



Open Enterprise Server 2018 File Systems Management Guide

November 2017

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2017 Micro Focus. All Rights Reserved.

Contents

About This Guide	7
1 File Systems Overview	9
1.1 Novell Storage Services File System	9
1.2 Linux POSIX File Systems	10
1.3 NCP Volumes for Linux	10
2 What's New or Changed in OES File Systems and Storage	11
2.1 What's New or Changed in OES File Systems and Storage (OES 2018)	11
3 Coexistence and Migration Issues	13
3.1 Comparison of NSS to Other File Systems	13
3.2 Compatibility Issues for Trustee Rights on Linux	13
3.2.1 Enforcing Trustee Rights on Linux	13
3.2.2 Assigning Trustee Rights on Linux	15
3.2.3 Key Considerations	16
3.3 NCP Server Directory and File-System Trustee Rights and Attributes	16
3.4 Acquiring eDirectory Security Equivalence Vectors for NSS Users	17
4 Management Tools for Files and Folders Management	19
4.1 iManager and the Files and Folders Plug-In	19
4.1.1 Files and Folders Plug-In Quick Reference	19
4.1.2 Accessing iManager	21
4.1.3 Using the Files and Folders Role in iManager	21
4.1.4 Using the Tree, Browse or Search View in iManager	22
4.2 Novell Remote Manager	23
4.2.1 Prerequisites for Using Novell Remote Manager	23
4.2.2 Novell Remote Manager for Linux	24
4.2.3 Accessing Novell Remote Manager	25
4.2.4 Starting, Stopping, or Restarting Novell Remote Manager on Linux	25
4.3 Novell NetStorage	25
4.4 Novell Client	26
5 Understanding File System Access Control Using Trustees	27
5.1 Understanding the OES Trustee Model for File System Access	27
5.1.1 Trustees	28
5.1.2 File System Trustee Rights	30
5.1.3 Inherited Trustee Rights	33
5.1.4 Security Equivalence	34
5.1.5 Effective Rights	37
5.1.6 Visibility	38
5.1.7 Visibility Lists	39
5.1.8 Security Equivalence Vector	40
5.2 Configuring a Non-Admin User to be an Admin-Equivalent User	40
5.3 Configuring [Public] as a File System Trustee	43

5.4	Configuring the [Public] Trustee Access Rights on NSS Volumes for Daemons Running as the Nobody User	45
5.5	Using QuickFinder with NCP Volumes and NSS Volumes	47
5.6	Access Control for NSS on Linux	47
5.7	Understanding Directory and File Attributes for NSS Volumes	48
5.8	Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions	50
5.9	Troubleshooting File Attributes Issues	54
6	Configuring Trustees and File System Attributes	55
6.1	Viewing a Trustee Report for a Directory or File	55
6.2	Viewing a Trustee Report for All Directories in a Volume	56
6.3	Viewing Properties of a File or Folder in iManager	56
6.4	Viewing Properties for a File or Folder with Novell Client	59
6.5	Using the Files and Folders Plug-In for iManager to Manage Trustees, Trustee Rights, and Inherited Rights	60
6.5.1	Prerequisites	61
6.5.2	Viewing, Adding, or Removing File System Trustees	61
6.5.3	Viewing, Granting, or Revoking File System Trustee Rights	62
6.5.4	Configuring the Inherited Rights Filter for a File or Directory	63
6.5.5	Viewing Effective Rights for a Trustee	64
6.6	Using Novell NetStorage to Manage Trustees, Trustee Rights, and Inherited Rights	64
6.7	Using the Novell Client to Manage Trustees and Trustee Rights	65
6.8	Using the Novell Client to Manage Inherited Rights and Filters	66
6.9	Using the Rights Utility to Set Trustee Rights for the NSS File System	67
6.9.1	Syntax	67
6.9.2	Options	67
6.9.3	Example	70
6.9.4	See Also	70
7	Managing Effective Rights	71
7.1	Understanding Effective Rights	71
7.2	Limitations for Effective Rights and Rights to Files and Folders	71
7.3	Viewing Effective Rights	72
7.4	Assigning Rights to Files and Folders	74
8	Understanding Directory Structures for the NSS File System	75
8.1	Directory Structures	75
8.2	Directory Path	76
8.3	Root Directory	76
8.4	Drive Map	76
9	Managing Files and Folders	77
9.1	Creating a Folder on an NSS Volume or NCP Volume	77
9.1.1	Prerequisites for Creating Folders	77
9.1.2	Tools for Creating Folders	78
9.1.3	Creating a Folder with iManager	78
9.2	Moving a File or Folder to a Different Folder on the Same Volume	79
9.2.1	Prerequisites	79
9.2.2	Procedure	79
9.3	Renaming a File or Folder on an NSS Volume or NCP Volume	80
9.3.1	Prerequisites	80

9.3.2	Procedure	80
9.4	Deleting a File or Folder on an NSS Volume or NCP Volume	81
9.4.1	Prerequisites	81
9.4.2	Procedure	81
9.5	Uploading Files to an NSS Volume or NCP Volume	81
9.5.1	Prerequisites	82
9.5.2	Procedure	82
9.6	Downloading Files from an NSS Volume or NCP Volume	82
9.6.1	Prerequisites	83
9.6.2	Procedure	83
9.7	Mapping Network Drives	83
9.7.1	Using Novell Map Network Drive	84
9.7.2	Using Map Network Drive in Windows Explorer	85
10 Managing Directory Quotas on NSS Volumes		87
10.1	Setting the Directory Quotas Attribute for an NSS Volume	87
10.2	Setting a Directory Quota in iManager	88
10.3	Setting a Directory Quota with Novell NetStorage	90
10.4	Setting a Directory Quota with the Novell Client	90
10.5	Removing a Directory Quota	91
10.6	Removing All Directory Quotas for an NSS Volume	92
10.7	Using the Quota Utility to Set Directory and User Space Quotas on NSS Volumes	92
10.7.1	Syntax	92
10.7.2	Options	92
10.7.3	Examples	93
11 Salvaging or Purging Deleted Files and Folders on NSS Volumes		95
11.1	Salvaging or Purging Deleted Files with iManager	95
11.1.1	Prerequisites	95
11.1.2	Salvaging a Deleted File	96
11.1.3	Purging Deleted Files	97
11.2	Salvaging or Purging Deleted Files with Other Tools	98
11.2.1	Using NetStorage	98
11.2.2	Using the Novell Client	99
12 Configuring File System Attributes for NSS Files and Folders		101
12.1	Viewing Properties of a File or Folder in iManager	101
12.2	Viewing or Modifying File Ownership	106
12.3	Viewing or Modifying File System Attributes for NSS Volumes	107
12.4	Using the Novell Client to Configure File System Attributes	108
12.5	Using Novell NetStorage to Configure File System Attributes	109
12.6	Using the Attrib Utility to Set NSS File System Attributes	109
12.6.1	Syntax	109
12.6.2	Options	110
12.6.3	Attributes	110
12.6.4	Example	111
12.6.5	See Also	111
13 Understanding Directory Structures in Linux POSIX File Systems		113
13.1	Linux Filesystem Hierarchy	113
13.2	Default Directories	113
13.3	Linux File Types	114

13.4 POSIX Access Control Lists 114

About This Guide

This document describes how to create directories and files on an Open Enterprise Server (OES), and to give users secure access to them. It discusses file system access control issues, such as file system trustees, trustee rights, inherited rights filters, and directory and file attributes, for the Novell Storage Services (NSS) file system and NetWare Core Protocol (NCP) volumes on Linux POSIX file systems.

For information about managing Linux POSIX file systems and access control lists, see the following resources:

- ♦ *SUSE Linux Enterprise Server 11 SP4 Storage Administration Guide* (https://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html)
- ♦ “Access Control Lists” (https://www.suse.com/documentation/sles11/book_security/data/cha_acls.html) in the *SLES 11 SP4 Security Guide* (https://www.suse.com/documentation/sles11/book_security/data/book_security.html)

This guide is divided into the following sections:

- ♦ Chapter 1, “File Systems Overview,” on page 9
- ♦ Chapter 2, “What’s New or Changed in OES File Systems and Storage,” on page 11
- ♦ Chapter 3, “Coexistence and Migration Issues,” on page 13
- ♦ Chapter 4, “Management Tools for Files and Folders Management,” on page 19
- ♦ Chapter 5, “Understanding File System Access Control Using Trustees,” on page 27
- ♦ Chapter 6, “Configuring Trustees and File System Attributes,” on page 55
- ♦ Chapter 7, “Managing Effective Rights,” on page 71
- ♦ Chapter 8, “Understanding Directory Structures for the NSS File System,” on page 75
- ♦ Chapter 9, “Managing Files and Folders,” on page 77
- ♦ Chapter 10, “Managing Directory Quotas on NSS Volumes,” on page 87
- ♦ Chapter 11, “Salvaging or Purging Deleted Files and Folders on NSS Volumes,” on page 95
- ♦ Chapter 12, “Configuring File System Attributes for NSS Files and Folders,” on page 101
- ♦ Chapter 13, “Understanding Directory Structures in Linux POSIX File Systems,” on page 113

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.

Documentation Updates

For the most recent version of the *File Systems Management Guide*, see the latest [Novell Open Enterprise Server 2015 SP1 documentation website \(http://www.novell.com/documentation/oes2015/\)](http://www.novell.com/documentation/oes2015/)

Additional Documentation

Consult the following guides for information about managing file systems and file access protocols:

- ♦ *OES 2018: NSS File System Administration Guide for Linux*
- ♦ *OES 2018: NCP Server for Linux Administration Guide*
 - ♦ [Novell Client for Linux \(http://www.novell.com/documentation/linux_client/\)](http://www.novell.com/documentation/linux_client/)
 - ♦ [Novell Client for Windows \(http://www.novell.com/documentation/windows_client/\)](http://www.novell.com/documentation/windows_client/)
- ♦ *OES 2018: Novell AFP for Linux Administration Guide*
- ♦ *OES 2018: Novell CIFS for Linux Administration Guide*
- ♦ *OES 2018: Novell Samba Administration Guide*
- ♦ *OES 2018: Domain Services for Windows Administration Guide*
- ♦ *Novell Kanaka for Mac Installation and Administration Guide* (http://www.novell.com/documentation/kanaka/kanaka_install_admin/data/a20gkue.html)
- ♦ *Novell FTP (Pure-FTPd)* (http://www.novell.com/documentation/oes2015/oes_implement_lx/data/bn0rvzm.html)
- ♦ *SUSE Linux Enterprise Server 11 SP4 Storage Administration Guide* (https://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html)
- ♦ “Access Control Lists” (https://www.suse.com/documentation/sles11/book_security/data/cha_acls.html) in the *SLES 11 SP4 Security Guide* (https://www.suse.com/documentation/sles11/book_security/data/book_security.html)

1 File Systems Overview

Open Enterprise Server (OES) 11 SP2 supports the Novell Storage Services (NSS) file system, NetWare Core Protocol (NCP) volumes on Linux POSIX file systems, and Linux POSIX file systems such as Btrfs, Ext2, Ext3, Reiser, and XFS. This section provides an overview of these file system options.

For an overview of file access protocols and other file services in OES 11 and later, see “[File Services](#)” in the *OES 2018: Planning and Implementation Guide*.

- ♦ [Section 1.1, “Novell Storage Services File System,”](#) on page 9
- ♦ [Section 1.2, “Linux POSIX File Systems,”](#) on page 10
- ♦ [Section 1.3, “NCP Volumes for Linux,”](#) on page 10

1.1 Novell Storage Services File System

Open Enterprise Server provides the Novell Storage Services (NSS) file system for Linux platforms. Its many features and capabilities include visibility, a trustee access control model, multiple simultaneous name space 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.

You can move NSS volumes on NetWare 6.5 SP8 to an OES 11 or later server. For information, see “[Cross-Platform Issues for NSS Volumes](#)” in the *OES 2018: NSS File System Administration Guide for Linux*.

Mixed-platform clusters are supported for temporary scenarios where you are converting a cluster from NetWare to Linux. In a mixed-platform cluster, NSS volumes that were created on NetWare can fail over between kernels, allowing for full data and file system feature preservation when converting clusters to Linux. For information, see the *OES 2015 SP1: Novell Cluster Services NetWare to Linux Conversion Guide*.

You can manage all storage management functions in the web-based iManager utility and the console-based 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 *OES 2018: NSS File System Administration Guide for Linux*

1.2 Linux POSIX File Systems

The OES platform supports a variety of Linux POSIX file systems. It requires a Linux POSIX file system, such as Btrfs, Ext3, Reiser, or XFS, 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 POSIX file systems are described in [Table 1-1](#). For more information, see “[Overview of Linux POSIX File Systems](#)” in the *OES 2015 SP1: Linux POSIX Volume Administration Guide*.

Table 1-1 Linux POSIX File Systems

Linux POSIX File System	Description
Btrfs	Btrfs is a copy-on-write (COW) file system based on COW-friendly B-trees. It provides fault tolerance, repair, and easy management features.
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.
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 upgrade from Ext2 to Ext3 without rebuilding your file system. It also offers options to coordinate its metadata journaling with data writes.
Reiser File System (Reiser)	Reiser 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.
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 more information, see the “[Overview of Linux POSIX File Systems](#)” in the *OES 2015 SP1: Linux POSIX Volume Administration Guide*.

1.3 NCP Volumes for Linux

NCP Server for Linux enables you to create NCP volumes on top of Linux POSIX file systems such as Btrfs, Ext3, XFS, and Reiser file systems. This allows you to use the same method of file system trustees and trustee rights to control access to data on Linux POSIX file systems as you use on NSS volumes.

For information, see “[Managing NCP Volumes](#)” in the *OES 2018: NCP Server for Linux Administration Guide*.

2 What's New or Changed in OES File Systems and Storage

This section describes the changes and enhancements made for file systems management since the Open Enterprise Server (OES) 2018 release.

- ♦ [Section 2.1, "What's New or Changed in OES File Systems and Storage \(OES 2018\)," on page 11](#)

2.1 What's New or Changed in OES File Systems and Storage (OES 2018)

Other than bug fixes and the what's new entries mentioned under Novell Storage Services (NSS), there are no changes to File Systems and Storage in the OES 2018 release.

3 Coexistence and Migration Issues

This section discusses the issues involved in the coexistence of Novell Storage Services (NSS) file system and the Linux POSIX file systems in Open Enterprise Server (OES) 11 and later. It also identifies some differences in how the OES Trustee Model is managed on Linux as compared to NetWare 6.5 SP8.

- ♦ [Section 3.1, “Comparison of NSS to Other File Systems,” on page 13](#)
- ♦ [Section 3.2, “Compatibility Issues for Trustee Rights on Linux,” on page 13](#)
- ♦ [Section 3.3, “NCP Server Directory and File-System Trustee Rights and Attributes,” on page 16](#)
- ♦ [Section 3.4, “Acquiring eDirectory Security Equivalence Vectors for NSS Users,” on page 17](#)

3.1 Comparison of NSS to Other File Systems

The *OES 2018: NSS File System Administration Guide for Linux* provides the following comparisons of the Novell Storage Services (NSS) file system on NetWare and Linux and of the NSS file system to NCP volumes on Linux POSIX file systems:

- ♦ [“List of NSS Features”](#)
- ♦ [“Comparison of NSS on Linux and NCP Volumes on Linux POSIX File Systems”](#)

3.2 Compatibility Issues for Trustee Rights on Linux

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

- ♦ [Section 3.2.1, “Enforcing Trustee Rights on Linux,” on page 13](#)
- ♦ [Section 3.2.2, “Assigning Trustee Rights on Linux,” on page 15](#)
- ♦ [Section 3.2.3, “Key Considerations,” on page 16](#)

3.2.1 Enforcing Trustee Rights on Linux

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

- ♦ User identity, such as eDirectory users, Linux-enabled eDirectory users, and local-only users
- ♦ Access method, such as NCP Server, other protocols, or core Linux utilities
- ♦ File system access control, such as NSS file and directory attributes

See the following sections for an overview of these issues:

- ♦ [“eDirectory Users” on page 14](#)
- ♦ [“Local-Only Users” on page 14](#)
- ♦ [“Core Linux Utilities” on page 15](#)

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 Linux Protocols (such as NFS or Samba)	Access via Core Linux Utilities
NSS on Linux	NCP and NSS enforce access. 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.	NCP and NSS enforce access. eDirectory users must be Linux-enabled with Linux User Management.	NCP and NSS enforce access. eDirectory users must be Linux-enabled with Linux User Management. Linux services need to be enabled for pluggable authentication modules (PAM) when you configure Linux User Management.
NCP volumes on Linux POSIX file systems	NCP enforces access. 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.	NCP enforces access. eDirectory users must be Linux-enabled with Linux User Management.	NCP enforces access. eDirectory users must be Linux-enabled with Linux User Management. Linux services need to be enabled for pluggable authentication modules (PAM) when you configure Linux User Management.
Linux POSIX file systems	eDirectory users have no access to files via NCP.	Linux ACLs and POSIX permissions are used to enforce access.	Linux ACLs and POSIX permissions are used to enforce access.

Local-Only Users

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

File System	NCP Server for Linux	Other Protocols (such as NFS or Samba)	Core Linux Utilities
NSS on Linux	Restricted to the <code>root</code> user.	Restricted to the <code>root</code> user.	Restricted to the <code>root</code> user.
NCP volumes on Linux POSIX	Restricted to the <code>root</code> user.	Restricted to the <code>root</code> user.	Restricted to the <code>root</code> user.
Linux POSIX file systems	Local users have no access to files via NCP. Linux ACLs and POSIX permissions are used to enforce access.	Linux ACLs and POSIX permissions are used to enforce access.	Linux ACLs and POSIX permissions are used to enforce access.

Core Linux Utilities

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

- ♦ 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`)
- ♦ Small Footprint CIM Broker (SFCB)

IMPORTANT: To enable users of NSS volumes and NCP volumes to use the core Linux utilities, you must PAM-enable the utility with Linux User Management (LUM) and Linux-enable the users with LUM. For information, see [OES 2018: Linux User Management Administration Guide](#).

3.2.2 Assigning Trustee Rights on Linux

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

IMPORTANT: Only eDirectory users are eligible for file-system trustee rights.

Management Tool	NSS File System on Linux		
	NCP	NFS or Samba	Core Linux Utilities
NSS <code>rights</code> utility	Yes	Yes	Yes
Files and Folders plug-in to iManager	Yes	No	No
Novell NetStorage	Yes	Yes	Yes, for NetStorage with SSH support
Novell Client for Windows XP/2003, Vista, 7, and 8	Yes	Not applicable	Not applicable
Novell Client for Linux	Yes	Not applicable	Not applicable

The following table identifies the management tools to use to assign Novell trustee-based trustee rights on Linux POSIX file systems:

Management Tool	Linux POSIX File Systems		
	NCP	NFS or Samba	Core Linux Utilities
NSS <code>rights</code> utility	Yes	Not applicable	Not applicable

Management Tool	Linux POSIX File Systems		
	NCP	NFS or Samba	Core Linux Utilities
Files and Folders plug-in to iManager	Yes	No	No
Novell NetStorage	Not supported by NetStorage	Not applicable	Not applicable
Novell Client for Windows XP/2003, Vista, 7, and 8	Yes	Not applicable	Not applicable
Novell Client for Linux	Yes	Not applicable	Not applicable

3.2.3 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:

- ◆ Ensure that 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 trustee rights information separately, the information is synchronized between them.

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

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

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

For information, see [Section 5.1, “Understanding the OES Trustee Model for File System Access,”](#) on page 27.

NCP Server supports all NSS file system attributes. For information about attributes, see [Section 5.7, “Understanding Directory and File Attributes for NSS Volumes,”](#) on page 48.

NCP volumes created on Linux POSIX file systems (such as Btrfs, Ext3, XFS, and Reiser) support only the Read Only, Hidden, and Shareable file system attributes.

3.4 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 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 Linux than they are for NSS on NetWare.

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](#)" in the *OES 2018: NSS File System Administration Guide for Linux*.

4 Management Tools for Files and Folders Management

This section identifies the various tools for managing files and folders on Open Enterprise Server (OES) 11 and later servers.

- ♦ [Section 4.1, “iManager and the Files and Folders Plug-In,” on page 19](#)
- ♦ [Section 4.2, “Novell Remote Manager,” on page 23](#)
- ♦ [Section 4.3, “Novell NetStorage,” on page 25](#)
- ♦ [Section 4.4, “Novell Client,” on page 26](#)

4.1 iManager and the Files and Folders Plug-In

iManager is a web browser-based tool used for configuring, managing, and administering eDirectory objects on your network.

- ♦ [Section 4.1.1, “Files and Folders Plug-In Quick Reference,” on page 19](#)
- ♦ [Section 4.1.2, “Accessing iManager,” on page 21](#)
- ♦ [Section 4.1.3, “Using the Files and Folders Role in iManager,” on page 21](#)
- ♦ [Section 4.1.4, “Using the Tree, Browse or Search View in iManager,” on page 22](#)

4.1.1 Files and Folders Plug-In Quick Reference

The Files and Folders plug-in for iManager 2.7 (or later) provides the Files and Folders role in **Roles and Tasks**. It is also integrated in iManager as the **View Objects** option in the iManager toolbar. File browsing in iManager is available for file systems that have a Volume object defined in eDirectory, such as for NSS volumes on Linux and for NCP volumes on Linux.

The Files and Folders Manager NPM file (`fileman.npm`) is automatically installed in iManager. For information about installing NPM files for iManager, see [“Downloading and Installing Plug-in Modules”](#) in the *NetIQ® iManager Administration Guide*.

The Files and Folders plug-in for iManager provides the tasks described in this section. All of the tasks and actions that are available under the **Files and Folders** role are also available from the **View Objects** tree view.

- ♦ [“Delete” on page 20](#)
- ♦ [“Deleted Files” on page 20](#)
- ♦ [“Download” on page 20](#)
- ♦ [“Move to Folder” on page 20](#)
- ♦ [“New Folder” on page 20](#)
- ♦ [“Properties” on page 20](#)
- ♦ [“Rename” on page 21](#)
- ♦ [“Upload” on page 21](#)

Delete

Delete a file or folder on an NSS volume or an NCP volume (NCP share on Ext3, XFS, or Reiser file systems) on Linux.

Deleted Files

Salvage or purge deleted files only for NSS volumes where the volume's Salvage attribute is enabled.

Other NSS volume settings determine how long deleted files and directories are retained for salvage or purge actions. For information about configuring salvage and purge behavior for NSS volumes, see “[Salvaging and Purging Deleted Volumes, Directories, and Files](#)” in the *OES 2018: NSS File System Administration Guide for Linux*.

Download

Select and download a file from an NSS volume or NCP volume to a specified location on your local drive or mapped network drive.

Move to Folder

Move a file or folder on an NSS volume or NCP volume to a different directory in the same volume.

New Folder

Create a folder on an NSS volume or NCP volume.

Properties

Add, remove, or modify file system trustees, trustee rights, and file attributes settings for files and folders.

Table 4-1 Properties Tasks

Tab	Task Description
Information	<p>View information about a selected file or directory, such as:</p> <ul style="list-style-type: none">◆ Current size◆ Time stamps for when the file was created, modified, accessed, and archived◆ File attributes <p>View or modify the file or folder owner for an NSS volume. (You must be logged in as an administrator user of the server.)</p> <p>View or modify a directory quota. Directory quotas management is available only for NSS volumes where the volume's Directory Quotas attribute is enabled.</p>
Rights	<p>View, add, or remove file system trustees for a selected file or directory.</p> <p>View, grant, or revoke file system trustee rights for trustees of the selected file or directory.</p> <p>View or modify the inherited rights filter for a selected file or directory.</p>

Tab	Task Description
Inherited Rights	View or modify the inherited rights filters at every level of the path for a selected file or directory.
	View the effective rights for the selected file or directory.

Rename

Rename a file or folder on an NSS volume or NCP volume.

Upload

Upload a specified file from your local drive or a mapped network drive to a specified location on an NSS volume or NCP volume.

4.1.2 Accessing iManager

- 1 Launch a web browser.
- 2 Click **File > Open**, then enter

```
https://server-IP-address/nps/iManager.html
```

The URL is case sensitive. Replace *server-IP-address* with the actual server DNS name or IP address. For example:

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

The iManager Login page opens.

- 3 Use your administrator user name and password to log in to the eDirectory tree that contains the server you want to manage.

In iManager, you can access only the roles and tasks you are authorized to manage. For full access to all available iManager features, you must log in as Supervisor of the tree.

To modify file or folder ownership on an NSS volume, log in as a user with the Write right to the NCP Server object. Usually, this is the administrator user or a user with rights equivalent to the administrator user. This user must additionally be assigned as a trustee of the file or folder and have the Access Control and Write trustee rights for it.

4.1.3 Using the Files and Folders Role in iManager

- 1 Access iManager, then log in to the eDirectory tree where the server you want to manage resides.

For information, see [Section 4.1.2, “Accessing iManager,” on page 21](#).

- 2 In **Roles and Tasks**, expand the Files and Folders role to reveal its main tasks:
 - ◆ **Delete**
 - ◆ **Deleted Files** (Salvage or purge deleted files on an NSS volume where the Salvage attribute is enabled)
 - ◆ **Download**
 - ◆ **Move to Folder**
 - ◆ **New Folder**

- ◆ **Properties**
 - ◆ **Rename**
 - ◆ **Upload**
- 3 Select a task from the list.
 - 4 Use one of the following methods to select a file or folder in the tree where you are logged in:
 - ◆ Click the **Search** icon to open the eDirectory Object Selector dialog box. Browse or search the list to locate the file or folder you want to manage, then click the object's name link.
 - ◆ Click the **Object History** icon to select a file or folder that you have recently managed.

The file or folder must be on a server that is in the same eDirectory tree where you are currently logged in.
 - 5 Wait for iManager to retrieve information about that file or folder and display the appropriate information to the task page you are in.

It might take several seconds to retrieve the information, depending on the size and complexity of your storage solution.
 - 6 Complete the information required for the action.
 - 7 Click **OK** to perform the action, or click **Cancel** to abandon the changes.

4.1.4 Using the Tree, Browse or Search View in iManager

The Files and Folders plug-in is also integrated in the **Tree**, **Browse**, and **Search** view of a server's eDirectory objects in the left pane. You can browse to locate the Volume object of interest, then perform actions on them.

- 1 Access iManager, then log in to the eDirectory tree where the server you want to manage resides.

For information, see [Section 4.1.2, "Accessing iManager," on page 21](#).
- 2 Click the **View Objects** icon in the iManager toolbar to view the **Tree**, **Browse**, and **Search** view of a server's eDirectory objects in the left pane.
- 3 Use any of the following methods to locate the file or folder of interest:
 - ◆ In the **Tree** view, navigate the tree to locate the volume of interest, then a **Volume** object to see the hierarchical file system tree view of the volume's folders and files.

Click the plus (+) or minus (-) icon next to a directory name to expand or collapse the view of its subdirectories.
 - ◆ In the **Browse** view, select a server, volume, or folder to see a list of its folders and files beneath that object in the right pane.
 - ◆ In the **Search** view, find a volume to see a list of its folders and files beneath that object in the right pane.
- 4 Perform any of the following tasks:

Task	Action to Perform
Create a folder	Select New > New Folder , specify the folder name, then click OK twice.
Delete a file or folder	Select the check box next to the file or folder, click Delete , then click OK .
Download a file	Select the check box next to the file that you want to download, select Actions > Download , browse to select the folder on a local drive or a mapped drive where you want to save the file, then click OK to download the file.

Task	Action to Perform
Move a file or folder to a different folder on the same volume	Select the check box next to the file or folder, click Edit , browse to select the file or folder to move, select the target folder in the same volume, then click OK .
Rename a file or folder	Select the check box next to the file or folder, click New > Rename , browse to select the file or folder to rename, specify the new name, then click OK twice.
Salvage or purge deleted files	Select the check box next to the folder on an NSS volume where the Salvage attribute is enabled, select Actions > Deleted Files to view a list of deleted files, select the files of interest, click Salvage or Purge, then click OK .
Upload a file	Select the check box next to the folder where you want to upload the file, select Actions > Upload , browse to select the file from a local drive or a mapped drive, then click OK to upload the file.
View or modify the properties of a file or folder	Select the check box next to the file or folder, select Actions > Properties , modify the Information, Rights, or Inherited Rights, then click OK twice.

4.2 Novell Remote Manager

Novell Remote Manager (NRM) is a browser-based management utility for monitoring server health, changing the configuration of your server, or performing diagnostic and debugging tasks. With NCP Server installed, you can create and manage NCP volumes as shares on Linux POSIX file systems. With Dynamic Storage Technology (DST) installed, you can create DST shadow volumes.

- ♦ [Section 4.2.1, “Prerequisites for Using Novell Remote Manager,” on page 23](#)
- ♦ [Section 4.2.2, “Novell Remote Manager for Linux,” on page 24](#)
- ♦ [Section 4.2.3, “Accessing Novell Remote Manager,” on page 25](#)
- ♦ [Section 4.2.4, “Starting, Stopping, or Restarting Novell Remote Manager on Linux,” on page 25](#)

4.2.1 Prerequisites for Using Novell Remote Manager

- ♦ [“Prerequisites for Remote Administration” on page 23](#)
- ♦ [“Prerequisites for Admin User Access on Linux Servers” on page 24](#)

Prerequisites for Remote Administration

Your configuration must satisfy the following prerequisites:

- ♦ Ensure that SSL 3.0 (where available) or SSL 2.0 is enabled in your web browser.

Novell Remote Manager requires an SSL connection between your web browser and the target server where it is running. You must enable SSL services for your web browser; otherwise, the browser displays an error when it tries to display the Novell Remote Manager web pages later.

- ♦ Ports 8008 (insecure) and 8009 (secure) are the default ports used for accessing Novell Remote Manager. If you change the port number assigned to it, ensure that you specify the same value for the port number when you log in.

Prerequisites for Admin User Access on Linux Servers

You can log into Novell Remote Manager for Linux as the `root` user for the OES server you are managing. Most tasks in Novell Remote Manager require `root` user privileges.

You can alternately log in to Novell Remote Manager with your eDirectory credentials if you first enable Linux User Management (LUM) in your eDirectory tree and install and configure LUM on the target server. The Admin user or equivalent must be Linux-enabled and at least one of the following conditions must be met:

- ♦ The Admin user (or equivalent user) must be associated to the eDirectory group that has the Supervisor right for the Entry Rights property for the UNIX Workstation object in eDirectory.
- ♦ The Admin user (or equivalent user) must have the Supervisor right for the Entry Rights property to the NCP object that represents the Linux server in the eDirectory tree.

To tell if a user is Linux-enabled, go to iManager, select the User role, then select the user to see if the following is true:

- ♦ The user has a Linux Profile tab on the Modify User page in iManager.
- ♦ The user's eDirectory object is associated with the UNIX Workstation object that represents the Linux server.

For information about configuring Linux User Management and enabling users for Linux, see the [OES 2018: Linux User Management Administration Guide](#).

4.2.2 Novell Remote Manager for Linux

Novell Remote Manager for Linux allows you to browse NSS volumes on your Linux servers. It requires that the NCP Server and NCP Server plug-in for Novell Remote Manager be installed and running.

Tasks

The NCP Server plug-in supports the following tasks:

- ♦ Managing connections to NSS volumes and viewing open files for a connection.

For information, see “[Managing Connections for NCP Volumes and NSS Volumes](#)” in the [OES 2018: NCP Server for Linux Administration Guide](#).

- ♦ Creating or managing shadow volumes with NSS volumes as the primary and secondary storage areas.

For information, see the [OES 2018: Dynamic Storage Technology Administration Guide](#).

Novell Remote Manager for Linux does not support the following tasks for NSS on Linux:

- ♦ Configuring directory quotas
- ♦ Salvaging and purging deleted files and directories
- ♦ Configuring file system trustees and attributes for directories and files
- ♦ Creating and managing partitions, pools, and volumes

Additional Information

For detailed information about NRM on Linux, see the [OES 2018: OES Remote Manager Administration Guide](#).

4.2.3 Accessing Novell Remote Manager

- 1 From your web browser, enter one of the following:

`http://server-ip-address:8008`

`https://server-ip-address:8009`

Replace *server-ip-address* with the IP address of the server you want to manage. If you have Domain Name Services (DNS) installed on your network for server name-to-IP address resolution, you can optionally use the server's DNS name instead of the IP address.

- 2 Determine the authenticity of the SSL certificate, then accept it if the certificate is valid.
- 3 When the Login page appears, type the `root` user name and password for that server, or type the user name and password of the Admin user (or equivalent user) who is an eDirectory user and who has been Linux-enabled.
- 4 Click **OK** to log in to the target server and initiate your SSL session.

The management interface opens in your web browser. After logging in, your SSL session for Novell Remote Manager remains open until you close all your browser windows at that workstation.

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

Novell Remote Manager on Linux is installed and runs by default. If it hangs, you can use the `/etc/init.d/novell-httpstkd` script to get status or to stop, start, or restart `httpstkd`. For the latest information about `httpstkd`, see “Starting or Stopping HTTPSTKD” in the *OES 2018: OES Remote Manager Administration Guide*.

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

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

4.3 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 eDirectory for authentication. Log in with your administrator user name and password to manage file system access for directories and files on NSS volumes. You can also log in as any user name 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.

4.4 Novell Client

In combination with NCP Server on your OES 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 2.0 SP3 for Linux Administration Guide](#)
- ♦ [Client for Open Enterprise Server Administration Guide](#) (Windows 7 and 8)
- ♦ [Novell Client 2 SP1 for Windows Administration Guide](#) (Windows Vista)
- ♦ [Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide](#)

5 Understanding File System Access Control Using Trustees

The Novell Storage Services (NSS) volumes and NCP (Netware Control Protocol) volumes use the OES Trustee Model to secure access to directories and files. eDirectory objects, file-system trustee rights, and file system attributes for directories and files work together to allow you to control who can access a directory or file and which actions are possible.

- ♦ [Section 5.1, “Understanding the OES Trustee Model for File System Access,” on page 27](#)
- ♦ [Section 5.2, “Configuring a Non-Admin User to be an Admin-Equivalent User,” on page 40](#)
- ♦ [Section 5.3, “Configuring \[Public\] as a File System Trustee,” on page 43](#)
- ♦ [Section 5.4, “Configuring the \[Public\] Trustee Access Rights on NSS Volumes for Daemons Running as the Nobody User,” on page 45](#)
- ♦ [Section 5.5, “Using QuickFinder with NCP Volumes and NSS Volumes,” on page 47](#)
- ♦ [Section 5.6, “Access Control for NSS on Linux,” on page 47](#)
- ♦ [Section 5.7, “Understanding Directory and File Attributes for NSS Volumes,” on page 48](#)
- ♦ [Section 5.8, “Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions,” on page 50](#)
- ♦ [Section 5.9, “Troubleshooting File Attributes Issues,” on page 54](#)

5.1 Understanding the OES Trustee Model for File System Access

The OES Trustee Model allows you to assign eDirectory objects as trustees on NSS volumes and NCP volumes and the directories and file on them, and then to assign file system rights to the trustees. The model's inheritance function allows subdirectories and files to inherit rights from a parent directory in the directory tree, or to mask the rights that should not be inherited. The security equivalence function allows permissions to be assigned indirectly. The model also controls visibility of files and folders so that users can see only the directory paths needed to access the files where they have trustee rights.

The NSS file system natively supports the Trustee Model to control user access. The NCP Server on Linux emulates the Trustee Model's functions for NCP volumes on traditional POSIX file systems (such as btrfs, Ext2/3, Reiser, and XFS). For NCP volumes, the actions are provided by the file access protocol and not the underlying native Linux file system. For NSS volumes, NCP Server synchronizes the emulated capabilities with the native capabilities of the NSS file system.

Before you assign trustees and set trustee rights, ensure that you have a solid understanding of the OES Trustee Model and how its various functions can be used to control user access to data on NSS volumes and NCP volumes.

- ♦ [Section 5.1.1, “Trustees,” on page 28](#)
- ♦ [Section 5.1.2, “File System Trustee Rights,” on page 30](#)
- ♦ [Section 5.1.3, “Inherited Trustee Rights,” on page 33](#)
- ♦ [Section 5.1.4, “Security Equivalence,” on page 34](#)

- ♦ [Section 5.1.5, “Effective Rights,” on page 37](#)
- ♦ [Section 5.1.6, “Visibility,” on page 38](#)
- ♦ [Section 5.1.7, “Visibility Lists,” on page 39](#)
- ♦ [Section 5.1.8, “Security Equivalence Vector,” on page 40](#)

5.1.1 Trustees

A trustee is any eDirectory object (such as a User, Group, Organizational Role, or container) that you grant rights to access a directory or file on an NSS volume or an NCP volume. Trustees and trustee rights can be assigned explicitly, or they can be assigned through inheritance and security equivalence. (These concepts are described in subsequent sections.)

IMPORTANT: NSS does not support dynamic and nested eDirectory groups. Although it is possible to add these groups as trustees in NSS volumes, NSS does not recognize the rights assigned to them as applying to group members.

Trustee assignments, and not file ownership, determine who can access a file. Administrator users can modify the ownership of files without affecting who has rights to access and use the files. Changing the file or folder ownership additionally requires that the user be the administrator user (or a user with the eDirectory Write right to the NCP Server object) for the server.

In OES, administrators, users, and network resources are represented as objects in an eDirectory database. The eDirectory structure is a flexible, hierarchical structure that can represent your business units, IT infrastructure, geographical locations, and so on.





[Figure 5-1](#) illustrates eDirectory objects and their relationship to network resources and users. 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. The `YourCo` container 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. In the `Accounts` container, `Bob` is a User object  for a system user who is assigned to the Accounts Department. Other OUs in the `Finance` container might represent Purchasing and Billing organizations. Other OUs in the `YourCo` container represent organizations at the same level as `Finance`, such as Sales, Marketing, and Manufacturing.

Figure 5-1 Example eDirectory Container and Objects



You can use the **Directory Administration** option in iManager to create eDirectory objects. For information, see [“Managing Objects”](#) in the *NetIQ eDirectory Administration Guide*.

Trustees can be set at multiple levels to get different results. The following sections describe how trustees work at different levels in the file system.

- ♦ [“Admin User and Admin-Equivalent Users” on page 29](#)
- ♦ [“\[Public\] Trustee” on page 29](#)
- ♦ [“Volume-Level Trustees” on page 29](#)

- ♦ “Subdirectory-Level Trustees” on page 30
- ♦ “File-Level Trustees” on page 30

Admin User and Admin-Equivalent Users

File system access for the Admin user and Admin-Equivalent users is not granted in the file system. Instead, a bit is set in the connection table to indicate that the user is an administrator and as such has full access to the server and all volumes thereon. The Admin user automatically has the Supervisor right to the Server object and can see all files and directories.

When you set a non-admin User object as security equal to the Admin user, you grant the user all the privileges of the Admin user. These privileges cannot be restricted by rights for that User object through explicit trustee assignment, security equivalence to other groups or other users, or inheritance. For information, see [Section 5.2, “Configuring a Non-Admin User to be an Admin-Equivalent User,”](#) on page 40.

Granting a user Admin-equivalence might be desired if the Admin-equivalent user has broad responsibilities for eDirectory and file system management. However, it provides more privileges than are needed if the administrator role you want to define has limited management responsibilities.

To increase security or to support a distributed administration model, you can create a special object for the administrator role and restrict file system and eDirectory rights required based on their administration responsibilities. For an example of how to set up a special GroupWise administrator identity and assign the appropriate eDirectory rights and file system rights, see [“Assigning Rights Based on Administration Responsibilities”](#) in the *GroupWise 2012 Administration Guide*.

[Public] Trustee

[Public] is a special trustee; it is not an eDirectory object. The [Public] trustee represents any network user, logged in or not, for rights assignment purposes. The [Public] trustee 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.

IMPORTANT: For security reasons, you should not provide the file system Supervisor right to the [Public] trustee.

For information, see [Section 5.3, “Configuring \[Public\] as a File System Trustee,”](#) on page 43.

For an example of how to use the [Public] trustee, see [Section 5.4, “Configuring the \[Public\] Trustee Access Rights on NSS Volumes for Daemons Running as the Nobody User,”](#) on page 45.

Volume-Level Trustees

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 (except Supervisor right) in any subdirectory on the volume. You can improve network security by granting users privileges only to the specific directories they use by setting trustees explicitly or by leveraging the inheritance and security equivalence functions.

Subdirectory-Level Trustees

An assignment of trustee rights for a user at the subdirectory level can revoke rights assigned at a parent directory, or it can allow additional rights. Trustee rights granted on directories determine which rights are allowed to flow down for that trustee to the child subdirectories and files. The effective rights for a user on the current subdirectory are the combined set of explicit rights for the user plus security equivalence rights plus the filtered inherited rights.

File-Level Trustees

An assignment of trustee rights for a user at the file level can revoke rights assigned at the parent directory, or it can allow additional rights. For this user, inherited rights are ignored. The user's rights are the combined set of explicit rights for the user plus security equivalence rights. More restrictive security-equivalent rights do not revoke the explicitly set user rights.

IMPORTANT: File-level rights work for read-only files or for file types where applications do not delete the original file when saving changes.

File-level trustee rights can be problematic because of how third-party applications handle file modifications. When a file is opened for writing, many applications function as follows:

1. The application copies the file to a temporary file in order to save internal memory or as a safety net to prevent data loss due to a power failure, system crash, or human error.
2. As the user makes changes, the application records changes in the temporary file.
3. When the user saves changes, the application deletes the original file, and then creates a new file (or renames the temporary file) with the same name as the original.

When the application deletes the original file, the trustee settings on the file are automatically deleted. The file system sees the replacement file as a new file. The file system is not application aware; that is, it does not track the ultimate intent of the applications that you might use.

5.1.2 File System Trustee Rights

Trustee rights are file system rights and not eDirectory rights. They govern the actions that a trustee can perform on a directory or file that resides on an NSS volume or NCP volume. Trustee rights can be granted explicitly. However, you can also leverage inheritance and security equivalence to provide effective rights to a user. (These concepts are described in subsequent sections.)

NCP Server stores the trustee IDs and rights settings on each volume in the `._NETWARE/.trustee_database.xml` file. For NSS volumes, the file system also stores each trustee's ID and rights assignment as metadata with the directory or file where the assignment is made.

- ♦ [“Rights Definitions” on page 30](#)
- ♦ [“Supervisor Right” on page 31](#)
- ♦ [“Access Control Right” on page 32](#)
- ♦ [“Default Trustee Rights” on page 32](#)
- ♦ [“Rights Needed for Typical Access Tasks” on page 32](#)

Rights Definitions

The actions for each right are described in [Table 5-1](#).

Table 5-1 File System Trustee Rights

File-System Trustee Right	Description
Supervisor (S)	<p>Grants the trustee all rights to the directory or file and any subordinate items.</p> <p>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.</p> <p>Default=Off</p>
Read (R)	<p>Grants the trustee the ability to open and read files, and open, read, and execute applications.</p> <p>Default=On</p>
Write (W)	<p>Grants the trustee the ability to open and modify (write to) an existing file.</p> <p>Default=Off</p>
Create (C)	<p>Grants the trustee the ability to create directories and files and salvage deleted files.</p> <p>Default=Off</p>
Erase (E)	<p>Grants the trustee the ability to delete directories and files.</p> <p>Default=Off</p>
Modify (M)	<p>Grants the trustee the ability to rename directories and files, and change file attributes. It does not allow the user to modify the contents of the file.</p> <p>Default=Off</p>
File Scan (F)	<p>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.</p> <p>Default=On</p>
Access Control (A)	<p>Grants the trustee the ability to add and remove trustees for directories and files, to modify the rights assigned for trustees, and set the inherited rights filters.</p> <p>This right does not allow the trustee to add or remove the Supervisor right for any user. Also, it does not allow to remove the trustee with Supervisor right.</p> <p>Default=Off</p>

Supervisor Right

An eDirectory trustee of a Server object is automatically granted the Supervisor right [S] to the root directory of every NSS volume attached to that server. You cannot override the file system rights of the user with the Supervisor right by applying explicit rights or masking inherited rights at the subdirectory or file level.

The Admin User object is automatically a trustee of the Server object.

The Supervisor user of the NSS 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.

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

Access Control Right

A non-Supervisor trustee must have the Access Control right [A] to make trustee assignments in a directory or file. The Access Control right does not permit the user to limit Supervisor right.

Default Trustee Rights

When you assign a trustee for a directory, the default rights are Read and File Scan [RF]. 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. These are made visible by the visibility function; they are not actually set on the directories in the path.

Rights Needed for Typical Access Tasks

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

Task	Trustee Right Needed
Change directory or file attributes	Modify
Change the file or folder ownership	Access Control and be an administrator user of the server
Change the Inherited Rights Filter	Access Control
Change trustee assignments	Access Control
Copy files into a directory	Create
Create and write to a file	Create
Delete a file	Erase
Modify a directory's disk space assignment for users	Access Control
Open or save a Microsoft Office file	Read, Write, File Scan, Create, Modify, Erase
Open or save an OpenOffice.org file	Read, Write, File Scan, Create, Modify, Erase
Read a closed file	Read
Remove an empty subdirectory	Erase
Rename a file	Modify
Search a directory	File Scan
See a file name (visibility)	File Scan
Write to a closed file	Write, Create, Erase, Modify

5.1.3 Inherited Trustee Rights

Subdirectories and files inherit rights from their parent directory. Typically, you set rights that you want to flow down to all users by assigning a Group object as the trustee of a directory located at the root of the volume. The trustee rights flow down through the file tree structure to its child subdirectories and files.

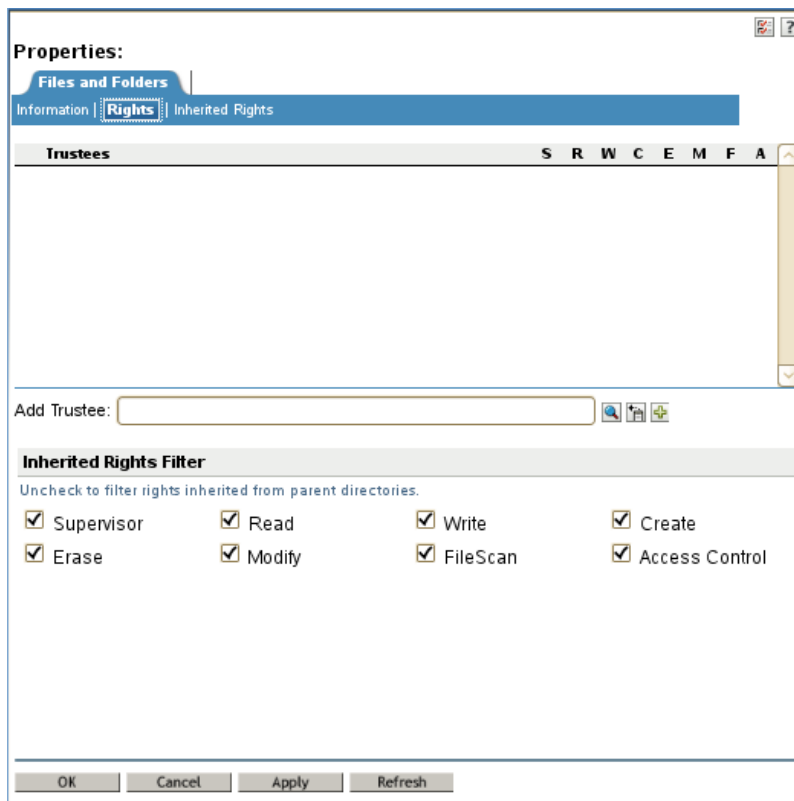
Setting rights for a trustee on a directory or a file changes inheritance in the following ways:

- ♦ **Directory:** Trustee rights granted on directories determine which rights are allowed to flow down for that trustee to the child subdirectories and files. The inherited rights filters set on child subdirectories and files are applied to the trustee's rights set on the parent directory.
- ♦ **File:** Trustee rights granted on a file determine which rights are allowed for the user. For this trustee or its security-equivalent trustees, inherited rights are ignored.

You can mask or filter what rights can be inherited. The Inherited Rights Mask (IRM) is the set of rights that you block from inheritance, while the Inherited Rights Filter (IRF) is the set of rights that you allow to be inherited. The IRM and IRF apply only to rights coming down the tree from parent directories. They do not affect any rights granted at the point where you set the IRM or IRF. The IRF settings for the file or directory apply for all trustees except users with the Supervisor right, the Admin user, or the Admin-equivalent users for the server.

For example, in iManager, the Files and Folders plug-in allows you to view or modify the Inherited Rights Filter for a selected file or folder by viewing its **Properties**, then clicking the **Rights** tab. By default, all rights (SRWCEMFA) are allowed to be inherited, as shown in [Figure 5-2](#). You deselect a right to disable it from being inherited by the file or folder. That is, the right is masked so that it cannot flow down.

Figure 5-2 Viewing or Modifying the Inherited Rights for a File or Folder



IRMs are taken into account when NSS or NCP Server 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 that NSS or NCP Server 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 that NSS or NCP Server 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, IRF, or explicit trustee assignment.

All rights other than Supervisor can be stripped away with an IRM or IRF at any level for nearly any user, except a user that has Supervisor right to the Server object itself (such as the Admin user and the Admin-equivalent users, which usually have rights resulting from an eDirectory rights inheritance). In this situation, the Admin user can see all files and directories regardless of IRMs or IRFs 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.

5.1.4 Security Equivalence

Security equivalence means having the same rights as another object. When you make one object security equivalent to another object, the rights of the second object are added to the rights of the first object when the system calculates the first object's effective rights.

Security equivalence helps 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 an eDirectory object. Security equivalence granted rights are added to any rights explicitly granted for an object. For a directory, they are also added to the filtered inherited rights.

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 the NCP Server. NCP Server 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.

You can establish security equivalence by using the following methods:

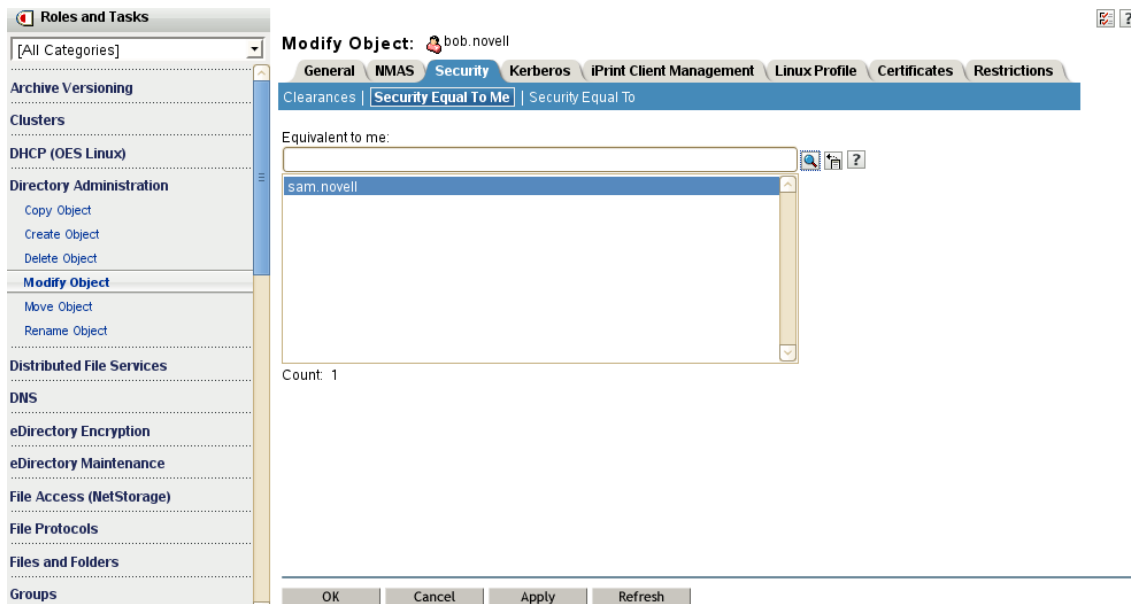
- ◆ “Explicit Security Equivalence” on page 35
- ◆ “Automatic Security Equivalence” on page 35
- ◆ “Implied Security Equivalence” on page 37

Explicit Security Equivalence

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, in iManager, you can use the **Directory Administration > Modify Object** option to make a User object named `sam` to be the security equivalent to the User object named `bob`, as shown in [Figure 5-3](#). After you create the security equivalence, `sam` effectively has the same rights to the file system tree as those explicitly assigned to `bob`.

Figure 5-3 The Security Equal To Property for eDirectory Objects



Automatic Security Equivalence

Security equivalence is also achieved 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 member object’s **Security Equal To** property.

For example, in iManager, you can use the **Directory Administration > Modify Object** option to add the User object named `sam` as a member of the Group object named `team`, as shown in [Figure 5-4](#). The `team` object is automatically added to the **Security Equal To** property for `sam`, as shown in [Figure 5-4](#). All members of the Group object, including `sam`, effectively have the same rights to the file system tree as those explicitly assigned to `team`.

Figure 5-4 The Membership Property for eDirectory Group Objects

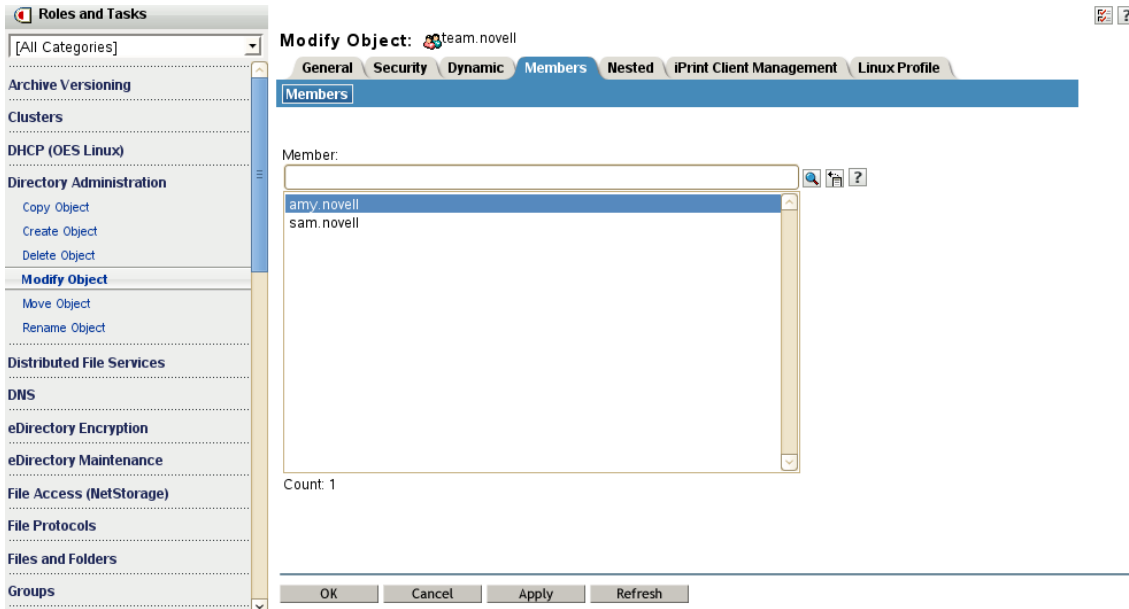
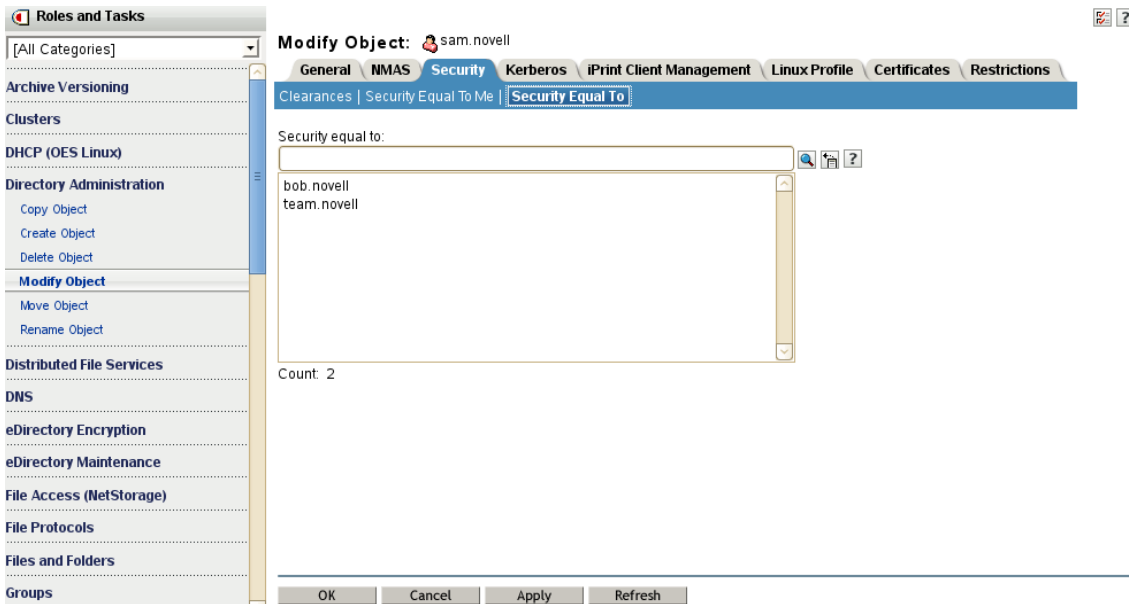


Figure 5-5 Group Memberships Added Automatically to the User's Security Equal To Property



An Organizational Role object defines a position or role within the organization that can be filled by any designated user. The organizational role is particularly useful for delegating administrative authority, such as for rotating positions that support multiple employees, where the responsibilities of the job, and the network access required, are static. Another use is for the segregation of duties, where company or regulatory policies require that specific tasks be performed by different users. For example, you might not want the same person both to acknowledge the receipt of goods and to process payment to the vendor. If a User object is assigned as an occupant of an organizational role, the user is automatically granted all file system trustee rights assigned to the role. Some organizational role examples include postmaster, network administrator, help-desk workers, physicians, and academic faculty.

Implied Security Equivalence

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. For information about setting rights for the [Public] trustee, see “[Public] Trustee” on page 29.

5.1.5 Effective Rights

A user’s explicit rights on a directory are combined with the filtered rights inherited from its parent directory. Any rights through security equivalence are also applied.

A user’s explicit rights on a file override any rights that can be inherited from its parent directory. In this case, the user has only the rights granted, and the inherited rights are ignored. If the user is a member of another group or role that also has explicit rights to the file, the user’s effective rights on the file are a combination of the rights granted for the user and the rights granted for the group or role. If the rights of the group or role are more restrictive than the user’s explicit rights, it has no effect on rights granted to the user.

An object’s effective rights to a subdirectory are the set of distinct rights from the following:

- ◆ Rights inherited for the user from the parent directory, with consideration of the inherited rights filter set for the subdirectory.
- ◆ Rights set explicitly for the user on the directory.
- ◆ Rights set explicitly for a security-equivalent object on the directory:
 - ◆ Explicit by assignment (**Security Equal To** property)
 - ◆ Automatic by membership in a group or role
 - ◆ Implied by its parent container and by the [Public] container

More restrictive security-equivalent rights do not override rights granted for the trustee on the directory or for the trustee’s filtered inherited rights.

An object’s effective rights to a file are determined by the following:

- ◆ Rights inherited for the user from the parent directory, with consideration of the inherited rights filter set for the file.

If the user has rights set on the parent directory or is security equivalent to an object with explicit rights set there, those are the rights that flow down to the file for the user and are subject to the IRF.

Inherited rights for a file are ignored if rights are set explicitly for the object or for a security equivalent of the object. This behavior is different than for a directory.

- ◆ Rights set explicitly for the user on the file.

Inherited rights are ignored. Explicit trustee rights for a security equivalent object are added. More restrictive security-equivalent rights do not override rights set for the trustee on the file.

- ◆ Rights set explicitly for a security-equivalent object on the file:
 - ◆ Explicit by assignment (**Security Equal To** property)
 - ◆ Automatic by membership in a group or role
 - ◆ Implied by its parent container and by the [Public] container

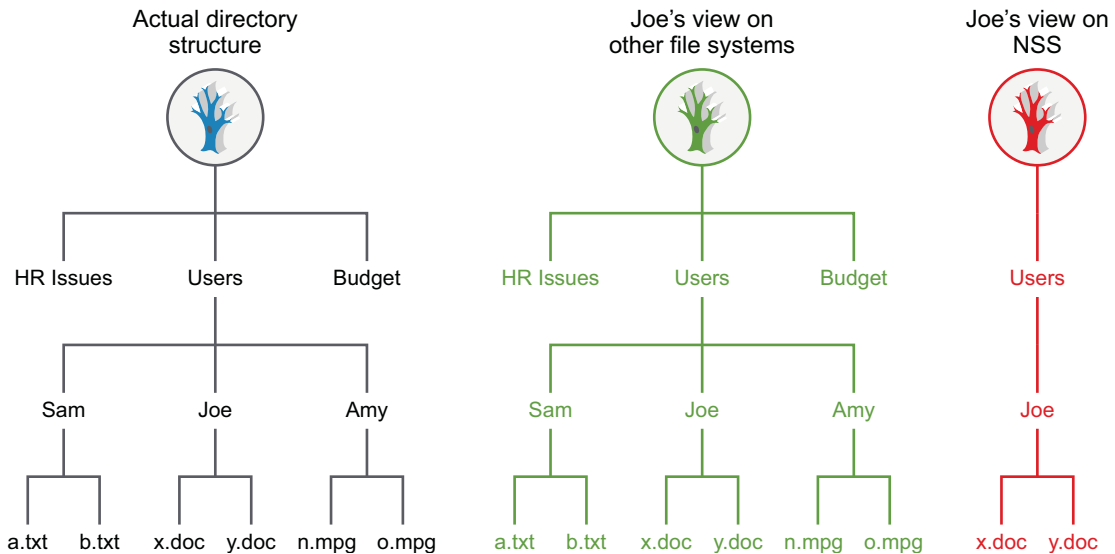
Inherited rights are ignored. Explicit trustee rights are added.

For more information, see “Hard Links and File System Trustees” in the *OES 2015 SP1: NSS File System Administration Guide for Linux* and “How Effective Rights Are Calculated” in the *NetIQ eDirectory Administration Guide*.

5.1.6 Visibility

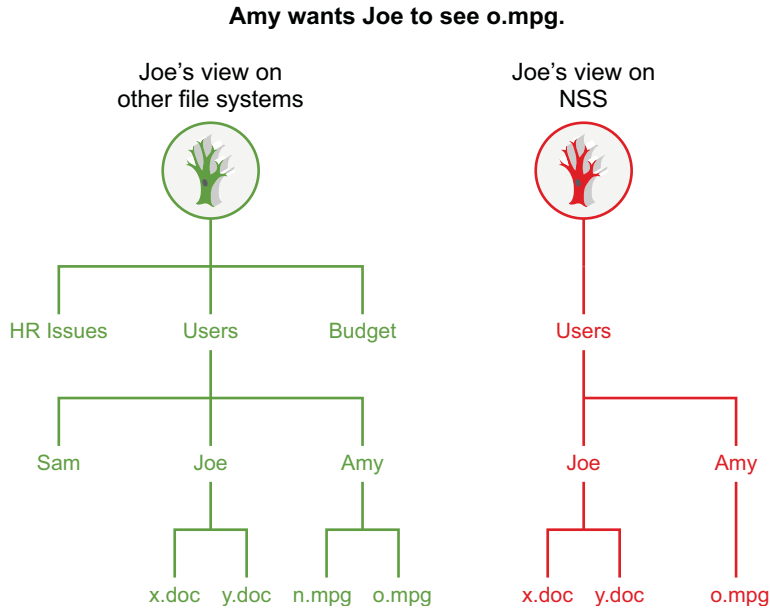
The OES Trustee Model also controls visibility into the file system. For example, the user Joe is made a trustee of the `Joe` folder, and has access only to files in the `Joe` folder. [Figure 5-6](#) demonstrates how Joe’s view of the file system differs if the files are on a volume where the Trustee Model is applied as compared to the ACL (Access Control Lists) method on other file systems.

Figure 5-6 File System Tree View for Joe with the Trustee versus ACL Methods



A user who is a trustee with the Access Control (A) right or Supervisor (S) right can assign other users as trustees of files in directories and set rights for them. A user who has only the Access Control right cannot modify the Supervisor right of another user. For example, the user Amy is the trustee of her home directory and has the Access Control right. Amy makes Joe a trustee of the read-only `o.mpg` file in her personal `Amy` folder, and grants Joe the Read Only access to the file. On an NSS file system, Joe now sees the `\Amy\o.mpg` path and file in addition to his personal `Joe` folder. Joe cannot see other files in the `Amy` folder.

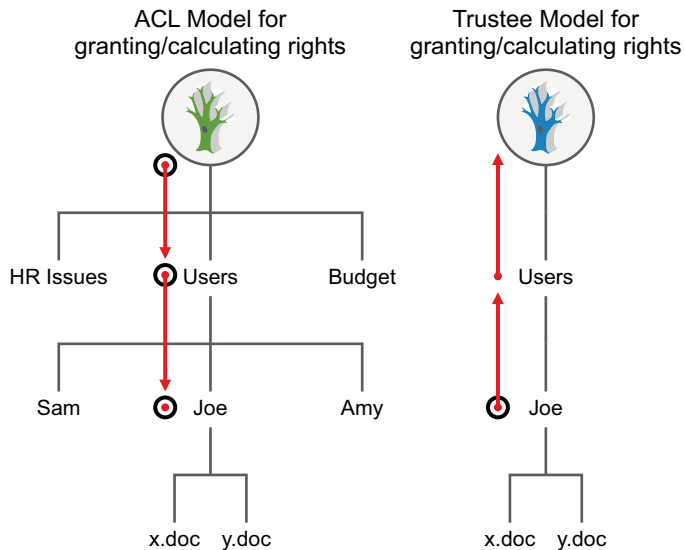
Figure 5-7 File System Tree View of a Shared File for Joe with the Trustee versus ACL Methods



5.1.7 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 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, as illustrated in [Figure 5-8](#).

Figure 5-8 Visibility for Trustee versus ACL Methods



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.

5.1.8 Security Equivalence Vector

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.

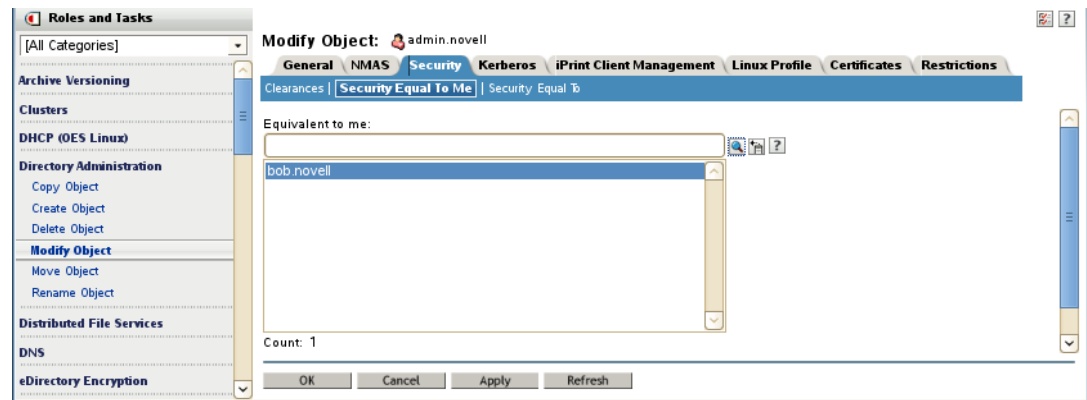
The Novell Client establishes an authenticated connection to the server through eDirectory. It does not perform periodic authentication checks, nor does it track rights. The client does not control the rights process. To do so would introduce a security flaw into the client/server relationship.

5.2 Configuring a Non-Admin User to be an Admin-Equivalent User

The following procedure describes how to set user bob.novell as an Admin-equivalent of the Admin user admin.novell. Ensure that you modify the context for your user according to where the object exists in your own eDirectory structure.

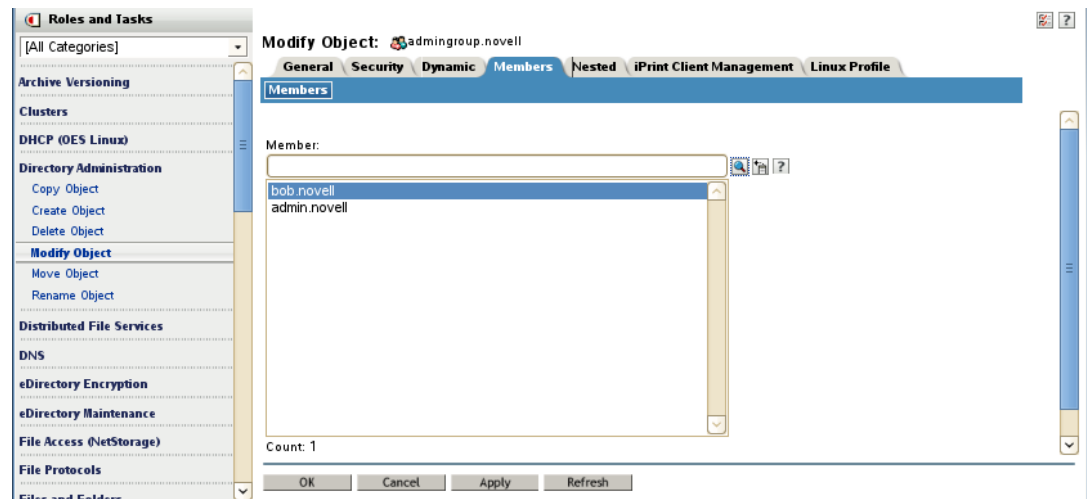
- 1 Log in to iManager as the Admin user in the same tree as the server you want to manage.
- 2 Set the bob.novell User object as security equal to the admin.novell User object.
 - 2a In the iManager **Roles and Tasks** list, select **Directory Administration > Modify Object**.
 - 2b On the Modify Object page, browse to locate and select the admin.novell User object, then click **OK**.
 - 2c On the Modify Object page for admin.novell, select the **Security** tab, then click the **Security Equal to Me** link.
 - 2d On the Security Equal to Me page, browse to locate and select the bob.novell User object, then click **OK**.

The bob.novell User object appears in the **Equivalent to Me** list of users who have security equal to the Admin user.



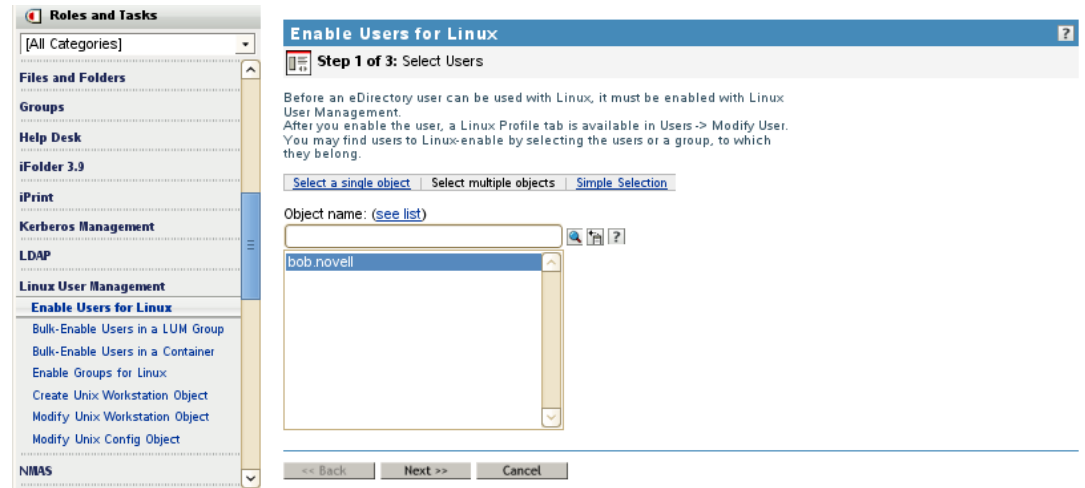
- 2e At the bottom of the page, click **Apply** or **OK**.
- 3 Add the bob.novell User object as a member of the admingroup.novell for the server you want to manage.
 - 3a In the iManager **Roles and Tasks** list, select **Directory Administration > Modify Object**.
 - 3b On the Modify Object page, browse to locate and select the admingroup.novell Group object, then click **OK**.
 - 3c On the Modify Object page for admingroup.novell, select the **Members** tab.
 - 3d On the Members page, browse to locate and select the bob.novell User object, then click **OK**.

The bob.novell User object appears in the **Members** list.



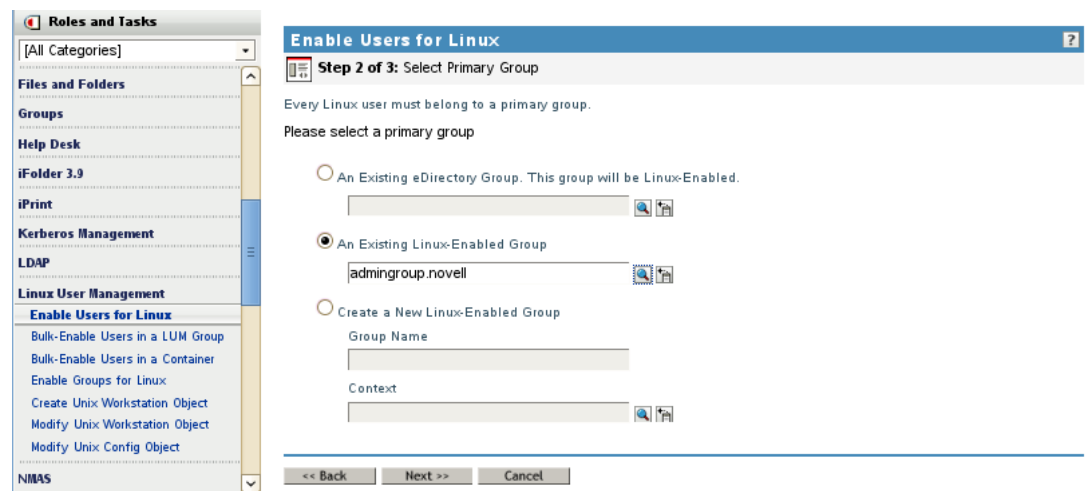
- 3e At the bottom of the page, click **Apply** or **OK**.
- 4 Enable the bob.novell User object with Linux User Management (LUM) by adding it to the existing LUM-enabled group admingroup.novell.
 - 4a In the iManager **Roles and Tasks** list, select **Linux User Management > Enable Users for Linux**.
 - 4b On the Select Users page, browse to locate and select the bob.novell User object, then click **OK**.

The bob.novell object appears in the **Object Name** list.



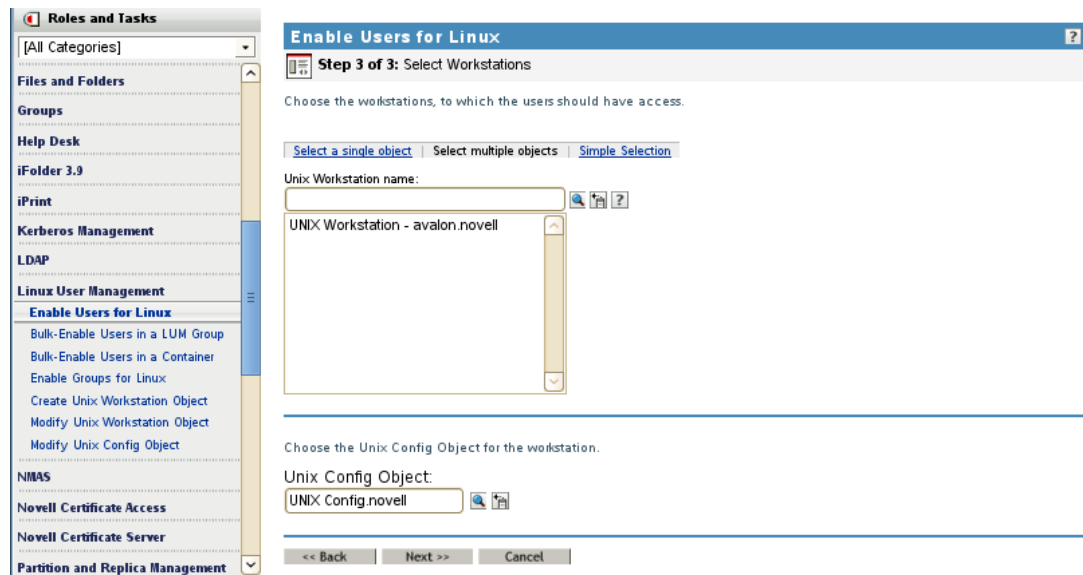
4c Click **Next**.

4d On the **Select Primary Group** page, select **An Existing Linux-Enabled Group**, then browse to locate and select the **admingroup.novell** Group object.



4e Click **Next**.

- 4f On the Select Workstations page, browse to select the UNIXConfig.novell **Unix Config Object** for the workstation.



- 4g Click **Next**.
- 4h On the Summary page, review the LUM settings, then click **Finish**.
- 4i Click **OK** to dismiss the confirmation message.

5.3 Configuring [Public] as a File System Trustee

The [Public] trustee is not an eDirectory object. It is a special trustee that represents any network user, logged in or not, for rights assignment purposes. By making [Public] a trustee of a directory or file, you effectively grant all objects in eDirectory the same trustee rights.

IMPORTANT: For security reasons, you should not provide the file system Supervisor right to the [Public] trustee.

To add the eDirectory [Public] trustee as a file system trustee of a directory:

- 1 Log in to iManager as a user with the **Supervisor** right or **Access Control** right on the NSS volume or NCP volume you want to manage.
- 2 Select the **View Objects** icon at the top of the page.
- 3 On the **Tree** tab, navigate to and select the NSS volume or NCP volume that you want to manage.
- 4 In the right panel, click the directory links to navigate to the directory.
- 5 Select the check box next to the directory of interest, then select **Actions > Properties** to open the directory's Properties page.
- 6 On the directory's Properties page, click the **Rights** tab to view the trustees, trustee rights, and inherited rights filter for the selected directory.

7 Add the eDirectory [Public] trustee as a file system trustee of the directory.

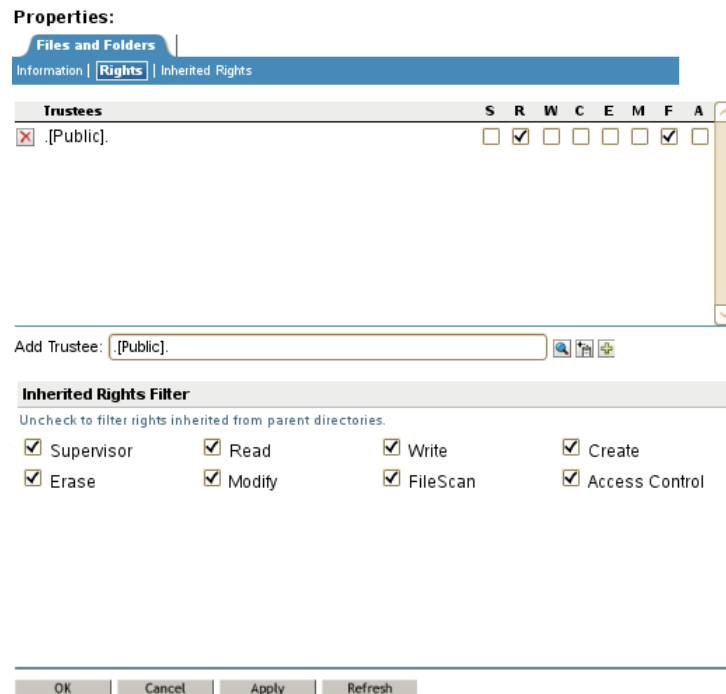
7a Scroll down to the **Add Trustees** field.

7b Type [Public] enclosed in square brackets with a dot before and after, then click the **Add (+)** icon.

For example:

. [Public].

The name appears in the Trustees list, but it is not actually added until you click **Apply** or **OK**. The Read and File Scan trustee rights are assigned by default.



7c (Optional) Add other trustee rights for the . [Public]. trustee by clicking the check box below the right, then click **Apply**.

7d On the Properties page, click **Apply** to save the changes.

8 Click **OK** to close the Properties page.

For an example of how to use the [Public] trustee, see [Section 5.4, “Configuring the \[Public\] Trustee Access Rights on NSS Volumes for Daemons Running as the Nobody User,”](#) on page 45.

5.4 Configuring the [Public] Trustee Access Rights on NSS Volumes for Daemons Running as the Nobody User

Access rights to files and folders on NSS volumes are controlled through the NSS file system trustees and rights set for eDirectory users, not with Linux POSIX rights. The only exception to this is the `root` user, which never has an eDirectory counterpart in order to allow the server to be administered even if eDirectory is not available.

NSS maps the Linux `nobody` user ID to the eDirectory `[Public]` trustee. When you use daemons that run as the `nobody` user to access Linux file system volumes, you typically set the Linux POSIX rights to `777` (`rwX rwX rwX`) in order to grant access to the `nobody` user. However, this does not work on the NSS file system. NSS expects the trustee rights for the `[Public]` trustee to be set up on the target directory and be granted at least the Read and File Scan access rights. This allows NSS to set up the proper NSS and eDirectory authorizations for the `nobody` user, and to provide the `nobody` user ID when interacting with native Linux daemons. Otherwise, the daemon cannot store files on the NSS volume.

The `[Public]` trustee is not an eDirectory object. It is a special trustee that represents any network user, logged in or not, for rights assignment purposes. By making `[Public]` a trustee of a directory or file, you effectively grant all objects in eDirectory the same trustee rights.

IMPORTANT: For security reasons, you should not provide the file system Supervisor right to the `[Public]` trustee.

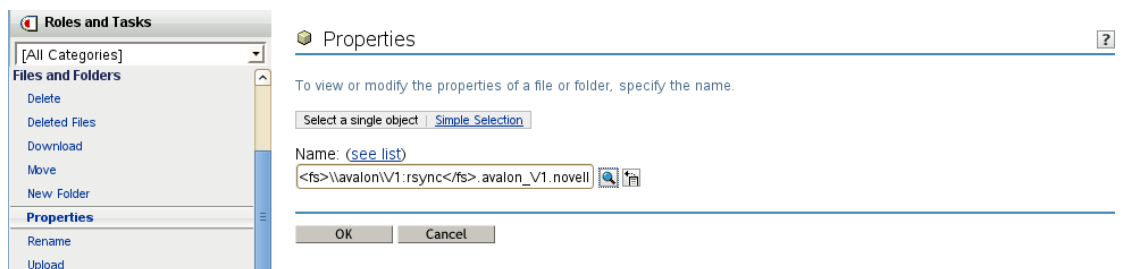
You can use the Files and Folders plug-in in iManager, or the NSS `rights` utility to configure trustees and trustee rights for volumes, directories, or files. For information about setting trustees in iManager, see [Section 6.5, “Using the Files and Folders Plug-In for iManager to Manage Trustees, Trustee Rights, and Inherited Rights,”](#) on page 60. For information about the `rights` utility, see [Section 6.9, “Using the Rights Utility to Set Trustee Rights for the NSS File System,”](#) on page 67. An example of using each method is provided below.

Example: [Public] Trustee Setup for the RSync Daemon

The `rsync` daemon runs as the `nobody` user. In the following example, you want the daemon to access files in the `/media/nss/VOL1/rsync` directory on an NSS volume named `VOL1`. You must assign the eDirectory `[Public]` trustee as a file system trustee of the directory, and give it the Read and File Scan access rights on that directory.

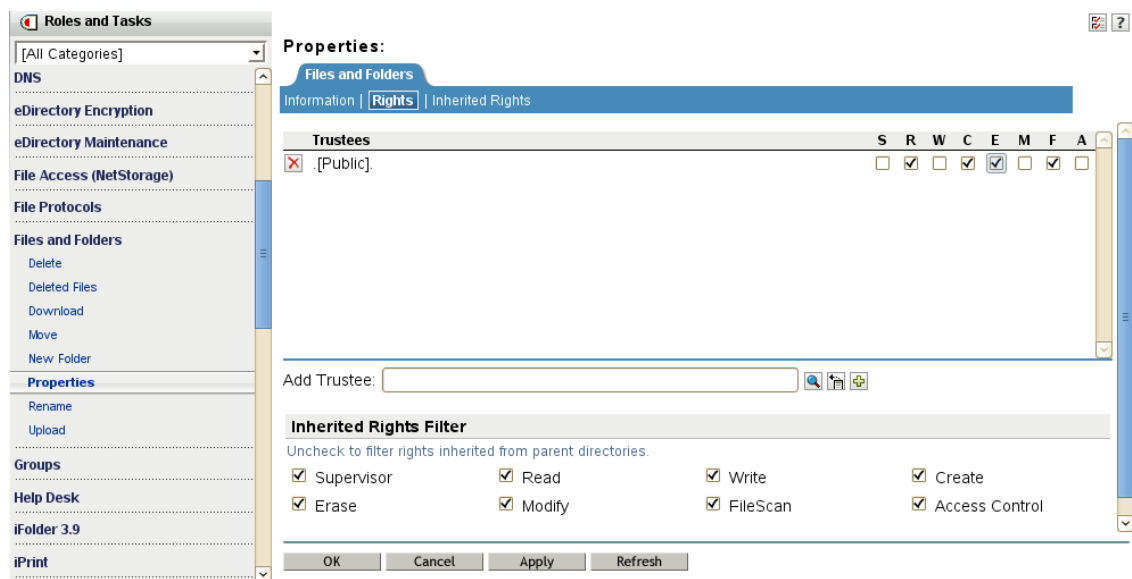
To use the Files and Folders Plug-In to iManager to set up the `[Public]` trustee as a file system trustee:

- 1 In iManager, click **Files and Folders**, then click **Properties** to open the Properties page.
- 2 On the Properties page, browse and select the `VOL1/rsync` directory, then click **OK**.



- 3 On the folder's Properties page, click the **Rights** tab to view the trustees, trustee rights, and inherited rights filter for the selected directory.
- 4 Add the eDirectory [Public] trustee as a file system trustee of the directory.
 - 4a Scroll down to the **Add Trustees** field.
 - 4b Type [Public] enclosed in square brackets with a dot before and after, then click the **Add (+)** icon.
For example:
.[Public].

The name appears in the **Trustees** list, but it is not actually added until you click **Apply** or **OK**. The Read and File Scan trustee rights are assigned by default.
 - 4c On the Properties page, click **Apply** to save the changes.
- 5 (Optional) Add other trustee rights for the .[Public]. trustee by clicking the check box below the right, then click **Apply**.



To use the Rights Utility to set up the [Public] trustee as a file system trustee:

- 1 Log in to the server as the `root` user, then open a terminal console.
- 2 At the console prompt, enter the following commands

```
cd /media/nss/VOL1/rsync

rights trustee "[Public]" -r rf
```

Modify the list of rights in this command to add other rights for the daemon if they are needed. For information about the options, see [Section 6.9, “Using the Rights Utility to Set Trustee Rights for the NSS File System,”](#) on page 67.

- 3 View the rights to verify that the settings are as expected by entering
- ```
rights show
```

The displayed response should be similar to the following:

```
Trustees and Inherited Rights Filter

File: /media/nss/VOL1/rsync

Trustees:
 (1) [Public]
 [read, scan]

Inherited Rights Filter:
 [supervisor, read, write, create, erase, access control, scan, modify]
```

## 5.5 Using QuickFinder with NCP Volumes and NSS Volumes

QuickFinder indexing honors Novell file system trustees and rights in what it returns to the requesting user for NCP volumes and NSS volumes. The user sees only those files that the user has rights to see.

## 5.6 Access Control for NSS on Linux

For an OES 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 POSIX file systems | Yes            | No                             | xNFS Independent |
| NCP/eDirectory, except for Root user | Linux POSIX file systems | No             | Yes                            | xNFS Independent |
| Local and NCP/eDirectory             | Linux POSIX 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 3.2, “Compatibility Issues for Trustee Rights on Linux,” on page 13](#)
- ◆ [“Access Control for NSS” in the \*OES 2018: NSS File System Administration Guide for Linux\*](#)

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 5.8, “Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions,” on page 50](#).

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.

## 5.7 Understanding Directory and File Attributes for NSS 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.

Table 5-2 describes directory and file attributes and whether they are apply to directories, files, or both.

**Table 5-2** Directory and File Attributes for NSS Volumes

| <b>Attribute Code</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                               | <b>Applies to</b>     |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| A                     | Archive Needed identifies files and folders that have been modified since the last backup. This attribute is assigned automatically.                                                                                                                                                                                                             | Directories and files |
| Ci                    | Copy Inhibit prevents users from copying a file. This attribute is works only for clients using Macintosh operating systems to access NSS volumes on NetWare.<br><br>This attribute overrides the trustee Read right and File Scan right. A trustee with the Modify right must disable this attribute to allow the file to be copied.            | 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.                                                                                                                                                                           | Files only            |
| Di                    | Delete Inhibit prevents users from deleting a directory or file.<br><br>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 attribute to allow the directory or file to be deleted. | Directories and files |
| Dm                    | Do Not Migrate prevents directories and files from being migrated from the server's disk to another storage medium.                                                                                                                                                                                                                              | Directories and files |
| Ds                    | Do Not Suballocate prevents data from being suballocated.                                                                                                                                                                                                                                                                                        | Files only            |
| Ex                    | The Execute attribute indicates program files such as .exe or .com.                                                                                                                                                                                                                                                                              | 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.                                                                                                                                                                                                                                                                                                   | Files only            |
| Rw                    | Read/Write allows you to write to a file. All files are created with this attribute.                                                                                                                                                                                                                                                             | Files only            |

| Attribute Code | Description                                                                                                                                                                                   | Applies to            |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 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). This option works only on NetWare.                                                          | Files only            |

## 5.8 Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions

On Linux, NSS displays its eDirectory Read Only (RO), Read/Write (RW), Execute (X), and Hidden (H) attributes for directories and files in the Linux POSIX permission fields. 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. 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 5.7, “Understanding Directory and File Attributes for NSS Volumes,” on page 48](#).

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`.

| NSS Directory and File Attributes Set in eDirectory                  | Displayed as POSIX Permissions (User, Group, Other) | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read Only is enabled.<br>Execute is disabled.<br>Hidden is disabled. | <code>r-- r-- r--</code>                            | <p>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.</p> <p>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.</p> <p>Example: <code>chmod 400</code> has the same result as <code>chmod 444</code></p> <p><code>r-- r-- r--</code></p> <p>The binary value for octal 4 is 100, which corresponds to Read=On, Write=Off, and Execute=Off.</p>                                                          |
| Read Only is enabled.<br>Execute is disabled.<br>Hidden is enabled.  | <code>--- --- ---</code>                            | <p>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.</p> <p>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.</p> <p>Example: <code>chmod 044</code> or <code>chmod 040</code> has the same result as <code>chmod 000</code></p> <p><code>--- --- ---</code></p> <p>The binary value for octal 0 is 000, which corresponds to Read=Off, Write=Off, and Execute=Off.</p> |

| NSS Directory and File Attributes Set in eDirectory | Displayed as POSIX Permissions (User, Group, Other) | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read Only 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Execute is disabled.                                |                                                     | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Hidden is disabled.                                 |                                                     | 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.<br><br>Example 1: <code>chmod 620</code> or <code>chmod 644</code> has the same result as <code>chmod 666</code><br><br><code>rw- rw- rw-</code><br><br>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.<br><br>Example 2: <code>chmod 420</code> or <code>chmod 466</code> has the same result as <code>chmod 444</code><br><br><code>r-- r-- r--</code><br><br>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. |

| NSS Directory and File Attributes Set in eDirectory | Displayed as POSIX Permissions (User, Group, Other) | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read Only is enabled.                               | r-x r-x r-x<br>[XXX]                                | 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.                                                                                                                                                                                                    |
| Execute is enabled.                                 |                                                     | 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.                                                                                                                                                                                                                                        |
| Hidden is disabled.                                 |                                                     | 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: <code>chmod 001</code> , <code>chmod 441</code> , or <code>chmod 401</code> has the same result as <code>chmod 555</code>                                                                                                                                                                                                                                                                 |
|                                                     |                                                     | 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: <code>chmod 622</code> , <code>chmod 700</code> , or <code>chmod 766</code> has the same result as <code>chmod 777</code>                                                                                                                                                                                                                                                                 |
|                                                     |                                                     | 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, <code>chmod 000</code> , <code>chmod 400</code> , and <code>chmod 022</code> have the same result as <code>chmod 555</code>                                                                                                                                                                                                                                              |
|                                                     |                                                     | 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 <code>chmod</code> 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. |
| Read Only 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.                                                                                                                                                        |
| Execute is enabled.                                 |                                                     |                                                                                                                                                                                                                                                                                                                                                                                                      |
| Hidden is disabled.                                 |                                                     |                                                                                                                                                                                                                                                                                                                                                                                                      |

## 5.9 Troubleshooting File Attributes Issues

See the following Technical Information Documents in the Novell Knowledgebase for information about issues with the Delete Inhibit and Rename Inhibit file attributes.

- ♦ *TID 7000323: Unable to Set the Delete Inhibit or Rename Inhibit Flags on OES NSS Directories* (<http://www.novell.com/support/kb/doc.php?id=7000323>)
- ♦ *TID 3796587: Cannot Rename or Delete Files that Were Migrated to OES Linux* (<http://www.novell.com/support/kb/doc.php?id=3796587>)

# 6 Configuring Trustees and File System Attributes

Open Enterprise Server (OES) 11 and later provides the OES Trustee Model to control user access to data on Novell Storage Services (NSS) volumes and NCP (NetWare Control Protocol) volumes. This section discusses how to configure trustees, trustee rights, inherited rights and filters, and file system attributes for directories and files.

For an explanation of the OES Trustee Model, see [“Understanding File System Access Control Using Trustees” on page 27](#).

- ◆ [Section 6.1, “Viewing a Trustee Report for a Directory or File,” on page 55](#)
- ◆ [Section 6.2, “Viewing a Trustee Report for All Directories in a Volume,” on page 56](#)
- ◆ [Section 6.3, “Viewing Properties of a File or Folder in iManager,” on page 56](#)
- ◆ [Section 6.4, “Viewing Properties for a File or Folder with Novell Client,” on page 59](#)
- ◆ [Section 6.5, “Using the Files and Folders Plug-In for iManager to Manage Trustees, Trustee Rights, and Inherited Rights,” on page 60](#)
- ◆ [Section 6.6, “Using Novell NetStorage to Manage Trustees, Trustee Rights, and Inherited Rights,” on page 64](#)
- ◆ [Section 6.7, “Using the Novell Client to Manage Trustees and Trustee Rights,” on page 65](#)
- ◆ [Section 6.8, “Using the Novell Client to Manage Inherited Rights and Filters,” on page 66](#)
- ◆ [Section 6.9, “Using the Rights Utility to Set Trustee Rights for the NSS File System,” on page 67](#)

## 6.1 Viewing a Trustee Report for a Directory or File

- 1 In iManager, use either of the following methods to locate the file or directory and display its properties.
  - ◆ In **Roles and Tasks**, select **Files and Folders > Properties**, then browse to locate and select the file or directory.
  - ◆ In the iManager toolbar, select the **View Objects** icon, browse the **Tree** view to locate and select the file or directory, then select **Actions > Properties**.
- 2 On the Properties page, select the **Rights** tab to view a list of trustees and their rights.

## 6.2 Viewing a Trustee Report for All Directories in a Volume

The NCP Trustee Report in Novell Remote Manager can be used to generate reports for an NSS volume, including a Dynamic Storage Technology shadow volume comprised of two NSS volumes. For information, see “[Generating and Viewing NCP Trustee Reports for NSS Volumes](#)” in the *OES 2018: OES Remote Manager Administration Guide*.

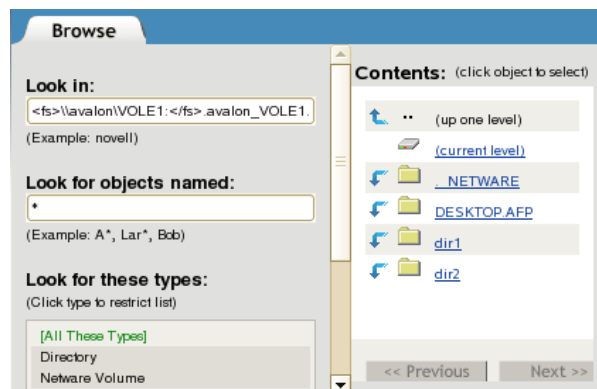
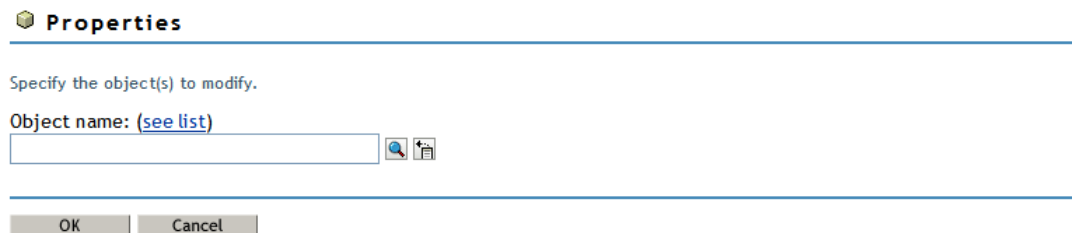
There are currently no supported tools that can generate a trustee report for all directories in an NCP volume on Linux. Check the [Novell Support](http://www.novell.com/support/) website and the [Novell Cool Solutions](http://www.novell.com/cool-solutions/) website for possible solutions that meet your needs. For example, one possible solution is [Display Trustee Assignments](http://www.novell.com/cool-solutions/tools/14092.html).

## 6.3 Viewing Properties of a File or Folder in iManager

- 1 In iManager, use either of the following methods to select a file or folder and open its Properties page:

- ♦ **Files and Folders Role:** In the iManager toolbar, select the **Roles and Tasks** icon. In the left panel, select **Files and Folders > Properties**.

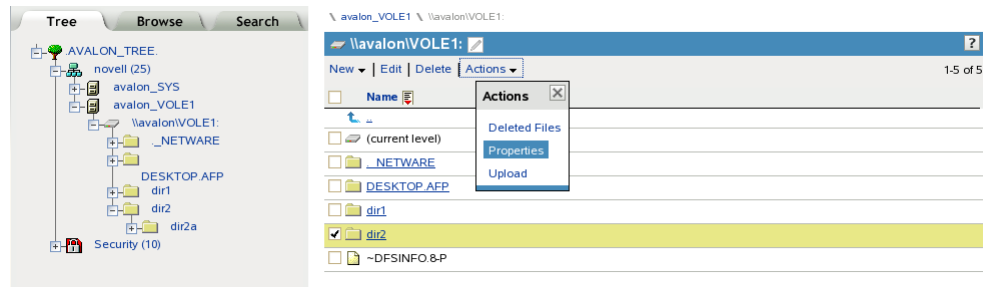
On the Properties page, click the **Search** icon, browse to locate and select the folder you want to manage on an NSS volume, then click **OK** to open the Properties page for the selected folder.





- ◆ **Tree View:** In the iManager toolbar, click **View Objects** icon. In the left panel, browse the Tree to locate and select the folder you want to manage on an NSS volume.

In the right panel, select the check box next to the folder, then select **Actions > Properties**.



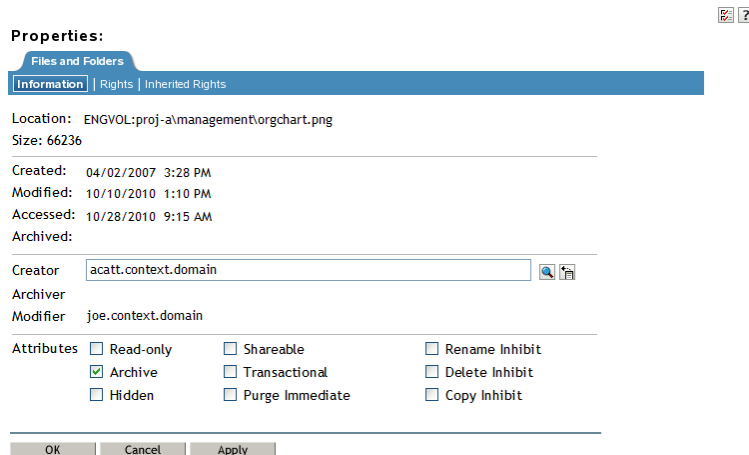
- 2 Use one of the following methods to specify the volume, folder, or file that you want manage:
  - ◆ Click the **Search** icon to browse and locate volume, folder or file from the Storage objects, then click the name link of the object to select it.
  - ◆ Click the **History** icon to select a volume, folder, or file from the list of Storage objects that you recently accessed.

The path name of the object appears in the **Name** field.

- 3 Click **OK** to view the properties for the selected volume, folder, or file.

The properties are displayed in three **Files and Folders** tabs: **Information**, **Rights**, and **Inherited Rights**.

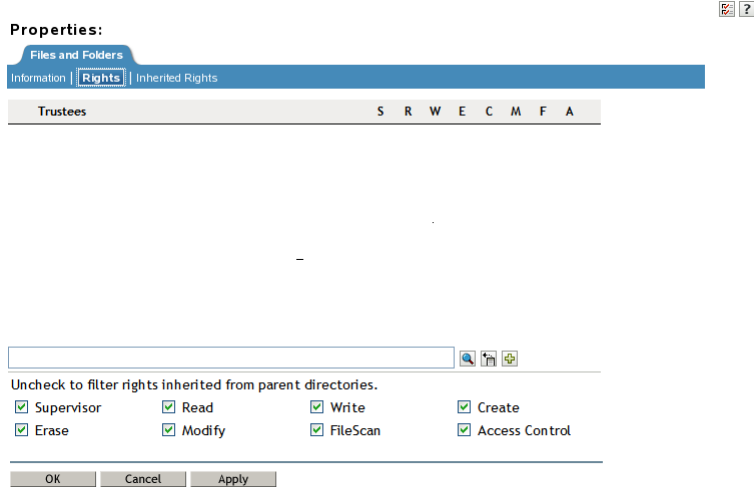
- 4 (Optional) Select the **Information** tab to perform the following tasks:
  - ◆ View details about the selected volume, folder, or file.
  - ◆ Configure directory quotas for folders on NSS volumes where the Directory Quotas attribute is enabled.
  - ◆ Modify the file owner.
  - ◆ Configure file or directory attributes.



See also [Section 12.3, “Viewing or Modifying File System Attributes for NSS Volumes,”](#) on page 107.

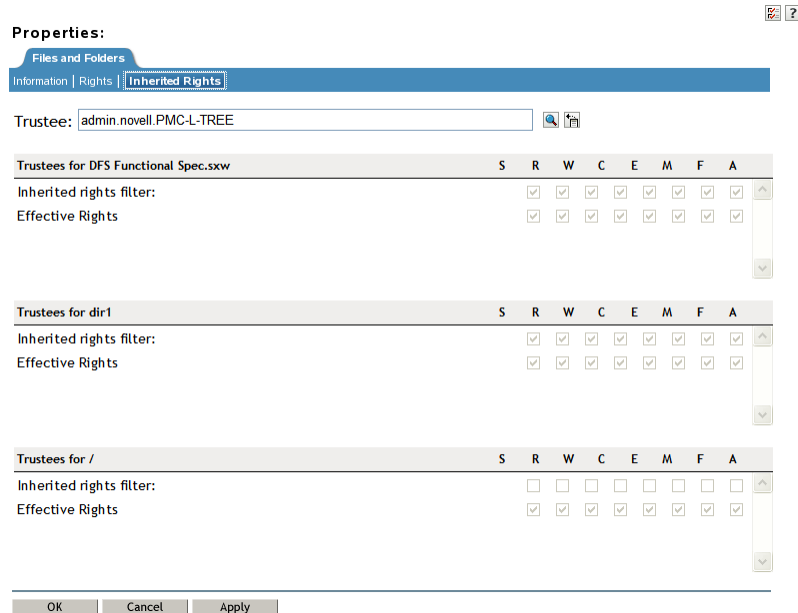
- 5 (Optional) Select the **Rights** tab to perform any of the following tasks:
  - ◆ View details about trustees, trustee rights, and inherited rights filter for the selected volume, folder, or file.

- ◆ Add or remove trustees.
- ◆ Grant or revoke trustee rights for one or multiple trustees.
- ◆ Configure the inherited rights filter.



See also [Section 6.5, “Using the Files and Folders Plug-In for iManager to Manage Trustees, Trustee Rights, and Inherited Rights,”](#) on page 60.

- (Optional) Select the **Inherited Rights** tab to perform the following tasks:
  - ◆ View details about explicitly assigned trustee rights and inherited rights at all levels along the path from the selected file or folder to the `root` of the volume.
  - ◆ View the effective rights for a given trustee for the selected volume, folder, or file.

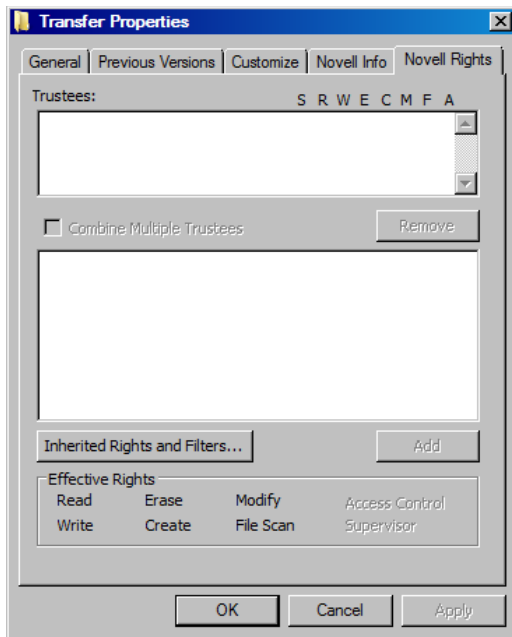


See also [Section 6.5.5, “Viewing Effective Rights for a Trustee,”](#) on page 64.

## 6.4 Viewing Properties for a File or Folder with Novell Client

If the Novell Client is installed on a computer, the file browser is modified to add tabs for Novell Rights. When you select a file or folder that resides on an NSS volume or NCP volume, the fields on the page are populated with its information.

- 1 In a file browser, right-click the file or folder and select **Properties**.
- 2 Click the **Novell Rights** tab to view its **Trustees**, **Trustee Rights**, **Inherited Rights and Filters**, and **Effective Rights**.



Use this page to do any of the following tasks:

- ◆ **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.

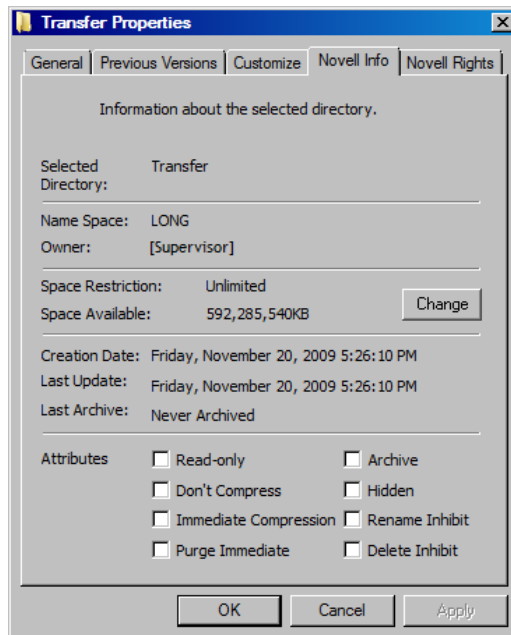
Select one or more trustees from the **Trustees** list, select **Combine Multiple Trustees**, then click **Apply**. The trustees' rights are combined and applied to all selected directories and files. All selected trustees become trustees of all selected directories and files.

- ◆ **Inherited Rights:** Select **Inherited Rights** to open a dialog where you can do 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 Click the **Novell Info** tab to view file system attributes.



For information about the file system properties on this page, see [Step 2 in Section 12.3, “Viewing or Modifying File System Attributes for NSS Volumes,”](#) on page 107.

## 6.5 Using the Files and Folders Plug-In for iManager to Manage Trustees, Trustee Rights, and Inherited Rights

NSS uses the OES Trustee Model for controlling access to user data. As an administrator or a user with the Supervisor right or Access Control right, you can use the Files and Folders plug-in for iManager to manage file system trustees, trustee rights, inherited rights filters, and attributes for a file or folder on an NSS volume. A user who has only the Access Control right cannot modify the Supervisor right of another user.

File system trustees, trustee rights, and inherited rights filters are used to determine access and usage for directories and files on NSS volumes and NCP volumes on OES.

---

**IMPORTANT:** Changes do not take effect until you click **OK** or **Apply**. If you click a different tab before you save, any changes you have made are lost.

---

- ♦ [Section 6.5.1, “Prerequisites,”](#) on page 61
- ♦ [Section 6.5.2, “Viewing, Adding, or Removing File System Trustees,”](#) on page 61
- ♦ [Section 6.5.3, “Viewing, Granting, or Revoking File System Trustee Rights,”](#) on page 62
- ♦ [Section 6.5.4, “Configuring the Inherited Rights Filter for a File or Directory,”](#) on page 63
- ♦ [Section 6.5.5, “Viewing Effective Rights for a Trustee,”](#) on page 64

## 6.5.1 Prerequisites

- ♦ The volume that you want to manage must be in the same tree where you are currently logged in to iManager.
- ♦ You must have trustee rights for the volume, folder, and file that you want to manage.
- ♦ The volume must be a file system that uses the OES Trustee Model for file access, such as an NSS volume or an NCP volume (an NCP share on Ext3, XFS, or Reiser file system).

## 6.5.2 Viewing, Adding, or Removing File System Trustees

A trustee is any eDirectory object (such as a User object, Group object, Organizational Role object, or other container object) that you grant one or more rights for a directory or file. Trustee assignments allow you to set permissions for and monitor user access to data.

- 1 In iManager, click **Files and Folders**, then click **Properties** to open the **Properties** page.
- 2 On the **Properties** page, select a volume, folder, or file to manage, then click **OK**.  
For instructions, see [Section 6.3, "Viewing Properties of a File or Folder in iManager," on page 56](#).
- 3 Click the **Rights** tab to view the trustees, trustee rights, and inherited rights filter for the selected volume, folder, or file.
- 4 To add trustees:

**4a** Scroll down to the **Add Trustees** field.

**4b** Use one of the following methods to add user names as trustees:

- ♦ Click the **Search** icon, browse to locate the user names of the users, groups, or roles that you want to add as trustees, click the name link of the objects to add them to the **Selected Objects** list, then click **OK**.
- ♦ Click the **History** icon to select user names from a list of users, groups, or roles that you recently accessed.
- ♦ Type the typeless distinguished user name (such as `username.context`) in the **Add Trustees** field, then click the **Add (+)** icon.
- ♦ To add the `[Public]` trustee, type `[Public]` with a dot before and after it in the **Add Trustees** field, then click the **Add (+)** icon. For example:

```
.[Public].
```

You might need to explicitly assign the `[Public]` trustee as a file system trustee on a directory in an NSS volume and grant it the Read right and File Scan right if you use daemons that run as the `nobody` user to access files in the directory. Granting trustee rights to the `[Public]` trustee is also required to allow anonymous access to the file system.

The `[Public]` trustee is not an eDirectory object. It is a specialized trustee that represents any network user, logged in or not, for rights assignment purposes. By making `[Public]` a trustee of a volume, directory, or file, you effectively grant all objects in eDirectory the same trustee rights.

---

**IMPORTANT:** For security reasons, you should not provide the file system Supervisor right to the `[Public]` trustee.

---

The user names appear in the Trustees list, but they are not actually added until you click **Apply** or **OK**. By default, each of the user names you add has the Read right and File Scan right assigned.

- 4c** On the **Properties** page, click **Apply** to save the changes.
- 5** To grant or revoke rights for a trustee:

For information about the rights, see [Section 6.5.3, “Viewing, Granting, or Revoking File System Trustee Rights,”](#) on page 62.

  - 5a** In the check boxes next to the trustee name, select the rights you want to grant.
  - 5b** In the check boxes next to the trustee name, deselect the rights you want to revoke.
  - 5c** On the **Properties** page, click **Apply** to save the changes.
- 6** To remove trustees:
  - 6a** Scroll down to locate and select the user name of the user, group, or role that you want to remove as a trustee.
  - 6b** Click the **Remove** (red X) icon next to the user name to remove it as a trustee.

The user name disappears from the list, but it is not actually removed until you click **Apply** or **OK**.
  - 6c** On the **Properties** page, click **Apply** to save changes.

### 6.5.3 Viewing, Granting, or Revoking File System Trustee Rights

Administrator users and users with the Supervisor right or the Access Control right can grant or revoke file system trustee rights for a volume, folder, or file. Only the administrator user or user with the Supervisor right can grant or revoke the Access Control right.

- 1** In iManager, click **Files and Folders**, then click **Properties** to open the **Properties** page.
- 2** On the **Properties** page, select a volume, folder, or file to manage.

For instructions, see [Section 6.3, “Viewing Properties of a File or Folder in iManager,”](#) on page 56.
- 3** Click the **Rights** tab to view the trustees, trustee rights, and inherited rights filter for the selected volume, folder, or file.
- 4** Scroll to locate the user name of the trustee you want to manage.
- 5** In the check boxes next to the trustee name, select or deselect the rights you want to grant or revoke for the trustee.

---

**IMPORTANT:** Changes do not take effect until you click **OK** or **Apply**. If you click a different tab before you save, any changes you have made on this page are lost.

---

| Trustee Right  | Description                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisor (S) | Grants the trustee all rights to the directory or file and any subordinate items.<br><br>The Supervisor right cannot be blocked with an inherited rights filter (IRF) 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.<br><br>Default=Off |

| Trustee Right      | Description                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read (R)           | Grants the trustee the ability to open and read files, and open, read, and execute applications.<br><br>Default=On                                                                                                                                                                                                                              |
| Write (W)          | Grants the trustee the ability to open and modify (write to) an existing file.<br><br>Default=Off                                                                                                                                                                                                                                               |
| Erase (E)          | Grants the trustee the ability to delete directories and files.<br><br>Default=Off                                                                                                                                                                                                                                                              |
| Create (C)         | Grants the trustee the ability to create directories and files and salvage deleted files.<br><br>Default=Off                                                                                                                                                                                                                                    |
| Modify (M)         | 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.<br><br>Default=Off                                                                                                                                                                      |
| File Scan (F)      | 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.<br><br>Default=On                                                                                                                                                         |
| Access Control (A) | Grants the trustee the ability to add and remove trustees for directories and files and modify their trustee assignments and inherited rights filters.<br><br>This right does not allow the trustee to add or remove the Supervisor right for any user. Also, it does not allow to remove the trustee with Supervisor right.<br><br>Default=Off |

6 Click **Apply** or **OK** to save changes.

## 6.5.4 Configuring the Inherited Rights Filter for a File or Directory

File system 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 filter. Only those rights allowed by the filter are inherited by the child object. The effective rights that are granted to a trustee are a combination of explicit rights set on the file or folder and the inherited rights. Inherited rights are overridden by rights that are assigned explicitly for the trustee on a given file or folder.

1 In iManager, click **Files and Folders**, then click **Properties** to open the **Properties** page.

2 On the **Properties** page, select a volume, folder, or file to manage.

For instructions, see [Section 6.3, “Viewing Properties of a File or Folder in iManager,” on page 56](#).

3 Click **Information**, then scroll down to view the inherited rights filter.

The selected rights are allowed to be inherited from parent directories. The deselected rights are disallowed to be inherited.

- 4 In the **Inherited Rights Filter**, enable a right to be inherited from its parent directory by selecting the check box next to it, or disable a right from being inherited by deselecting the check box next to it.
- 5 Click **Apply** or **OK** to save the changes.

## 6.5.5 Viewing Effective Rights for a Trustee

Effective rights are the explicit rights defined for the trustee plus the rights that are inherited from the parent directory. The **Inherited Rights** page shows the inheritance path for a trustee for the selected file or folder and the effective rights at each level from the current file or directory to the root of the volume. You can use this information to help identify at which directory in the path a particular right was filtered, granted, or revoked. Explicit file-system trustee rights override inherited rights. If there are no trustees listed for effective rights, the effective rights are the same as the inherited rights.

- 1 In iManager, click **Files and Folders**, then click **Properties** to open the **Properties** page.
- 2 On the **Properties** page, select a volume, folder, or file to manage.  
For instructions, see [Section 6.3, "Viewing Properties of a File or Folder in iManager," on page 56](#).
- 3 On the **Properties** page, click the **Inherited Rights** tab to view the effective rights for a given trustee.  
By default, the page initially displays the effective rights for the user name you used to log in to iManager.
- 4 On the **Inherited Rights** page, click the **Search** icon next to the **Trustee** field to browse for and locate the user name of the trustee you want to manage, then select the user name by clicking the name link.  
The path for the selected file or folder is traced backwards to the root of the volume. At each level, you can see the rights that have been granted and inherited to create the effective rights for the trustee.
- 5 If you make any changes, click **Apply** or **OK** to save them.

## 6.6 Using Novell NetStorage to Manage Trustees, Trustee Rights, and Inherited Rights

- 1 Open your web browser to NetStorage and log in.
- 2 Right-click the directory or file you want to manage, then select **Properties**.
- 3 Do one or more of the following:
  - ♦ **Add Trustees:** Click the **Novell Rights** tab, click the **eDirectory Object** viewer and brows to select the trustee you want to add, then click **Plus (+)**.
  - ♦ **Remove Trustees:** Click the **Novell Rights** tab, select the **Trustee** check box next to one or more trustees you want to remove, then click **Remove**.
  - ♦ **Modify Trustee Rights:** Click the **Novell 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 5.1, "Understanding the OES Trustee Model for File System Access," on page 27](#).



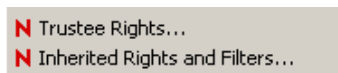
- ◆ **Modify Inherited Rights Filter:** Click the **Novell Rights** tab, select or deselect **Inherited Rights**, then click **Apply**.

For information, see [Section 5.1, “Understanding the OES Trustee Model for File System Access,”](#) on page 27.

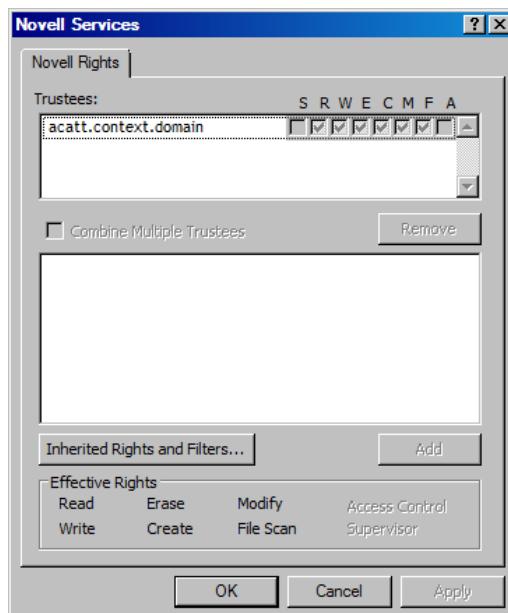
## 6.7 Using the Novell Client to Manage Trustees and Trustee Rights

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 user name 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.

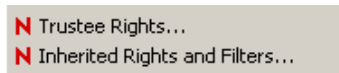
5 When you are done, click **OK** to apply your changes.

## 6.8 Using the Novell Client to Manage Inherited Rights and Filters

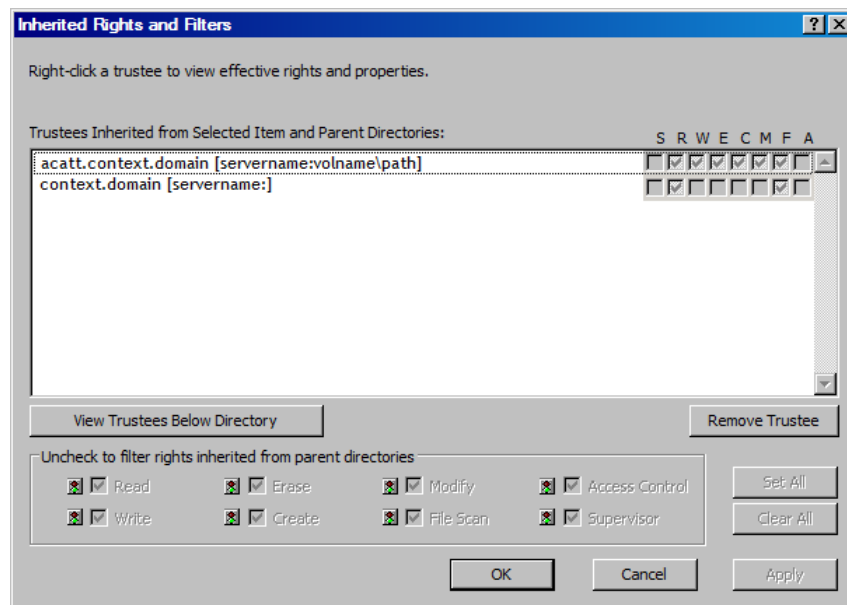
Administrators and users can manage file system inherited rights and filters for network directories and files, using the Novell Client on their workstations. For information about filtering inherited rights, see [Section 5.1.3, "Inherited Trustee Rights,"](#) on page 33.

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**.

## 6.9 Using the Rights Utility to Set Trustee Rights for the NSS File System

The NSS Rights Utility (`rights`) for Linux allows you to specify trustee rights for directories and files in the NSS file system. 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 NetWare. The trustee information is saved in the file and directory metadata in the NSS volume and works seamlessly with NetWare if the volume is moved to a NetWare server.

- ♦ [Section 6.9.1, “Syntax,” on page 67](#)
- ♦ [Section 6.9.2, “Options,” on page 67](#)
- ♦ [Section 6.9.3, “Example,” on page 70](#)
- ♦ [Section 6.9.4, “See Also,” on page 70](#)

### 6.9.1 Syntax

```
rights [OPTIONS]
rights [TOPTIONS] trustee username
rights [DOPTIONS] delete username
rights [IOPTIONS] irf
rights [EROPTIONS] effective username
rights [SOPTIONS] show
```

### 6.9.2 Options

#### ACTIONS

The first argument indicates the action to be taken.

| Option    | Description                                        |
|-----------|----------------------------------------------------|
| trustee   | Adds or modifies a trustee on a file or directory. |
| delete    | Removes a trustee from a file or directory.        |
| irf       | Sets the inherited rights filter on a directory.   |
| effective | Displays a user's effective rights.                |
| show      | Displays the trustees and inherited rights filter. |

## OPTIONS

| Option        | Description                               |
|---------------|-------------------------------------------|
| -v, --version | Displays the program version information. |
| -h, --help    | Displays the help screen.                 |

## TOPTIONS

| Option                      | Description                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r, --rights=MASK           | <p>Specifies the rights to be given to this trustee. For more information, see <a href="#">"MASK" on page 70</a>.</p> <p>If the No Rights (n) option is assigned, the trustee is removed.</p> <p>If rights are not specified, the default assignment is Read and File Scan rights.</p>                   |
| -f, --file= <i>filename</i> | <p>Specifies the name of file or directory to assign trustees to. <i>Filename</i> is the path for the file or directory. For example:</p> <pre>-f /users/username/userfile.sxi</pre> <pre>--file=/designs/topsecret</pre> <p>If a file or directory is not specified, the current directory is used.</p> |
| -S, --softlink              | Do not follow link option.                                                                                                                                                                                                                                                                               |

## DOPTIONS

| Option                      | Description                                                                                                                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -f, --file= <i>filename</i> | <p>Specifies the name of file or directory to delete trustees from. <i>Filename</i> is the path for the file or directory.</p> <p>If a file or directory is not specified, the current directory is used.</p> |
| -S, --softlink              | Do not follow link option.                                                                                                                                                                                    |

## IOPTIONS

| Option                           | Description                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-r, --rights=MASK</code>   | Specifies the rights to be passed through the filter. For more information, see <a href="#">“MASK” on page 70</a> .<br><br>If rights are not specified, the default assignment is All Rights. |
| <code>-f, --file=filename</code> | Specifies the name of the directory where the filter is to be applied. <i>Filename</i> is the path for the directory.<br><br>If a directory is not specified, the current directory is used.  |
| <code>-S, --softlink</code>      | Do not follow link option.                                                                                                                                                                    |

## EROPTIONS

| Option                           | Description                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-f, --file=filename</code> | Specifies the name of file or directory where effective rights are to be calculated. <i>Filename</i> is the path for the file or directory.<br><br>If a file or directory is not specified, the current directory is used. |
| <code>-S, --softlink</code>      | Do not follow link option.                                                                                                                                                                                                 |

## SOPTIONS

| Option                           | Description                                                                                                                                                                          |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-f, --file=filename</code> | Specifies the name of the file or directory to display a list of trustees for that file or directory.<br><br>If a file or directory is not specified, the current directory is used. |
| <code>-S, --softlink</code>      | Do not follow link option.                                                                                                                                                           |

## USERNAME OPTION

The user name is the Fully Distinguished Name of an eDirectory object, including the tree name. Use the `username.context.treename` format, such as

```
joe.engineer.acme_tree
```

If you use special characters in a user name, you must escape those special characters in the command line.

For example, the \$ (dollar sign) is a special character reserved to the shell and must be escaped. For the bash shell, the command could be written in one of two ways on the command line:

```
rights -f /media/nss/DATA/stuff -r none \$j\$o\$e.engineer.acme_tree
```

```
rights -f /media/nss/DATA/stuff -r none 'jo$e.engineer.acme_tree'
```

If you are using another shell, the special characters might need a different escape technique. In this case, please refer to the shell documentation for this information.

## MASK

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

| Right          | Letter | Description                                                                                                                                                                                                                                                            |
|----------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisor     | s      | Has all rights to the file or directory. Also can grant or revoke the Access Control right.                                                                                                                                                                            |
| Read           | r      | Grants the right to open and read files in the directory.                                                                                                                                                                                                              |
| Write          | w      | Grants the right to open and write to files in the directory.                                                                                                                                                                                                          |
| Create         | c      | Grants the right to create files and subdirectories. The user can also salvage (undelete) deleted files.                                                                                                                                                               |
| Erase          | e      | Grants the right to erase files and directories. The user can also purge deleted files.                                                                                                                                                                                |
| Modify         | m      | Grants the right to modify the content of files and directories, and change file attributes.                                                                                                                                                                           |
| File Scan      | f      | Grants the right to display and search on file and directory names in the file system structure.                                                                                                                                                                       |
| Access Control | a      | Grants the right to add and remove trustees, and change trustee rights to files and directories.<br><br>This right does not allow the trustee to add or remove the Supervisor right for any user. Also, it does not allow to remove the trustee with Supervisor right. |
| No Rights      | none   | Revokes all rights.                                                                                                                                                                                                                                                    |
| All Rights     | all    | Grants all rights except Supervisor (rwcemfa)                                                                                                                                                                                                                          |

### 6.9.3 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.

### 6.9.4 See Also

For information about setting file system directory and file attributes, see [“Using the `Attrib` Utility to Set NSS File System Attributes” on page 109](#).

# 7 Managing Effective Rights

The Files and Folders plug-in for iManager provides an Effective Rights Management enhancement in Open Enterprise Server (OES) 11 SP2.

- ♦ [Section 7.1, “Understanding Effective Rights,” on page 71](#)
- ♦ [Section 7.2, “Limitations for Effective Rights and Rights to Files and Folders,” on page 71](#)
- ♦ [Section 7.3, “Viewing Effective Rights,” on page 72](#)
- ♦ [Section 7.4, “Assigning Rights to Files and Folders,” on page 74](#)

To access the online documentation for Novell Storage Services (NSS), see the [OES 2018: NSS File System Administration Guide for Linux](#).

## 7.1 Understanding Effective Rights

The effective rights that are granted to a trustee are a combination of explicit rights set on the file or folder and the inherited rights. Inherited rights are overridden by rights that are assigned explicitly for the trustee on a given file or folder. If there are no trustees listed for effective rights, the effective rights are the same as the inherited rights. The **Inherited Rights** page shows the inheritance path for a trustee for the selected file or folder and the effective rights at each level from the current file or directory to the root of the volume. You can use this information to help identify at which directory in the path a particular right was filtered, granted, or revoked.

For information about the Novell Trustees Model for file access, see [Chapter 5, “Understanding File System Access Control Using Trustees,” on page 27](#).

## 7.2 Limitations for Effective Rights and Rights to Files and Folders

The Novell Trustees Model is used to control file access for NSS volumes and NCP volumes (NCP shares on Linux POSIX file systems). As an administrator (or an administrator-equivalent user) with the Supervisor right or Access Control right, you can use the Files and Folders plug-in for iManager to manage file system trustees, trustee rights, and inherited rights filters for a file or folder on an NSS volume or NCP volume. A user who has only the Access Control right cannot modify the Supervisor right of another user. The administrator (or administrator equivalent user) must be enabled for Linux with Linux User Management (LUM) (that is, LUM-enabled) in order to view effective rights.

The following limitations apply for effective rights management:

- ♦ It is not supported to view the effective rights on non-NSS and non-NCP volumes.
- ♦ It is not supported to view the soft-linked files or folders in a volume by using the **Files and Folders > Properties** option in iManager.
- ♦ You see the primary file when rights are modified for hard linked files.

- ♦ It is not supported to view the effective rights directly on the secondary volume of a DST shadow volume pair. You must use the merged view to manage effective rights for files and folders on the DST shadow volume pair. DST stores the rights settings on the primary volume and copies the settings to the secondary volume. DST applies the primary volume's rights settings to files whether they physically reside on the primary volume or secondary volume.
- ♦ Modifying rights for DFS junctions is disabled in this interface. Use DFS tasks in iManager to manage rights on DFS junctions.

## 7.3 Viewing Effective Rights

Users can receive rights in a number of ways, such as explicit trustee assignments, inheritance, and security equivalence. Rights can also be limited by inherited rights filters and changed or revoked by lower trustee assignments. The net results of all these actions—the rights a user can employ—are called effective rights. Effective rights can be viewed by administrators who are enabled for Linux with Linux User Management (LUM) (that is, they must be LUM-enabled).

---

**NOTE:** Ensure that you LUM-enable the non-default administrators for viewing effective rights.

---


Effective rights information includes the following:

- ♦ **Server:** The name of the server where the file, folder, or volume exists along with the trustee information.
- ♦ **Location:** The location of the file, folder, or volume.
- ♦ **Trustees:** The list of trustees and their effective rights.

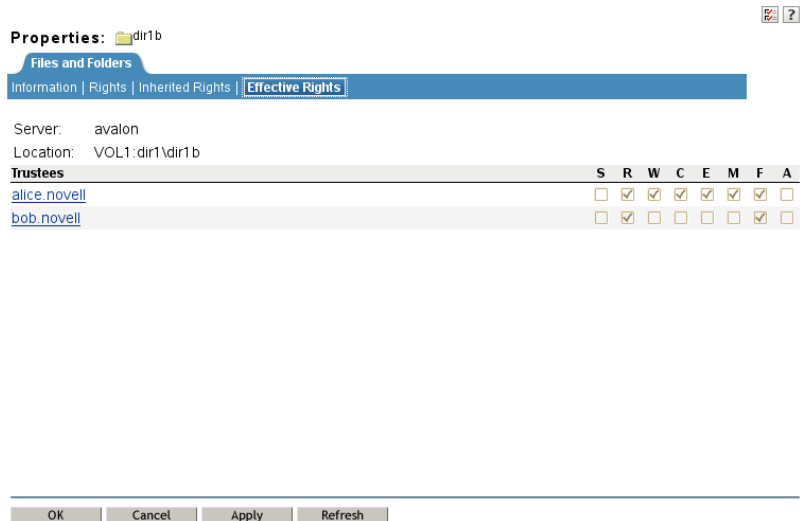
To view or modify the effective rights of trustees for a particular folder or file:

- 1 In iManager, click **Files and Folders > Properties** to open the Properties page.

You can also access the Properties page for a file or folder from the Tree View page. Browse the tree to locate the file or folder, click the check box next to the object, then click **Actions > Properties**.

- 2 Click the **Search**  (**Object Selector**) icon to browse the Storage objects, locate and select the name link of the file or folder you want to manage, then click **OK** to view the properties for the file.
- 3 Click the **Effective Rights** tab to view the list of trustees and their effective rights on the chosen folder or file.





- Click a trustee name to view a list of all files and folders on the selected volume where that user has been assigned rights explicitly.



- (Optional) On the Rights to Files and Folder page, modify the rights, then click **Apply**.
- Return to the Effective Rights page to view the modified effective rights for the trustee.

## 7.4 Assigning Rights to Files and Folders

This section describes the procedures to assign or modify rights to a user or a group on a set of files and folders.

Rights to file and folder information include the following:



**Modify User:** The name of the selected trustee.

**Volume:** The selected volume name.

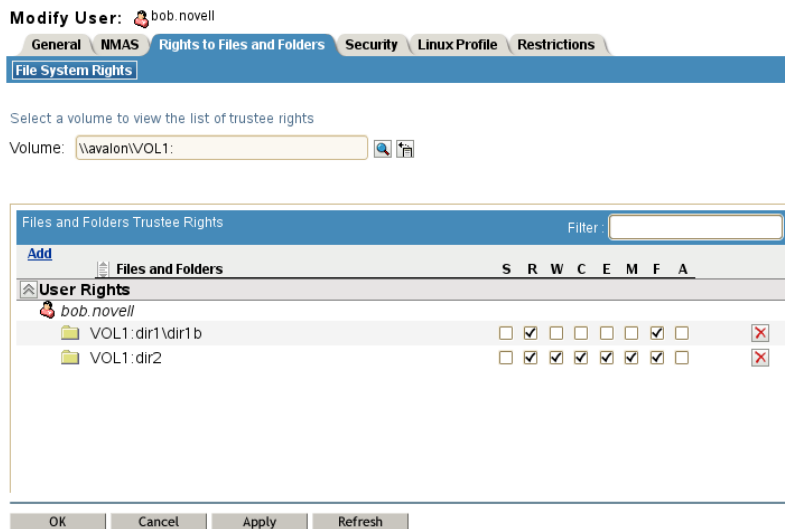
**Add File or Folder:** You can choose the files or folders on the selected volume that the selected trustee is allowed to use. The selected files are added to the list under Files and Folders.

**Files and Folders:** The files and folders that the selected trustee is allowed to use. You can assign or modify the rights for the selected trustee on each file or folder.

To add or modify rights of the trustee on files or folders:


- 1 In iManager, click **Users > Modify User** to open the Modify User page.
- 2 Click the  (**Object Selector**) icon to browse and select an admin user objects, then click **OK**.
- 3 Click the **Rights to Files and Folders** tab to view the File System Rights page.
- 4 Under Volume, use the  (**Object Selector**) icon to select the volume.

Only the files and folders that are part of the selected volume and where rights were explicitly assigned for the selected user are listed under **Files and Folders**.



- 5 (Optional) Click **Add**, then browse to select files or folders where you want to assign rights for this user.

The selected files and folders are added to the list with the default rights of Read and File Scan.

- 6 (Optional) In Files and Folders section in the **Rights** check boxes for a file or folder, select the check box to assign a right or deselect a check box to remove the right, then click **Apply**.
- 7 (Optional) In Files and Folders section next to the rights for a file or folder, click the **Delete** icon  to remove a file or a folder from the list, then click **Apply**.

# 8

# Understanding Directory Structures for the NSS File System

This section describes the following key concepts for the Novell Storage Services (NSS) File System for Open Enterprise Server (OES) 11 and later servers:

- ◆ [Section 8.1, “Directory Structures,” on page 75](#)
- ◆ [Section 8.2, “Directory Path,” on page 76](#)
- ◆ [Section 8.3, “Root Directory,” on page 76](#)
- ◆ [Section 8.4, “Drive Map,” on page 76](#)

## 8.1 Directory Structures

The NSS file system provides 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.

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.

Volumes are similar to drawers in an office filing cabinet that contain related information. For example, volumes might contain applications, corporate data, or user home directories and files.

To control who can access directories and files on your NSS file system, you must assign file system trustees, trustee rights, and inherited rights filters. For information, see [Section 5.1, “Understanding the OES Trustee Model for File System Access,” on page 27](#).

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

- ◆ [Section 5.7, “Understanding Directory and File Attributes for NSS Volumes,” on page 48](#)
- ◆ [Section 5.8, “Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions,” on page 50](#)

## 8.2 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. 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.

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.

## 8.3 Root Directory

The root directory is the base directory in the volume. The root directory of a volume typically contains only directories and only the administrator has rights at that level.

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 Using Trustees” on page 27](#).

## 8.4 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, or use the mapping functionality of your client operating system. The network drive map is valid only until you log out.

# 9 Managing Files and Folders

This section discusses how to create, modify, or remove files and folders for Novell Storage Services (NSS) volumes and NCP (NetWare Core Protocol) volumes on Open Enterprise Server (OES) 11 and later servers.

---

**IMPORTANT:** The instructions in this section focus primarily on the Files and Folders role in iManager. Many of the tasks can be performed natively in a file browser if you map the volume or a network share on the volume to a local drive letter on your computer.

---

- ♦ [Section 9.1, “Creating a Folder on an NSS Volume or NCP Volume,” on page 77](#)
- ♦ [Section 9.2, “Moving a File or Folder to a Different Folder on the Same Volume,” on page 79](#)
- ♦ [Section 9.3, “Renaming a File or Folder on an NSS Volume or NCP Volume,” on page 80](#)
- ♦ [Section 9.4, “Deleting a File or Folder on an NSS Volume or NCP Volume,” on page 81](#)
- ♦ [Section 9.5, “Uploading Files to an NSS Volume or NCP Volume,” on page 81](#)
- ♦ [Section 9.6, “Downloading Files from an NSS Volume or NCP Volume,” on page 82](#)
- ♦ [Section 9.7, “Mapping Network Drives,” on page 83](#)

## 9.1 Creating a Folder on an NSS Volume or NCP Volume

- ♦ [Section 9.1.1, “Prerequisites for Creating Folders,” on page 77](#)
- ♦ [Section 9.1.2, “Tools for Creating Folders,” on page 78](#)
- ♦ [Section 9.1.3, “Creating a Folder with iManager,” on page 78](#)

### 9.1.1 Prerequisites for Creating Folders

Before you can create a folder (directory) on an NSS volume, you must be a trustee of the parent folder where you want to create the new folder, and have been granted the Create right for it. When creating a folder in the root directory of a volume, you must be a trustee the Volume object and have the Create right for it. For information about assigning trustees and trustee rights, see [Chapter 6, “Configuring Trustees and File System Attributes,” on page 55](#).

## 9.1.2 Tools for Creating Folders

For OES servers, you can create folders by using the following management tools for NSS volumes and NCP volumes:

*Table 9-1 Tools for Creating Folders on NSS and NCP Volumes*

| Management Tool                                           | NSS on Linux | NCP Volumes on Linux POSIX File Systems |
|-----------------------------------------------------------|--------------|-----------------------------------------|
| Files and Folders plug-in for iManager 2.7                | Yes          | Yes                                     |
| Novell Client for Linux                                   | Yes          | Yes                                     |
| Novell Client for Windows XP/2003 and for Windows Vista/7 | Yes          | Yes                                     |
| Novell NetStorage                                         | Yes          | Yes                                     |
| Novell Remote Manager for Linux                           | No           | No                                      |

## 9.1.3 Creating a Folder with iManager

As an administrator, you can use the Files and Folders plug-in to iManager to create a folder on NSS volumes and NCP volumes (NCP shares on Linux POSIX file systems such as Ext3, XFS, and Reiser).

- ♦ [“Prerequisites” on page 78](#)
- ♦ [“Procedure” on page 78](#)

### Prerequisites



- ♦ The destination NSS volume must be in the same tree where you are currently logged in to iManager.
- ♦ You must have trustee rights for the volume and destination location where you want to create the new folder. The Create right is required for creating files and folders.

### Procedure

- 1 In iManager, click **Files and Folders**, then click **New Folder** to open the **New Folder** page.

New Folder ?

Specify the path and name for the new folder.

Path:   

Folder Name:

- 2 Use one of the following methods to specify the destination path on the NSS volume where you want to create the new folder:
  - ♦ Click the **Search** icon to browse and locate the destination folder, then click the name link of the folder to select it.
  - ♦ Click the **History** icon to select a folder from the list of folders that you recently accessed.
 The path name of the folder appears in the **Path** field.
- 3 In **Folder Name**, type the name the folder you want to create in the selected location.
- 4 Click **OK** to create the folder, or click **Cancel** to abandon it.
 

A message confirms when the folder has been successfully created.
- 5 Click **Repeat Task** to create another folder, or click **OK** to dismiss the confirmation message.
- 6 Click **Files and Folders**, then click **Properties** to set file system trustees, trustee rights, and attributes for the new folder or folders.

## 9.2 Moving a File or Folder to a Different Folder on the Same Volume

You can use the Files and Folders plug-in for iManager to move a file or folder to a different folder on the same volume.

- ♦ [Section 9.2.1, “Prerequisites,” on page 79](#)
- ♦ [Section 9.2.2, “Procedure,” on page 79](#)

### 9.2.1 Prerequisites

You must have the Create and Modify trustee rights for the file or folder that you want to move and for the target folder where you want to move it. You must also have the Erase right to the source directory, because moving files includes deleting them from the source directory.

### 9.2.2 Procedure

- 1 In iManager, select **Files and Folders > Move**.

The screenshot shows a dialog box titled "Move" with a help icon in the top right corner. Below the title bar, the text "Specify a file to move." is displayed. There are two input fields: "File Name:" and "Folder Name:". Each input field has a search icon and a folder icon to its right. At the bottom of the dialog, there are "OK" and "Cancel" buttons.

- 2 Use one of the following methods to select the file that you want to move:
  - ♦ Click the **Search** icon to browse and locate the file or folder, then click its **Name** link to select it.
  - ♦ Click the **History** icon to select a file or folder from the list of files or folders that you recently accessed.

- 3 Click **Browse** to open a local **File Browser** dialog box. Browse to locate and select the folder where you want to move the file, then click **Open**.

The path name for the selected folder appears in the **Folder Name** field.

- 4 Click **OK** to begin the move, or click **Cancel** to discard the changes.

A message confirms that the file has been successfully moved. Wait until the move completes before proceeding to other tasks.

## 9.3 Renaming a File or Folder on an NSS Volume or NCP Volume

You can use the Files and Folders plug-in for iManager to rename a file or folder on an NSS volume.

- ♦ [Section 9.3.1, “Prerequisites,” on page 80](#)
- ♦ [Section 9.3.2, “Procedure,” on page 80](#)

### 9.3.1 Prerequisites

You must have the Create and Modify trustee rights for the file or folder in order to be able to find and rename it. You must also have the Erase right to the source directory, because renaming a file includes deleting the old file name from the source directory.

### 9.3.2 Procedure

- 1 In iManager, select **Files and Folders > Rename**.

Rename ?

Specify a file or folder to rename.

File Name:   

New name

- 2 Use one of the following methods to select the file that you want to rename:
  - ♦ Click the **Search** icon to browse and locate the file or folder, then click its **Name** link to select it.
  - ♦ Click the **History** icon to select a file or folder from the list of files or folders that you recently accessed.

The path name appears in the Path field.

- 3 Type the new name in the **New Name** field.
- 4 Click **OK** to rename the file, or click **Cancel** to discard the changes.

A message confirms that the file has been successfully renamed. Wait until the rename completes before proceeding to other tasks.



## 9.4 Deleting a File or Folder on an NSS Volume or NCP Volume

As an administrator, you can use the Files and Folders plug-in to iManager to delete a file or folder on an NSS volume.

- ◆ [Section 9.4.1, “Prerequisites,” on page 81](#)
- ◆ [Section 9.4.2, “Procedure,” on page 81](#)

### 9.4.1 Prerequisites

- ◆ The NSS volume must be in the same tree where you are currently logged in to iManager.
- ◆ You must have trustee rights for the file or folder that you want to delete. The Erase right is required to delete the file.

### 9.4.2 Procedure

- 1 In iManager, click **Files and Folders**, then click **Delete** to open the **Delete File or Folder** page.



Delete File or Folder ?

Specify a file or folder to delete.

Name:   

OK Cancel

- 2 Use one of the following methods to specify the file or folder that you want to delete from the NSS volume:
  - ◆ Click the **Search** icon to browse and locate the file or folder, then click the name link of the object to select it.
  - ◆ Click the **History** icon to select a file or folder from the list of files and folders that you recently accessed.The path name of the folder appears in the **Name** field.
- 3 Click **OK** to delete the selected file or folder, or click **Cancel** to abandon the delete process. A message confirms when the file or folder has been successfully deleted.
- 4 Click **Repeat Task** to delete another folder, or click **OK** to dismiss the confirmation message.

## 9.5 Uploading Files to an NSS Volume or NCP Volume

As an administrator, you can use the Files and Folders plug-in to iManager to upload files from your local computer to an existing folder on an NSS volume.

- ◆ [Section 9.5.1, “Prerequisites,” on page 82](#)
- ◆ [Section 9.5.2, “Procedure,” on page 82](#)

## 9.5.1 Prerequisites

- ♦ The destination NSS volume must be in the same tree where you are currently logged in to iManager.
- ♦ You must have trustee rights for the destination folder in order to be able to find the folder and upload the file. The Create right is required for file uploads.

## 9.5.2 Procedure

- 1 In iManager, click **Files and Folders**, then click **Upload** to open the **Upload File** page.

The screenshot shows the 'Upload File' dialog box. At the top, it says 'Upload File' with a help icon. Below that, it says 'Specify the uploaded path and the file to upload.' There are two input fields: 'Path:' and 'File Name:'. The 'Path:' field has a search icon and a history icon. The 'File Name:' field has a 'Browse...' button. At the bottom, there are 'OK' and 'Cancel' buttons.

- 2 Use one of the following methods to specify the path to the folder on the NSS volume where you want to put the file:
  - ♦ Click the **Search** icon to browse and locate the folder, then click the name link of the folder to select it.
  - ♦ Click the **History** icon to select a folder from the list of folders that you recently accessed.

The path name appears in the Path field.

- 3 Select the file on your local computer that you want to upload:

- 3a Click **Browse** to open a local file browser dialog box.
- 3b Browse and locate the file.
- 3c Select the file, then click **Open**.

The local path name for the selected file appears in the **File Name** field.

- 4 Click **OK** to begin the upload, or click **Cancel** to abandon the process.

A message confirms when the file has been successfully uploaded. Wait until the upload completes before proceeding to other tasks.

- 5 Click **Repeat Task** to upload another file, or click **OK** to dismiss the confirmation message.

## 9.6 Downloading Files from an NSS Volume or NCP Volume

As an administrator, you can use the Files and Folders plug-in to iManager to download a file from an NSS volume or NCP volume to your local computer.

- ♦ [Section 9.6.1, “Prerequisites,” on page 83](#)
- ♦ [Section 9.6.2, “Procedure,” on page 83](#)

## 9.6.1 Prerequisites

- ♦ The NSS volume must be in the same tree where you are currently logged in to iManager.
- ♦ You must have trustee rights for the file in order to be able to browse to and download the file.

## 9.6.2 Procedure

- 1 In iManager, click **Files and Folders**, then click **Download** to open the **Download File** page.



- 2 Use one of the following methods to select the file that you want to download from the NSS volume to your local drive:
  - ♦ Click the **Search** icon to browse and locate the file, then click the name link of the file to select it.
  - ♦ Click the **History** icon to select a file from the list of files that you recently accessed.

The path name appears in the **File Name** field.

- 3 Click **OK** to open the **File Download** dialog box.

---

**IMPORTANT:** If the File Download dialog box does not open, ensure that the security settings in your browser allow downloads from the server by adding the server as a trusted site, then try again.

---

- 4 Use one of the following methods to save the file to the local computer:
  - ♦ Click **Open** to view the file in an appropriate application, then save the file by using the application's **File > Save** options.

The application that opens the file must already be installed on your computer.
  - ♦ Click **Save** to open the **Save As** dialog box, browse to an existing folder or create a new local folder where you want to save the file, then click **Save**.

The browser's download manager manages the download and notifies you when the download is complete.

You can continue with other iManager tasks while the file is downloading.

## 9.7 Mapping Network Drives

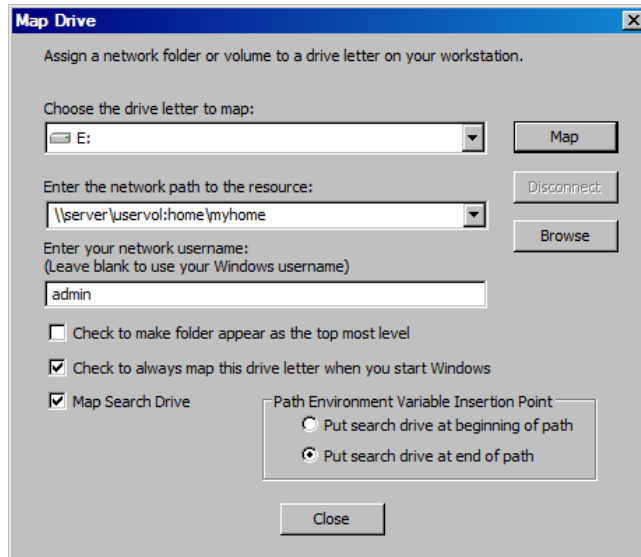
You can map a network drive to your local computer in order to create, modify, and remove files in your file browser. Mapping a drive with the Novell Client additionally provides the ability to set trustees, trustee rights, and file system attributes for NSS and NCP volumes.

- ♦ [Section 9.7.1, "Using Novell Map Network Drive," on page 84](#)
- ♦ [Section 9.7.2, "Using Map Network Drive in Windows Explorer," on page 85](#)

## 9.7.1 Using Novell Map Network Drive

The Novell Client provides a tool to map drives on NSS and NCP volumes for NCP access.

- 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 user name. If necessary, the client later prompts you for the password that matches the server login user name 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**.

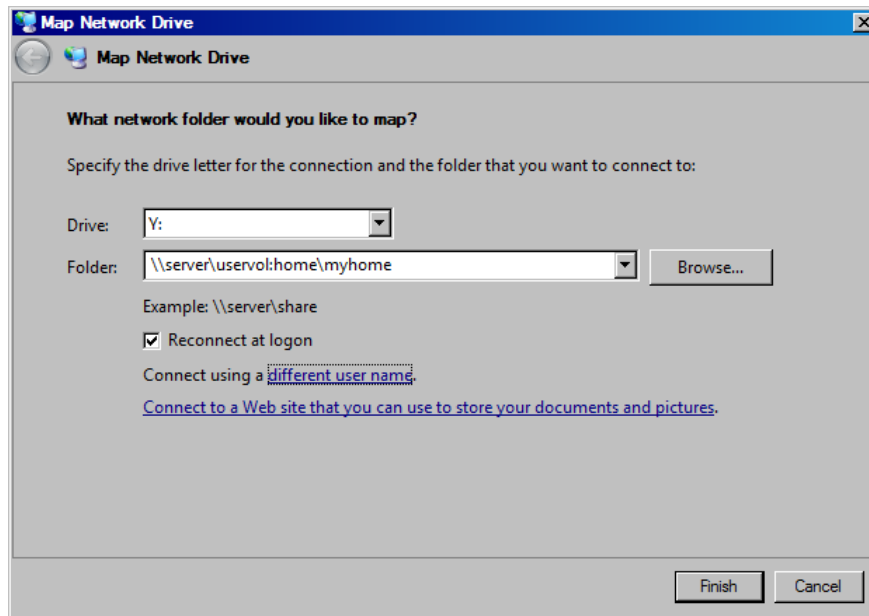
For more information, see the following:

- ♦ [“Configuring Map Settings”](#) in the *Novell Client 2.0 SP3 for Linux Administration Guide*
- ♦ [Novell Login Scripts Guide](#)

## 9.7.2 Using Map Network Drive in 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**.



# 10 Managing Directory Quotas on NSS Volumes

A directory quota limits the amount of space on a Novell Storage Services (NSS) volume that can be consumed by all of the files and folders in that directory. If the value you specify exceeds the volume quota, the volume quota overrides the directory quota. If the current size of the directory exceeds the specified limit, users cannot save data to the directory until space is cleared by removing files from the directory.

Before you can set directory quotas, you must enable the volume's Directory Quotas attribute. As the administrator user, you can view and configure directory quotas with the Files and Folders plug-in for iManager, NetStorage, and the Novell Client.

This section discusses how to configure directory quotas for folders on NSS volumes.

- ◆ [Section 10.1, “Setting the Directory Quotas Attribute for an NSS Volume,” on page 87](#)
- ◆ [Section 10.2, “Setting a Directory Quota in iManager,” on page 88](#)
- ◆ [Section 10.3, “Setting a Directory Quota with Novell NetStorage,” on page 90](#)
- ◆ [Section 10.4, “Setting a Directory Quota with the Novell Client,” on page 90](#)
- ◆ [Section 10.5, “Removing a Directory Quota,” on page 91](#)
- ◆ [Section 10.6, “Removing All Directory Quotas for an NSS Volume,” on page 92](#)
- ◆ [Section 10.7, “Using the Quota Utility to Set Directory and User Space Quotas on NSS Volumes,” on page 92](#)

## 10.1 Setting the Directory Quotas Attribute for an NSS Volume

Before setting directory quotas on an NSS volume, you must enable the Directory Quotas attribute for the volume. You can set the attribute at create time or at any time for an existing volume.

To set the Directory Quotas attribute for an existing volume:

- 1 In iManager, click **Storage > Volumes**.
- 2 Select a server to manage to view a list of NSS volumes on the server.
- 3 In the **Volumes** list, select a volume that you want manage.  
Wait for the volume details to be displayed before you continue.
- 4 Click **Properties**.  
The **Properties** page has three tabs: **Attributes**, **Statistics**, and **Quota Usage**. It opens to the **Attributes** tab.
- 5 On the **Attributes** tab, select or deselect the **Directory Quotas** check box, then click **Apply**.
- 6 If you enabled or disabled the **Directory Quotas** attribute, restart NCP2NSS by entering the following at a terminal console prompt:

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

## 10.2 Setting a Directory Quota in iManager

1 In iManager, use either of the following methods to select a file or folder and open its Properties page:

- ♦ **Files and Folders Role:** In the iManager toolbar, select the **Roles and Tasks** icon. In the left panel, select **Files and Folders > Properties**.

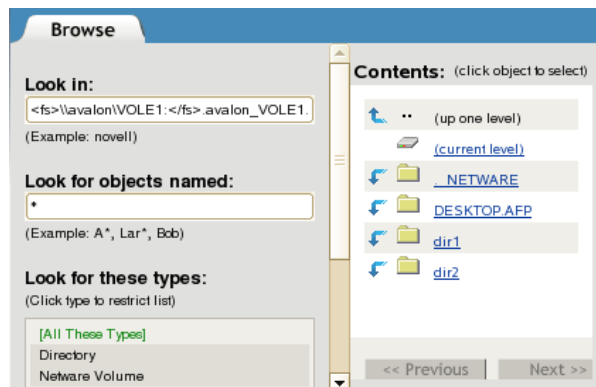
On the Properties page, click the **Search** icon, browse to locate and select the folder you want to manage on an NSS volume, then click **OK** to open the Properties page for the selected folder.

### Properties

Specify the object(s) to modify.

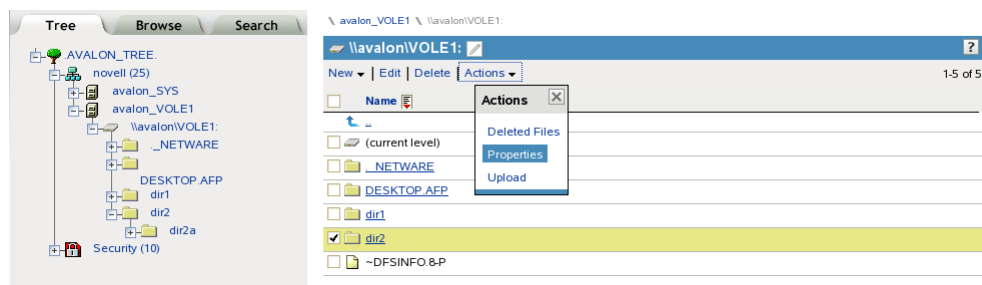
Object name: [\(see list\)](#)

OK Cancel



- ♦ **Tree View:** In the iManager toolbar, click **View Objects** icon. In the left panel, browse the Tree to locate and select the folder you want to manage on an NSS volume.

In the right panel, select the check box next to the folder, then select **Actions > Properties**.





- On the Properties page, view the current status of the Directory Quota on the selected folder.  
If a Directory Quota is set, the **Restrict Size** field is selected and the **Limit** fields show the quota size in KB, MB, GB, or TB.

**Properties:**

Files and Folders

Information | Rights | Inherited Rights

Server: avalon  
Location: VOLE1:dir2

Restrict size

Limit

If the Directory Quota is not set, the **Restrict Size** field is deselected and the **Limit** fields are dimmed (not available).

**Properties:**

Files and Folders

Information | Rights | Inherited Rights

Server: avalon  
Location: VOLE1:dir2

Restrict size

Limit

- (Optional) Set or modify a Directory Quota on the selected folder:
  - Add a Quota:** Select the **Restrict Size** check box to enable space restrictions for the selected directory. In the **Limit** field, type the quota value, then select whether this is KB, MB, GB, or TB from the Units drop-down list.
  - Modify an Existing Quota:** In the **Limit** field, type the new directory quota, then select whether this is KB, MB, GB, or TB from the Units drop-down list.

**Properties:**

Files and Folders

Information | Rights | Inherited Rights

Server: avalon  
Location: VOLE1:dir2

Restrict size

Limit

Created: Tue Oct 26 12:28 2010  
Modified: Tue Oct 26 13:18 2010

- (Optional) Remove a directory quota by deselecting the **Restrict Size** check box.  
This disables space restrictions for the selected folder. The **Limit** fields are automatically dimmed (not available).
- At the bottom of the **Properties Information** page, click **Apply** or **OK** to apply the changes.

## 10.3 Setting a Directory Quota with Novell NetStorage

Using Novell NetStorage, you can manage directory quotas for directories in an NSS volume from any computer with a supported web browser. This requires you to first configure a NetStorage server in the same context. For information, see the [OES 2018: NetStorage Administration Guide for Linux](#).

To create or modify NSS directory quotas with NetStorage:

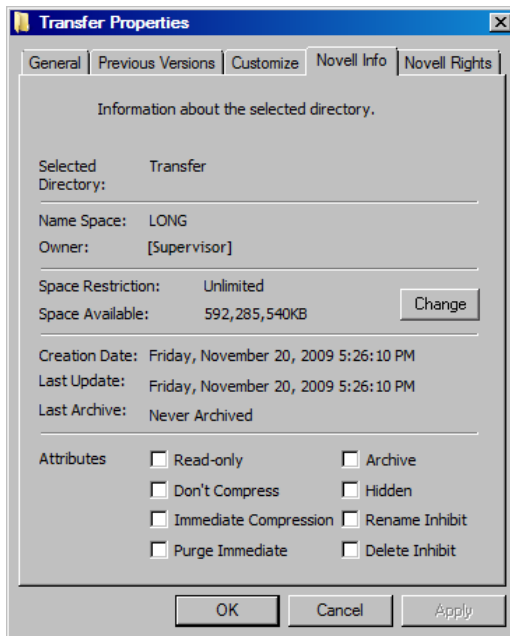
- 1 In a web browser, connect to NetStorage.
- 2 Log in to NetStorage with the user name and password of the Admin user or equivalent user.
- 3 Navigate to the directory you want to manage.
- 4 Right-click the directory, then select **Properties**.
- 5 Click the **Novell Info** tab.
- 6 Do one of the following to configure the directory quota:
  - ♦ **Space Restriction:** Select **Restrict Size**, then specify the directory quota in KB. The value must be a multiple of 4.
  - ♦ **No Space Restriction:** Deselect **Restrict Size** to set the directory quota to Unlimited.
  - ♦ **Complete Space Restriction:** Select **Restrict Size**, then specify the directory quota as 0 KB. If the directory already contains files and subdirectories, the directory cannot grow beyond the current space consumed.
- 7 Click **Apply** to accept the directory quota configuration.

## 10.4 Setting a Directory Quota with the Novell Client

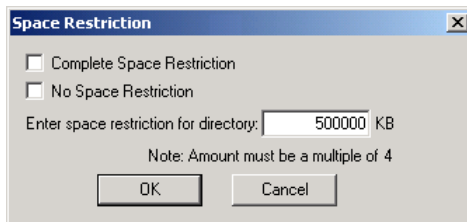
The Novell Client allows the admin user to manage directory quotas for directories in an NSS volume.

- 1 In the Novell Client, map a drive to the NSS directory you want to manage, or map to its parent directory.
  - 1a Right-click the **Novell Client** icon (the red N icon in the notification area), then select **Novell Map Network Drive**.
  - 1b Specify the network path to the directory. For example: `192.168.1.1/users`.
  - 1c Specify the user name of the Admin user or equivalent user, then click **Map**.
  - 1d When prompted, enter the user's password.

- 2 In a file browser, locate and right-click the directory you want to manage, then click **Properties > Novell Info**.



- 3 In the **Space Restriction** field, click **Change** to open the **Space Restriction** dialog box.



- 4 Do one of the following to configure the directory quota:
  - ♦ **Space Restriction:** Specify the directory quota in KB. The value must be a multiple of 4.
  - ♦ **No Space Restriction:** Select **No Space Restriction** to set the directory quota to Unlimited.
  - ♦ **Complete Space Restriction:** Select **Complete Space Restriction** to set the directory quota to 0 KB. If the directory already contains files and subdirectories, the directory cannot grow beyond the current space consumed.
- 5 Click **OK** to accept the directory quota.

## 10.5 Removing a Directory Quota

- 1 In iManager, select **Files and Folders > Properties**.
- 2 Click the **Search** icon, then browse to locate and select the folder you want to manage on an NSS volume.
- 3 On the **Information** tab, deselect **Restrict Size** to disable space restrictions for the selected folder.
- 4 Click **Apply** or **OK** to apply the changes.

## 10.6 Removing All Directory Quotas for an NSS Volume

To delete the directory quotas for all directories on an NSS volume without dealing individually with each directory, you can simply disable the Directory Quotas attribute for the NSS volume.

- 1 In iManager, click **Storage > Volumes**.
- 2 Select a server to manage.
- 3 In the **Volumes** list, select a volume that you want manage.
- 4 Click **Properties**.

The **Properties** page has three tabs: **Attributes**, **Statistics**, and **Quota Usage**. It opens to the **Attributes** tab.

- 5 On the **Attributes** tab, deselect the **Directory Quotas** check box, then click **Apply**.
- 6 Restart NCP2NSS by entering the following at a terminal prompt:

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

## 10.7 Using the Quota Utility to Set Directory and User Space Quotas on NSS Volumes

Use this utility to set or get the user space quota and directory quota on NSS volumes and files.

- ♦ [Section 10.7.1, “Syntax,” on page 92](#)
- ♦ [Section 10.7.2, “Options,” on page 92](#)
- ♦ [Section 10.7.3, “Examples,” on page 93](#)

### 10.7.1 Syntax

| Command                                              | Description                                                         |
|------------------------------------------------------|---------------------------------------------------------------------|
| <code>quota &lt;USERQUOTAOPTIONS&gt;</code>          | It is used to set or get user space quota on NSS volumes and files. |
| <code>quota<br/>&lt;DIRECTORYQUOTAOPTIONS&gt;</code> | It is used to set or get directory quota on NSS volumes and files.  |

### 10.7.2 Options

#### Usage Options

| Option                     | Description                               |
|----------------------------|-------------------------------------------|
| <code>-h, --help</code>    | Displays the help information.            |
| <code>-v, --version</code> | Displays the program version information. |

## User Quota Options

| Option                        | Description                                                           |
|-------------------------------|-----------------------------------------------------------------------|
| -U, --userquota               | To set the user quota options.                                        |
| s, --size=quota (in KB/MB/GB) | Storage space allowed for the specified user. The default unit is MB. |
| -V, --volumename=volumename   | Name of the volume for which quota has to be set.                     |
| -u, --username                | Specify the user name.                                                |
| -g, --getquotas               | Gets the user quota.                                                  |

## Directory Quota Options

| Option                                       | Description                                |
|----------------------------------------------|--------------------------------------------|
| -D, --directoryquota                         | To set the directory quota options.        |
| -s, --size=quota (in Multiples of 4KB/MB/GB) | Size of the quota. The default unit is KB. |
| -d, --directoryname                          | Directory name.                            |
| -g, --getquotas                              | Gets the directory quota.                  |

### 10.7.3 Examples

```
quota -U -V VOL1 -u wwrn.novell -s 30GB
```

This example is for user quota.

```
quota -D -d /media/nss/VOL/test -s 4GB
```

This example is for directory quota.

```
quota -g -V VOL1
```

This example is for viewing user quota.

```
quota -g -d /media/nss/VOL/test
```

This example is for viewing directory quota.



# 11 Salvaging or Purging Deleted Files and Folders on NSS Volumes

The Novell Storage Services (NSS) file system provides a mechanism for recovering deleted files and folders. The Salvage attribute must be enabled on the NSS volume.

- ♦ [Section 11.1, “Salvaging or Purging Deleted Files with iManager,” on page 95](#)
- ♦ [Section 11.2, “Salvaging or Purging Deleted Files with Other Tools,” on page 98](#)

## 11.1 Salvaging or Purging Deleted Files with iManager

As an administrator, you can use the Files and Folders plug-in to iManager to salvage or purge deleted files from an NSS volume where the Salvage attribute is enabled. When salvaging deleted files, the file content, trustees, trustee rights, and inherited rights filter are just as they were before the file was deleted. If the rights in the tree above the salvaged file have changed, then the inherited rights for the salvaged deleted file is calculated based on the current rights above it in the directory tree.

- ♦ [Section 11.1.1, “Prerequisites,” on page 95](#)
- ♦ [Section 11.1.2, “Salvaging a Deleted File,” on page 96](#)
- ♦ [Section 11.1.3, “Purging Deleted Files,” on page 97](#)

### 11.1.1 Prerequisites

- ♦ The NSS volume that you want to manage must be in the same tree where you are currently logged in.
- ♦ You must have trustee rights for the file that you want to manage.
- ♦ The NSS volume must be configured for salvage in order for deleted files to be available. Enable the Salvage attribute by going to the volume’s **Attributes** page (**Storage > Volumes > Properties > Attributes**), select **Salvage**, then click **OK**.
- ♦ Deleted files are typically purged according to the Purge Delay settings on the server. When the delay time elapses, the deleted file is no longer available for salvage.
- ♦ Deleted files can be salvaged by any trustee for the file with the Create right. If another user has salvaged the deleted file, it is no longer available for salvage.
- ♦ Deleted files can be purged by any trustee for the file with the Erase right. If another user has purged the deleted file, it is no longer available for purge.
- ♦ If the Purge Immediate attribute is set for a file or folder, it is immediately and permanently removed from the volume upon deletion.
- ♦ If the deleted file resided in a directory that has been deleted, you must first salvage the deleted directories in the path. Salvage each lower directory in turn until you have salvaged the deleted directory that contained the file. You can then search for the deleted file in the salvaged directory.
- ♦ The files must have been deleted by a trustee from an NCP-aware tool, such as an NCP client, Novell Remote Manager, the iManager Files and Folders plug-in, or NetStorage. Files and folders deleted by the `root` user from a native Linux file browser are not salvageable.

## 11.1.2 Salvaging a Deleted File

You can salvage a deleted file and restore it to the directory from which it was deleted if you are a trustee of the file with the Create write. You can choose to overwrite any existing copies of the file in that location, or to rename the deleted file before it is salvaged. Review the guidelines in [Section 11.1.1, "Prerequisites," on page 95](#) to understand when deleted files are available for salvage.

- 1 In iManager, click **Files and Folders**, then click **Deleted File** to open the **Deleted File** page.

| Name | Size | Date | Deleted By |
|------|------|------|------------|
|------|------|------|------------|

- 2 If the folder that contained the file has also been deleted, salvage the deleted directories in the path to that folder.
  - 2a On the **Deleted File** page, click the **Search** icon to browse and locate the folder that contains a deleted folder in the path, then click the name link of the folder to select it.
  - 2b Browse the list of deleted files and folders in the selected directory, and locate the version of the folder you want to salvage.

Deleted Files ?

Select a Directory path to list deleted files. You can recover deleted files by salvaging them, or purge them to remove them completely.

Salvage | Purge

| <input type="checkbox"/> | Name    | Size | Date                           | Deleted By   |
|--------------------------|---------|------|--------------------------------|--------------|
| <input type="checkbox"/> | gconf.d | 0    | Wed 24 Apr 2013 03:13:22 PMMDT | admin.novell |

- 2c Select the check box next to the deleted folder, then click **Salvage**.
  - 2d Repeat the process to salvage each lower directory in turn until you salvage the directory of interest.
- 3 On the **Deleted File** page, use one of the following methods to locate the folder on an NSS volume where the deleted file existed when it was deleted:
    - ♦ Click the **Search** icon to browse and locate the folder, then click the name link of the folder to select it.
    - ♦ Click the **History** icon to select a folder from the list of folders that you recently accessed.The **Deleted Files** report lists the deleted files in the folder and shows who deleted each file and when it was deleted.
  - 4 Browse the list of deleted files to locate the version of the file you want to salvage.



## Deleted Files



Select a Directory path to list deleted files. You can recover deleted files by salvaging them, or purge them to remove them completely.

| Salvage   Purge          |                |      |                                |            |
|--------------------------|----------------|------|--------------------------------|------------|
| <input type="checkbox"/> | Name           | Size | Date                           | Deleted By |
| <input type="checkbox"/> | base.conf      | 497  | Wed 24 Apr 2013 03:27:36 PMMDT |            |
| <input type="checkbox"/> | oes_httpd.conf | 179  | Wed 24 Apr 2013 03:27:36 PMMDT |            |

- 5 Select the deleted file that you want to salvage, then click **Salvage**.
- 6 If a current file in the folder is named the same as the salvaged file, you are prompted to do one of the following:
  - ◆ Type a new name for the salvaged file, then click **OK**.
  - ◆ Click **OK** to overwrite the current file with the salvaged file.A confirmation message indicates that the file was successfully saved.
- 7 Click **Repeat Task** to salvage or purge other deleted files, or click **OK** to dismiss the confirmation message.

### 11.1.3 Purging Deleted Files

You can purge a deleted file to remove it immediately from the volume if you are a trustee of the file with the Erase right. Purged files can no longer be salvaged. Review the guidelines in [Section 11.1.1, "Prerequisites," on page 95](#) to understand when deleted files are available.

You can purge a single deleted file, purge all deleted files in a folder, or purge a deleted folder and all of the deleted subfolders and files it contains.

- 1 In iManager, click **Files and Folders**, then click **Deleted File** to open the **Deleted File** page.

**Deleted Files**

Object name:

| Name | Size | Date | Deleted By |
|------|------|------|------------|
|------|------|------|------------|

- 2 If the folder that contained the file has also been deleted, salvage the deleted directories in the path to that folder.
  - 2a On the **Deleted File** page, click the **Search** icon to browse and locate the folder that contains a deleted folder in the path, then click the name link of the folder to select it.
  - 2b Browse the list of deleted files and folders in the selected directory, and locate the version of the folder you want to salvage.

## Deleted Files



Select a Directory path to list deleted files. You can recover deleted files by salvaging them, or purge them to remove them completely.

| Salvage   Purge          |         |      |                                |              |
|--------------------------|---------|------|--------------------------------|--------------|
| <input type="checkbox"/> | Name    | Size | Date                           | Deleted By   |
| <input type="checkbox"/> | gconf.d | 0    | Wed 24 Apr 2013 03:13:22 PMMDT | admin.novell |

**2c** Do one of the following:

- ♦ To continue in the path to purge one or multiple deleted files in a salvaged folder, select the check box next to the deleted folder, click **Salvage**, then continue to [Step 2d](#).
- ♦ To purge a deleted folder and all of the deleted subfolders and files it contains, select the check box next to the deleted folder, click **Purge**, then continue to [Step 6](#).

**2d** Repeat the process to salvage each lower directory in turn until you salvage the directory of interest.

**3** On the **Deleted File** page, use one of the following methods to locate the folder on an NSS volume where the deleted file existed when it was deleted:

- ♦ Click the **Search** icon to browse and locate the folder, then click the name link of the folder to select it.
- ♦ Click the **History** icon to select a folder from the list of folders that you recently accessed.

The **Deleted Files** report lists the deleted files in the folder and shows who deleted each file and when it was deleted.

**4** Browse the list of deleted files to locate the version of the file you want to purge.

**5** Select one or multiple deleted files that you want to purge, then click **Purge**.

A confirmation message indicates that the file was successfully purged.

**6** Click **Repeat Task** to salvage or purge other deleted files, or click **OK** to dismiss the confirmation message.

## 11.2 Salvaging or Purging Deleted Files with Other Tools

Use any of the following methods to salvage or purge deleted files. To purge, the user must be a trustee of the file with the Erase right. To salvage, the user must be a trustee of the file with the Create right.

- ♦ [Section 11.2.1, "Using NetStorage," on page 98](#)
- ♦ [Section 11.2.2, "Using the Novell Client," on page 99](#)

### 11.2.1 Using NetStorage

Using NetStorage, the Admin user, the Admin-equivalent user, and individual users can purge and possibly undelete NSS files that were previously deleted on your Linux server.

- 1 Access NetStorage.
- 2 In the left column, select the directory where the deleted files were located when they were deleted.

If the directory was also deleted, you must salvage all of the deleted directories in turn in the path to the file before you can search for the deleted file.

- 3 Click **View**, then click **Show Deleted Files**.
- 4 Select the check box next to one or more files you want to undelete or purge.
- 5 Click **File**, then click **Undelete** or click **Purge**.

## 11.2.2 Using the Novell Client

Using the Novell Client, Admin users, Admin-equivalent users, and individual users can purge and possibly undelete NSS files that were previously deleted on your Linux server.

- 1 Right-click the Novell Client icon (the red N) in the notification area to display the menu.
- 2 If the directory was also deleted, you must salvage all of the deleted directories in turn in the path to the file before you can search for the deleted file.
- 3 If you want to salvage a deleted file, click **Novell Utilities > Salvage**, browse to locate the directory where the deleted file resided, then do one of the following:
  - ♦ To restore one or more deleted files, select the deleted files, then click **Salvage File**.
  - ♦ To restore all deleted files in the directory, click **Salvage All**.

When you are done, click **OK**.

- 4 If you want to purge a deleted file, click **Novell Utilities > Purge**, browse to locate the directory where the deleted file resided, then do one of the following:
  - ♦ To purge one or more deleted files, select the deleted files, then click **Purge File**.
  - ♦ To purge all deleted files in the directory, click **Purge All**.
  - ♦ To purge the directory's subdirectories and all deleted files in them, click **Purge Subdirectories**.
- 5 When you are done, click **OK**.



# 12 Configuring File System Attributes for NSS Files and Folders

Novell Storage Services (NSS) provides file system attributes for folders and files that allow you to specify how the file or folder behaves when accessed by any user. If the **Directory Quotas** option is enabled on the NSS volume, you can also specify space quotas on folders. If you and the Supervisor right, you can modify the file owner. You might want to do this if you have set user space restrictions.

- ♦ Section 12.1, “Viewing Properties of a File or Folder in iManager,” on page 101
- ♦ Section 12.2, “Viewing or Modifying File Ownership,” on page 106
- ♦ Section 12.3, “Viewing or Modifying File System Attributes for NSS Volumes,” on page 107
- ♦ Section 12.4, “Using the Novell Client to Configure File System Attributes,” on page 108
- ♦ Section 12.5, “Using Novell NetStorage to Configure File System Attributes,” on page 109
- ♦ Section 12.6, “Using the Attrb Utility to Set NSS File System Attributes,” on page 109

## 12.1 Viewing Properties of a File or Folder in iManager

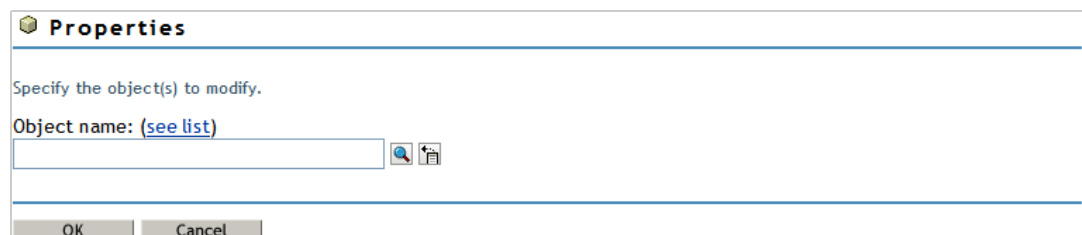
As an administrator or a user with the Supervisor right or Access Control right, you can manage file system trustees, trustee rights, inherited rights, and attributes for a file or folder. A user who has only the Access Control right cannot modify the Supervisor right of another user.

Ensure that you meet the following prerequisites for managing properties for the file or folder:

- ♦ The network volume that you want to manage must be in the same tree where you are currently logged in.
- ♦ You must have trustee rights for the volume, folder, and file that you want to manage.
- ♦ The volume must be a file system that uses the OES trustee model for file access.

To view properties:

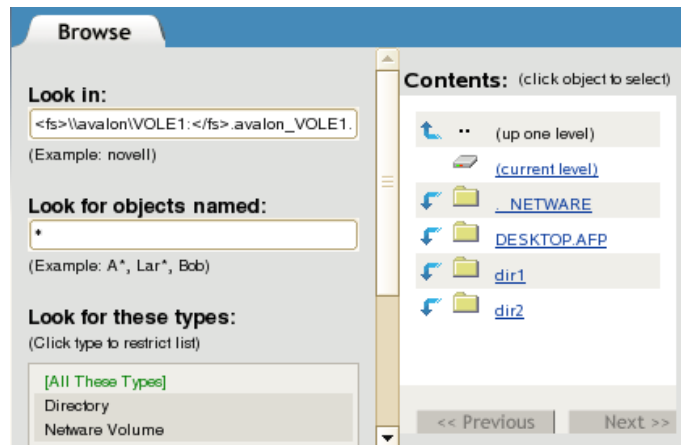
- 1 In iManager, use either of the following methods to select a file or folder and open its Properties page:
  - ♦ **Files and Folders Role:** In the iManager toolbar, select the **Roles and Tasks** icon. In the left panel, select **Files and Folders > Properties**.



The screenshot shows a dialog box titled "Properties". Inside the dialog, there is a subtitle "Specify the object(s) to modify." Below this, there is a text input field with the label "Object name: (see list)". To the right of the input field are two small icons: a magnifying glass and a refresh symbol. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Use one of the following methods to specify the volume, folder, or file that you want manage:

- ◆ Click the **Search** icon to browse and locate volume, folder or file from the Storage objects, click the name link of the object to select it, then click **OK** to open the Properties page for the selected folder.



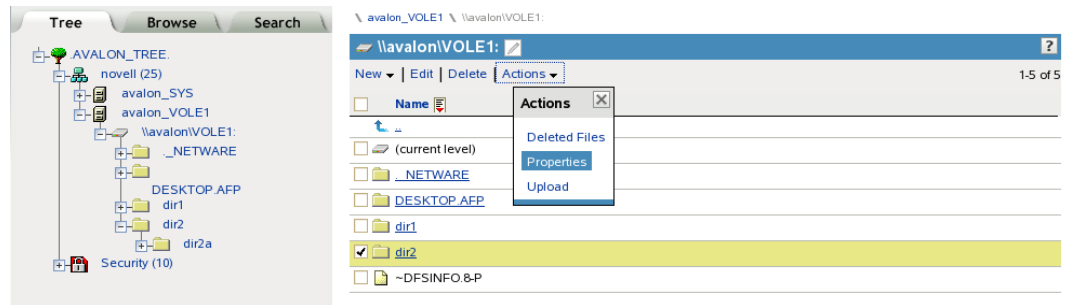
- ◆ Click the **History** icon to select a volume, folder, or file from the list of Storage objects that you recently accessed.

On the Properties page, the path name of the object appears in the **Name** field. Click **OK** to view the properties for the selected volume, folder, or file.

The properties are displayed in three **Files and Folders** tabs: **Information**, **Rights**, and **Inherited Rights**.

- ◆ **Tree View:** In the iManager toolbar, click **View Objects** icon. In the left panel, browse the Tree to locate and select the folder you want to manage on an NSS volume.

In the right panel, select the check box next to the folder, then select **Actions > Properties**.



The properties are displayed in three **Files and Folders** tabs: **Information**, **Rights**, and **Inherited Rights**.

**2** Select the **Information** tab to perform the following tasks:

- ◆ View details about the selected volume, folder, or file.
- ◆ Configure directory quotas for folders on NSS volumes. This option is available only when the Directory Quotas attribute is enabled on the NSS volume.
- ◆ Modify the file owner.
- ◆ Configure file or directory attributes.



### Properties:

Files and Folders

Information | Rights | Inherited Rights

Location: ENGVOL:proj-a\management\orgchart.png  
 Size: 66236

---

Created: 04/02/2007 3:28 PM  
 Modified: 10/10/2010 1:10 PM  
 Accessed: 10/28/2010 9:15 AM  
 Archived:

---

Creator:

Archiver:

Modifier: joe.context.domain

---

Attributes

|                                             |                                          |                                         |
|---------------------------------------------|------------------------------------------|-----------------------------------------|
| <input type="checkbox"/> Read-only          | <input type="checkbox"/> Shareable       | <input type="checkbox"/> Rename Inhibit |
| <input checked="" type="checkbox"/> Archive | <input type="checkbox"/> Transactional   | <input type="checkbox"/> Delete Inhibit |
| <input type="checkbox"/> Hidden             | <input type="checkbox"/> Purge Immediate | <input type="checkbox"/> Copy Inhibit   |

---

The Information page displays the following properties:

| Property                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location                                                           | The path name of the selected volume, folder, or file. For example:<br><br><code>VOL1:dir1\dirB\filename.ext</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Restrict Size<br>(Enable or Disable a Directory Quota on a Folder) | <p>Enable (select) or disable (deselect) a directory quota on the specified folder on an NSS volume where the Directory Quotas attribute is enabled. The default is Disabled.</p> <p>If this option is enabled, you must also specify a value for the quota in the Limit field.</p> <p>A directory quota limits the amount of space on a volume that can be consumed by all of the files and folders in that directory. The directory quota applies to files and folders created by any user of the directory.</p> <p>Select <b>Restrict Size</b> to enable a directory quota for the selected folder, specify the quota value in <b>Limit</b>, then click <b>Apply</b>.</p> <p>Deselect <b>Restrict Size</b> to disable a directory quota for the selected folder, then click <b>Apply</b>.</p> |

| Property                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Limit<br><br>(Set Limit for a Directory Quota on a Folder) | <p>The maximum size allowed for the specified directory and its contents.</p> <p>Default: Disabled (not available unless <b>Restrict Size</b> is enabled).</p> <p>If you enable <b>Restrict Size</b> for the selected folder, you must specify a limit for the directory quota. Type a value in KB for the quota. The value must be an increment of 4 KB; that is, it must be divisible by 4 with no remainder. Click <b>Apply</b> to save the changes.</p> <p>If the value you specify exceeds the volume quota, the volume quota overrides the directory quota.</p> <p>If the current size of the selected folder exceeds the specified limit, users cannot save data to the folder until space is cleared by removing files from it.</p> <p>If a user quota is set for a user on the volume, the user space restriction overrides the directory quota. That is, the user cannot save data to the folder if doing so causes the user to exceed his or her user quota.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Created                                                    | The time stamp (MM/DD/YYYY hh:mm) for when the file or folder was created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Modified                                                   | The time stamp (MM/DD/YYYY hh:mm) for when the file or folder was last modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Accessed                                                   | The time stamp (MM/DD/YYYY hh:mm) for when the file or folder was last accessed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Archived                                                   | The time stamp (MM/DD/YYYY hh:mm) for when the file or folder was last archived.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Creator<br><br>(View or Modify Ownership)                  | <p>The typeless distinguished eDirectory user name (such as <code>username.context</code>) of the user who created the file or folder. If the user name becomes invalid, such as if an employee leaves the company, the GUID of the user name is reported. For NSS, any number of files or folders can be represented by GUIDs instead of valid user names.</p> <p>To modify the ownership of file or folder, you must be logged in as an administrator user of the server. Specifically, you need the eDirectory Write right on the NCP Server object for the server. You also need to be assigned as a trustee of the file or folder and have the Access Control and Write rights for it.</p> <p>User quotas for NSS volumes consider file ownership to enforce user space restrictions. You might need to change the ownership of a file or folder in order to make the space it consumes be charged against a different user.</p> <p>For NSS volumes and NCP volumes on Linux, all access to data is controlled by file system trustees and trustee rights instead of by ownership. When a user creates a file or folder, the trustees and trustee rights for accessing the file are automatically inherited from the directory where the file is created. If you intend different trustees and rights for the file, you must assign them explicitly. For instructions, see <a href="#">Section 6.5, "Using the Files and Folders Plug-In for iManager to Manage Trustees, Trustee Rights, and Inherited Rights," on page 60.</a></p> <p>Changing the ownership of the file or folder does not modify who can access it, but it does modify whose user name is charged for the space it consumes. If you modify the ownership, you must click Apply or OK to save the changes.</p> |
| Archiver                                                   | The distinguished user name (such as <code>username.context</code> ) of the user who modified the version of the file or folder that was last archived.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Modifier                                                   | The distinguished user name (such as <code>username.context</code> ) of the user who last modified the current version of the file or folder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



| Property   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attributes | <p>File system attributes determine how the file or folder behaves when accessed by any user. Enable or disable an attribute by selecting or deselecting the check box next to it. If you modify a setting, click <b>Apply</b> or <b>OK</b> to save the changes.</p> <p>File attributes apply universally to all users. For example, a file that has a read-only attribute is read-only for all users.</p> <p>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.</p> <p>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.</p> |

The following table defines file system attributes and whether they apply to files, folders, or both files and folders.

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                      | Files | Folders |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|
| Read Only               | Prevents a file from being modified.                                                                                                                                                                                                                                                                                                                             | Yes   | No      |
| Archive                 | Identifies files and folders that have been modified since the last backup. This attribute is assigned automatically.                                                                                                                                                                                                                                            | Yes   | Yes     |
| Hidden                  | Hides directories and files so they do not appear in a file manager or directory listing.                                                                                                                                                                                                                                                                        | Yes   | Yes     |
| Shareable               | Allows more than one user to access the file at the same time. This attribute is usually used with Read Only.                                                                                                                                                                                                                                                    | Yes   | No      |
| Transactional (NetWare) | <p>Allows a file on an NSS volume or a NetWare Traditional volume to be tracked and protected by the Transaction Tracking System (TTS) for NetWare.</p> <p>For NSS, the TTS attribute for the volume must be enabled in order for this setting to be enforced. TTS is not available for NSS on Linux.</p>                                                        | Yes   | No      |
| Purge Immediate         | 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     |
| Rename Inhibit          | Prevents the directory or file name from being modified.                                                                                                                                                                                                                                                                                                         | Yes   | Yes     |
| Delete Inhibit          | <p>Prevents users from deleting a directory or file.</p> <p>This attribute overrides the file system trustee Erase right. When Delete Inhibit 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 attribute to allow the directory or file to be deleted.</p> | Yes   | Yes     |

| Attribute    | Description                                                                                                                                                                                                                                                                                                           | Files | Folders |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|
| Copy Inhibit | Prevents users from copying a file. This attribute works only for clients using Macintosh operating systems to access NSS volumes on NetWare.<br><br>This attribute overrides the trustee Read right and File Scan right. A trustee with the Modify right must disable this attribute to allow the file to be copied. | Yes   | No      |

## 12.2 Viewing or Modifying File Ownership

The owner of a file is assigned by default to be the identity of the user who creates the file. Ownership does not determine who can access a file because the NSS file system uses the Novell Trustee Model to control access. However, user quotas for NSS volumes consider file ownership to enforce user space restrictions. You might need to change the ownership of a file or folder in order to make the space it consumes be charged against a different user. Changing the ownership of the file or folder does not modify who can access it, but it does modify whose user name is charged for the space it consumes.

The Creator field shows the typeless distinguished eDirectory user name (such as `username.context`) of the user who owns the file or folder. If the user name becomes invalid, such as if an employee leaves the company, the GUID of the user name is reported. For NSS, any number of files or folders can be represented by GUIDs instead of valid user names.

To modify the ownership of file or folder, you must be logged in as an administrator user of the server. Specifically, you need the eDirectory Write right on the NCP Server object for the server.

- 1 In iManager, click **Files and Folders**, then click **Properties** to open the **Properties** page.
- 2 Click the **Search** icon to browse and locate file from the Storage objects, click the name link of the file to select it.

The path name of the file or folder appears in the **Name** field.

- 3 Click **OK** to open the file's Properties page.

**Properties:**

Files and Folders

Information | Rights | Inherited Rights



---

Location: VOL1:mytest\dir1\schema.log  
Size: 8192

---

Created: Tue Sep 23 17:27:48 2008  
Modified: Tue Sep 23 17:27:48 2008  
Accessed: Tue Sep 23 00:00:00 2008  
Archived:

---

Creator: admin.novell  

Archiver:  
Modifier: admin.novell

---

Attributes

|                                             |                                          |                                         |
|---------------------------------------------|------------------------------------------|-----------------------------------------|
| <input type="checkbox"/> Read-only          | <input type="checkbox"/> Shareable       | <input type="checkbox"/> Rename Inhibit |
| <input checked="" type="checkbox"/> Archive | <input type="checkbox"/> Transactional   | <input type="checkbox"/> Delete Inhibit |
| <input type="checkbox"/> Hidden             | <input type="checkbox"/> Purge Immediate | <input type="checkbox"/> Copy Inhibit   |

---

OK Cancel Apply Refresh

- 4 On the Information page, the **Creator** field shows the typeless distinguished user name of the current owner, such as `username.context`.



- 5 If you want to modify the owner, click the **Search** icon to open the **Object Browser** dialog box, then locate and select the user name of the new owner.
- 6 If you modified the owner, click **Apply** or **OK** on the Information page in order to save the change.

## 12.3 Viewing or Modifying File System Attributes for NSS Volumes

- 1 Select a volume, folder, or file to manage.  
For instructions, see [Section 6.3, "Viewing Properties of a File or Folder in iManager," on page 56](#).
- 2 Click the **Information** tab to view or modify the following attributes for the selected volume, folder, or file:

---

**IMPORTANT:** Changes do not take effect until you click **OK** or **Apply**. If you click a different tab before you save, changes you make on this page are lost.

---

The following table defines file system attributes and whether they apply to files, folders, or both files and folders.

| Attribute               | Description                                                                                                                                                                                                                                                                                        | Files | Folders |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|
| Read Only               | Prevents a file from being modified.                                                                                                                                                                                                                                                               | Yes   | No      |
| Archive                 | Identifies files and folders that have been modified since the last backup. This attribute is assigned automatically.                                                                                                                                                                              | Yes   | Yes     |
| Hidden                  | Hides directories and files so they do not appear in a file manager or directory listing.                                                                                                                                                                                                          | Yes   | Yes     |
| Shareable               | Allows more than one user to access the file at the same time. This attribute is usually used with Read Only.                                                                                                                                                                                      | Yes   | No      |
| Transactional (NetWare) | Allows a file on an NSS volume or a NetWare Traditional volume to be tracked and protected by the Transaction Tracking System (TTS) for NetWare.<br><br>For NSS, the TTS attribute for the volume must be enabled in order for this setting to be enforced. TTS is not available for NSS on Linux. | Yes   | No      |
| Purge Immediate         | 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     |
| Rename Inhibit          | Prevents the directory or file name from being modified.                                                                                                                                                                                                                                           | Yes   | Yes     |

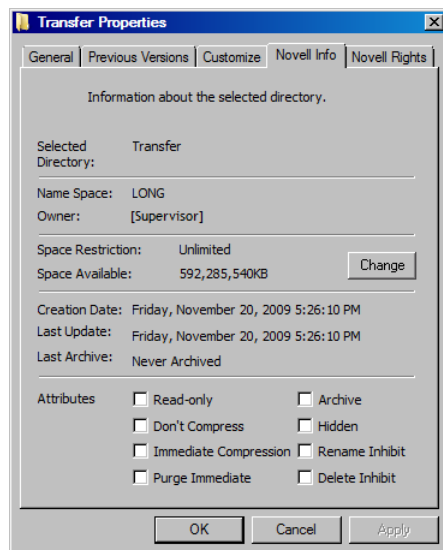
| Attribute      | Description                                                                                                                                                                                                                                                                                                                                               | Files | Folders |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|
| Delete Inhibit | Prevents users from deleting a directory or file.<br><br>This attribute overrides the file system trustee Erase right. When Delete Inhibit 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 attribute to allow the directory or file to be deleted. | Yes   | Yes     |
| Copy Inhibit   | Prevents users from copying a file. This attribute works only for clients using Macintosh operating systems to access NSS volumes on NetWare.<br><br>This attribute overrides the trustee Read right and File Scan right. A trustee with the Modify right must disable this attribute to allow the file to be copied.                                     | Yes   | No      |

- 3 If you modified any settings, click **Apply** or **OK** to save your changes.

## 12.4 Using the Novell Client to Configure File System Attributes

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 **Novell Info**.



- 2 In the **Attributes** area, select an 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 volumes.
  - ♦ The attribute must be enforceable by NCP or NSS in the current network configuration.
- 3 Click **OK**.

## 12.5 Using Novell NetStorage to Configure File System Attributes

- 1 Open your web browser to NetStorage and log in.
- 2 Right-click the directory or file you want to manage, then select **Properties**.
- 3 Click the **Novell Info** tab, select or deselect attributes for the selected directory or file, then click **Apply**.

Select from the following attributes:

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

For information, see [Section 5.7, “Understanding Directory and File Attributes for NSS Volumes,”](#) on page 48

## 12.6 Using the `Attrib` Utility to Set NSS File System Attributes

Use the Attribute (`attrib`) utility to set NSS file system directory and file attributes on Linux.

- ♦ [Section 12.6.1, “Syntax,”](#) on page 109
- ♦ [Section 12.6.2, “Options,”](#) on page 110
- ♦ [Section 12.6.3, “Attributes,”](#) on page 110
- ♦ [Section 12.6.4, “Example,”](#) on page 111
- ♦ [Section 12.6.5, “See Also,”](#) on page 111

### 12.6.1 Syntax

```
attrib [options] [filename]
```

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

## 12.6.2 Options

| Option                         | Description                                          |
|--------------------------------|------------------------------------------------------|
| -s, --set=ATTRIBUTES           | Set the attributes on the file.                      |
| -c, --clear=[ATTRIBUTES   all] | Clear the attributes on the file.                    |
| -l, --long                     | Displays a long version of the file attributes.      |
| -q, --quiet                    | Does not display any normal output.                  |
| -d, --dos                      | Use DOS compatible attributes (that is, ro=ro,di,ri) |
| -v, --version                  | Displays the program version information.            |
| -h, --help                     | Displays the ATTRIB help screen.                     |
| -S, --softlink                 | Do not follow link option.                           |
| -r, --recursive                | Set the attributes recursively on the directory.     |

## 12.6.3 Attributes

Multiple attributes are separated with commas.

| Attribute | 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                     |
| 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 Read and File Scan trustee rights. This attribute works only for clients using Macintosh operating systems to access NSS volumes on NetWare.                                                                                                                   | Yes              | No                     |
| cm        | Compressed (status display only) indicates whether the file is currently stored in compressed format.                                                                                                                                                                                                                                        | Yes              | No                     |
| dc        | Don't 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.<br><br>This attribute overrides the Erase trustee 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 files.                                                                                                                                                                                                                                                                                 | Yes              | No                     |

| Attribute | Description                                                                                                                                                                                                                                                                                                                                                                                            | Applies to Files | Applies to Directories |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------------------|
| hi        | Hidden hides directories and files so they do not appear in a file manager or directory listing.                                                                                                                                                                                                                                                                                                       | Yes              | Yes                    |
| ic        | Immediate Compression 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.<br><br>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 file or directory name from being modified.                                                                                                                                                                                                                                                                                                                                | Yes              | Yes                    |
| ro        | Read Only prevents a file from being modified.                                                                                                                                                                                                                                                                                                                                                         | Yes              | No                     |
| sd        | Subdirectory (status display only) indicates that the entry is a directory, not a file.                                                                                                                                                                                                                                                                                                                | No               | Yes                    |
| sh        | Shareable 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. This attribute is normally used with 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                     |

## 12.6.4 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.

## 12.6.5 See Also

For information about setting Novell Trustee Rights, see [“Using the Rights Utility to Set Trustee Rights for the NSS File System” on page 67.](#)





# 13 Understanding Directory Structures in Linux POSIX File Systems

This section discusses directory structures for Linux POSIX file systems on your Open Enterprise Server (OES) 11 or later server.

- ◆ Section 13.1, “Linux Filesystem Hierarchy,” on page 113
- ◆ Section 13.2, “Default Directories,” on page 113
- ◆ Section 13.3, “Linux File Types,” on page 114
- ◆ Section 13.4, “POSIX Access Control Lists,” on page 114

For information about OES file systems, see the *SUSE Linux Enterprise Server 11 SP3 Storage Administration Guide* ([https://www.suse.com/documentation/sles11/stor\\_admin/data/bookinfo.html](https://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html)).

## 13.1 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.

---

## 13.2 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/ <i>username</i> | 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 file names 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.

## 13.3 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 |

## 13.4 POSIX Access Control Lists

For information, see “Access Control Lists” ([https://www.suse.com/documentation/sles11/book\\_security/data/cha\\_acls.html](https://www.suse.com/documentation/sles11/book_security/data/cha_acls.html)) in the *SLES 11 SP3 Security Guide* ([https://www.suse.com/documentation/sles11/book\\_security/data/book\\_security.html](https://www.suse.com/documentation/sles11/book_security/data/book_security.html)).