation/oes/sles_admin/data/cha-acls.html) in the *SUSE Linux Enterprise Server 9 Administration Guide* (http://www.novell.com/documentation/oes/sles_admin/data/front.html).

Documentation Updates

A

This section contains information about documentation content changes made to the *File Systems Management Guide for OES* since the initial release of Novell® Open Enterprise Server. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the front cover and the Legal Notices page, to determine the release date of this guide. For the most recent version of the *File Systems Management Guide for OES*, see the Novell documentation Web site (http://www.novell.com/documentation/oes/stor_filesys/data/hn0r5fzo.html).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

A.1 November 1, 2005

The entire guide was reformatted to comply with revised Novell documentation standards. The content is unchanged.

A.2 September 29, 2005

Updates were made to the following sections. The changes are explained below.

A.2.1 Understanding File System Access Control for NSS and NetWare Traditional File Systems

The following changes were made to this section:

Location	Change
Section 6.1, "eDirectory Objects and Security Equivalence," on page 39	This section was reorganized and graphics were added for clarity.
Section 6.3, "Access Control for NSS on Linux," on page 44	For an OES Linux server, you can control access to services locally or with eDirectory.

A.3 August 19, 2005

Updates were made to the following sections. The changes are explained below.

- Section A.3.1, "Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes," on page 74

A.3.1 Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes

The following changes were made to this section:

Location	Change
Managing File System Trustees, Trustee Rights, and Inherited Rights Filters	In Section 7.4.1, "Using Novell NetStorage," on page 56, added instructions for the following: • Add trustees • Remove trustees • Modify file system rights • Modify inherited rights filter
Managing Attributes for Directories and Files	In Section 7.5.1, "Using Novell NetStorage," on page 60, added a list of the attributes available in NetStorage.