Novell NetWare® 6.5

www.novell.com

February 28, 2005

TRADITIONAL FILE SYSTEM ADMINISTRATION GUIDE

Novell®

Legal Notices

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

www.novell.com

NetWare 6.5 Traditional File System Administration Guide

February 28, 2005

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

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
NetWare is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare Loadable Module and NLM are trademarks of Novell, Inc.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Client is a trademark of Novell, Inc.
Novell Storage Services is a trademark of Novell, Inc.
Storage Management Services and SMS are trademarks of Novell, Inc.
Transaction Tracking System and TTS are trademarks of Novell, Inc.
ZENworks is a registered trademark of Novell, Inc. in the United States and other countries.

Third-Party Materials

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

Contents

About This Guide

This guide discusses how to configure and manage NetWare® 6.5 Traditional File System (Traditional). This guide is intended for network administrators and is divided into the following sections:

Documentation Conventions

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

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

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

User Comments

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

Documentation Updates

For the most recent version of the *NetWare 6.5 Traditional File System Administration Guide*, see the NetWare 6.5 Documentation Web Site (http://www.novell.com/documentation/lg/nw65/index.html).

Additional Documentation

For information about the NSS storage and file management system, see the *Novell Storage Services File System Administration Guide for NetWare 6.5*.

For information about server disks and storage devices, see the *NetWare 6.5 Server Disks and Storage Devices Administration Guide*.

For information about managing Traditional file systems using Novell Remote Manager, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

1 Overview of Traditional File System

The NetWare® Traditional File System (Traditional) provides legacy storage and file system management in NetWare 6 and later. You can use the NetWare Traditional file system for data volumes, but your default operating system for NetWare 6.5 is the Novell Storage Services™ (NSS) file system.

NSS provides the primary system for storage and file management. For a direct comparison of Traditional file systems and NSS file systems, see "Comparison of NSS on NetWare and the NetWare Traditional File System" in the *Novell Storage Services File System Administration Guide for NetWare 6.5*.

You can optionally use the Traditional volumes on the same server with your NSS volumes. However, if you are planning to implement Apple* File Protocol (AFP), Network File System (NFS), or Common Internet File System (CIFS) for this server, you must use the NSS file system, not the Traditional file system for your system volume and for any data volumes that use these protocols.

To upgrade your Traditional volumes to NSS volumes, see "Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade" in the *Novell Storage Services File System Administration Guide for NetWare 6.5*.

This section discusses the following key concepts:

- "NetWare Traditional Volumes" on page 11
- "Traditional Volume Segments" on page 12
- "What's Next" on page 13

NetWare Traditional Volumes

Traditional volumes consist of a fixed amount of physical space on one or more server disks. A NetWare server supports up to 255 volumes of any combination of Traditional and NSS volumes, plus the system volume. A Traditional volume can use space from up to 32 logical or physical devices

The sys: volume is created during NetWare installation and is automatically created as an NSS volume. After installation, you can use Novell Remote Manager for NetWare to create a new Traditional volume on any disk that has a NetWare partition. For information, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

You subdivide Traditional volumes in two ways:

- **Physically:** Traditional volumes consist of physical partitions called volume segments. If a Traditional volume contains multiple volume segments, its member segments can reside on multiple server disks. For information about volume segments, see "Traditional Volume Segments" on page 12.

- **Logically:** You divide volumes into directories. In turn, the directories contain files and subdirectories created by network supervisors and users who have the appropriate rights. For information about directories and subdirectories, see "Directories" on page 51.

What Happens When You Mount a Traditional Volume

When you boot a NetWare server, each Traditional volume is mounted, meaning the following:

- The volume becomes visible to the operating system.
- The volume's File Allocation Table (FAT) is loaded into memory.

  A single block of data in the file takes up one entry in the FAT. Because of this, volumes with a smaller block size require more server memory to mount and manage, and it takes longer to mount the volume. However, if most of your files are small, a large block size wastes disk space.
- The volume's directory entry table (DET) is loaded into the server memory.

As the Traditional volume is mounted, the FAT and DET fill cache buffers in the server memory. The more files and directories in the volume, the longer it takes to mount. If a Traditional volume fails to mount, it might be because you have run out of server memory.

Traditional Volume Objects in eDirectory

In Novell eDirectory™, each Traditional volume is represented by a Volume object. Volume objects are leaf objects that represent a physical volume or logical volume on the network.

The Volume object's properties contains the following information:

- The NetWare server the physical volume resides on
- The volume name recorded when the volume was initialized on the server (for example, sys:)
- The volume's owner
- Space use restrictions for users
- A description of the volume's use
- Statistical information on disk space availability, block size, directory entries, name space support, and so on.

Traditional Volume Segments

A Traditional volume segment is a physical segmentation of the NetWare partition. A Traditional volume contains 1 to 32 volume segments and can grow up to 1 TB in size. A segment is space from a NetWare partition on a single device. A Traditional volume can span server disks by using multiple segments contributed from multiple disks. By distributing a volume's segments across multiple server disks, different parts of the same volume can be read from or written to concurrently, speeding up disk I/O.

Each server disk can contain up to four NetWare partitions, or three NetWare partitions and one DOS partition. (The hard drive that contains the sys: volume also contains a DOS partition.)

Each NetWare partition can contain up to eight Traditional volume segments. Thus, a single server disk can contain up to 32 volume segments (4 NetWare partitions with 8 segments each). A single

NetWare partition can contain up to eight Traditional NetWare volumes, each with a single volume segment.

A single disk can contain volume segments from multiple volumes. If a single disk fails, each volume segment on it fails, causing all of the volumes that have volume segments on that server disk to fail. To achieve fault tolerance, you should protect the volumes against disk failure by setting up a software RAID 1 (mirroring) device for the partitions. See "Using Software RAID-1 Devices for Data Fault Tolerance" on page 31.

You can add volume segments to a Traditional volume if free space is available, but you cannot remove them. Removing a segment from a volume destroys the entire volume.

You can increase the size of a Traditional volume by adding another server disk to the NetWare server, setting up a NetWare partition on the disk, then adding one or more segments in the partition to the existing volume.

What's Next

Use the table below to determine where next to go in this document.

Task	Reference
Configure and manage Traditional NetWare partitions and volumes	Configuring and Managing Traditional File System
Optimize storage performance	Conserving Disk Space
Create a software RAID device	Using Software RAID-1 Devices for Data Fault Tolerance Using Software RAID-0 Devices to Enhance Disk I/O Performance
Troubleshoot problems	Troubleshooting
Plan your directory structure	Planning Your Directory Structure
Configure and manage directories and files	Configuring and Managing Directories and Files

2 Configuring and Managing Traditional File System

In NetWare® 6.5, you manage Novell® Traditional File System using Novell Remote Manager. For information about this management tool, see *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

This section discusses the following file and directory management tasks:

Using Novell Remote Manager

To access Novell Remote Manager for NetWare:

1 From your Web browser, enter

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

Replace *server-ip-address* with the IP address or DNS name of the server you want to manage.

The login page opens.

2. Type your administrator username and password.
3. Click OK.

   The management interface opens in your Web browser.

In Novell Remote Manager, the Partition Disks page displays the server disk's layout according to the physical connections in your server. It uses indentation to indicate where a volume physically resides. It lists adapters, devices, partitions, Traditional volumes, and free space at different levels of indentation.

Depending on what tasks can be performed on the listed storage item, NRM displays task-based links next to the devices, Traditional volumes, and free space:

- **Create:** Create a new volume on the selected device.
- **Mirror:** Create a mirrored partition on the selected device.
- **Expand:** Expand an existing Traditional volume or software RAID-1 device (mirrored partition).
- **Rename:** Change the name of the Traditional NetWare partition or Traditional volume.
- **Delete:** Remove the Traditional NetWare partition or Traditional volume. Deleting a partition or volume destroys all the data in it.
- **Remove Mirror:** Remove a mirrored partition from the mirrored group (a software RAID-1 device).

You must assign the free space on the disk to create a Traditional volume. With Traditional volumes, you assign physical volume segments from physical partitions on multiple devices. There are physical limitations in how you combine member segments to create the volume. For information, see "Traditional Volume Segments" on page 12.

Managing NetWare Partitions

NetWare partitions can be created on any hard drive and can coexist with other partitions such as DOS, Windows, and UNIX. Disk space not assigned to NetWare partitions can be used for the Novell Storage Services file system.

When there is a DOS partition on the drive, it should always be the *first* partition. The NetWare partition should always be the *last* partition on the drive.

You can have as many as four partitions on the same drive, including multiple NetWare partitions.

If you have partitions from previous versions of NetWare that you are no longer using, you can delete them and create a new NetWare partition.

WARNING: When creating a disk partition, never specify a partition size larger than the actual size of the disk. If you specify a larger size, NetWare will eventually try to use the excess disk space. When it determines there is no corresponding disk location, it deactivates the volume stored on the disk.

For more information, see Chapter 2, "Configuring and Managing Traditional File System," on page 15.

Creating a Traditional NetWare Partition

The first task for setting up the Traditional file system is to create partitions on your storage devices.

1. In NRM, click Manage Server > Partition Disks.
2. Locate the device that you want to create the partition on, then click Create.
3. In the Partition Type drop-down list, select the type of partition you want to create. For example, Traditional NetWare partition.
4. Click Create Partition and Volume.
5. Specify the size of the partition in bytes (B), kilobytes (KB), megabytes (MB), or gigabytes (GB).

   If you plan to make this a mirrored partition, it must be compatible in data area size with other partitions you plan to use. The physical size of the partition must be at least 100 KB, but no more than 120 MB larger than the data size of the existing partitions in the mirror group.
6. (Conditional) To create a partition that can be mirrored, select Mirror and select one of the following options:
   - **Create New Mirror:** This option means you are making the partition capable of being part of a mirror group. You do not actually create the group until you add another mirrored partition to the partition you are creating.
   - **Existing Mirror Group:** (If you select this option, also select the ID of the mirrored partition.) This shows a list of existing mirror groups that are compatible in data area size. This option lets you add this new partition to one of the mirror groups in the list.
7. Complete the required fields, click Create, then click OK to confirm your decision.

   If this is a mirrored partition, NetWare displays the status as “100% mirrored” when the mirroring is complete.

Expanding the Size of a Traditional NetWare Partition

1. Locate the partition you want to expand, then click Expand.
2. Select the Free Disk Space with the amount of space available that you want to use.
3. Enter the amount of space (in megabytes) that you want to use, then click Expand.

Unmirroring a Mirrored Traditional NetWare Partition

To unmirror a partition, locate the partition you want to unmirror, then click Remove

This removes the partition from the mirror group. You can now delete the partition, if desired.

Deleting a Traditional NetWare Partition

If you delete a partition, you destroy all volumes and data on that partition.

If the partition is mirrored, the other partitions in the mirror group will retain the data from the deleted partition. If you want to delete a mirrored partition, you must unmirror that partition before you delete it.

Unmirror a Partition

To unmirror a partition, locate the partition you want to unmirror, then click Remove.

This removes the partition from the mirror group. You can now delete the partition.

Delete a Partition

1. Locate, then delete all Traditional volumes contained in the partition you want to delete.
2. Locate the partition you want to delete, then click Delete.
3. Click OK.

Creating and Mounting a Traditional Volume

To create Traditional volumes in NetWare 6.5, follow these guidelines:

- You can use the Vrepair utility command to fix Traditional volumes. For instructions, see "VREPAIR" in the *NetWare 6.5 Utilities Reference*.
- You cannot put Traditional volumes in an NSS storage pool.
- If you create a Traditional volume in NetWare 6.5, you cannot access that volume from previous releases of NetWare.

To create a Traditional volume:

1. Locate the free space on the device that you want to create the volume on, then click Create.
2. In the Partition Type drop down-list, select the type of partition you want to create. For example, Traditional NetWare partition.
3. Provide information for the required fields for the type of partition and volume you want to create, then check the check boxes for the volume attributes that you want to set.

   IMPORTANT: Some attributes cannot be changed after the volume is created. You must decide before you go forward what attributes you want to assign.

   Select any of the following options:

   - **Compression**. Enables the file system to compress the files in the volume. You set up file compression when you create volumes. After you enable file compression, you cannot turn it off for the life of the volume. You can back up the data in uncompressed form, create a new uncompressed volume, then restore the uncompressed data to the new volume.
   - **Migration**. Enables the operating system to move infrequently accessed data to remote areas on your server. This creates space for new and more commonly accessed data. Selecting this option only enables the attribute. The data migration feature uses a third-party software package that does the migration function.
   - **Suballocation**. Enables the file system to divide partially used disk blocks into suballocation blocks of 512 bytes. These blocks can be used by other data files.
   - **Mount Volume on Creation**. Instructs the operating system to mount the volume when you create it. Otherwise, you can mount it later.
4. Click Create, then click OK to confirm.
5. After creating a volume, you need to mount it in order to use it. Locate the newly created volume in the list, then click Mount Volume.

Expanding the Size of a Traditional Volume

To increase the size of a Traditional volume, you need to add another segment to that volume.

1. Locate the volume you want to expand, then click Expand.
2. Select the Free Disk Space with the amount of space available that you want to use.
3. Enter the amount of space (in megabytes) that you want to use, then click Expand.

   NetWare creates a volume segment of that size, then adds it to the volume.

Setting the Space Quota for a Traditional Volume

1. Locate the volume you want to set quotas for, then click Space Quota.
2. Click Volume Space Quota.
3. Specify the value (in megabytes) of the space size you want to specify, then click Apply.
4. To confirm your decision, click OK.

Loading and Installing Name Spaces on a Traditional Volume

1. Locate the volume you want to view, then click Name Spaces.
2. Locate the name space you want to load, then click Not Loaded in the Name Space Module Status column.
3. Locate the name space you want to install, then click Not Installed in the Volume Name Space Status column.
4. To confirm your decision, click OK.

Storing Non-DOS Files on a Traditional Volume

By default, NetWare Traditional volumes support DOS naming conventions. To store non-DOS files on a Traditional volume, you must load the appropriate name-space NetWare Loadable Module™ (NLM™) program and add the name-space support to that volume. The following NLM programs are available with NetWare:

- mac.nam (Macintosh*)
- long.nam (IBM OS/2, Windows)
- nfs.nam (NFS)

An FTAM name space module is available from third-party providers.

Each name space you add to a Traditional NetWare volume requires additional server memory. If you add name-space support to a volume and do not have enough memory, that volume cannot be mounted.

If you have insufficient memory to mount a Traditional volume with a long name space, you might want to convert the volume to an NSS volume. For information, see "Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade" in the *Novell Storage Services File System Administration Guide for NetWare 6.5*.

This section discusses the following:

Calculating Memory Required for Name Space Support

Use the following formula to calculate the name space memory requirement for Traditional NetWare non-DOS volumes:

0.032 x *volume_size* (in MB) / *block_size* (in MB)

Round the size up to the highest number.

For example, adding Macintosh name space to a 100 MB volume with a block size of 4 MB would require 1 MB of additional memory:

0.032 x 100 MB / 4 = 0.8 MB

Adding a Name Space

Prerequisites

- ❑ A mounted Traditional volume
- ❑ Sufficient memory

Procedure

1. To load the appropriate name space: At the server console prompt, enter:

   ```
   load [path]name_space
   ```

   For example, to load the name space module for Macintosh support, enter:

   ```
   load mac.nam
   ```

2. To add name-space support to the volume: At the server console prompt, enter:

   ```
   add name space name to volume_name
   ```

   In this example, *name* is the name space NLM and *volume_name* is the name of the volume that will store the non-DOS files.

   NOTE: You need to add name spaces only once, not each time you start the server.

3. To verify that the name space loaded: At the server console prompt, enter:

   ```
   volumes
   ```

   This displays a list of all name spaces for the server.

Removing Name Spaces

You can remove the name space by deleting the volume and re-creating it, or by using the Vrepair utility. For instructions, see "Repairing a Traditional Volume" on page 21.

Creating an eDirectory Object for a Traditional Volume

If a NetWare volume exists on the server and does not have a corresponding object in the eDirectory, a Create eDir Object link appears on the volume line in Novell Remote Manager on the Partition Disks page. This can occur when you create a new server and keep an existing Traditional volume.

To create the eDirectory object for the volume, click Create eDir Object next to the applicable volume name.

Naming or Renaming a Traditional NetWare Partition or Volume

After creating a partition, you can give the partition a name (label). You can rename the partition by modifying the label. You can also delete the label.

Naming or Renaming the Partition Label

1. Locate the partition you to want to label or rename, then click Set Partition Label, or click the *name_of_the_partition*.
2. In the Enter the New Partition Label field, enter the name for the partition.
3. Click Apply, then click OK.

Deleting the Partition Label

1. Locate the partition you want to delete the label from, then click the *name_of_the_partition*.
2. Click Delete Partition Label, then click OK.

Deleting a Traditional Volume

1. Locate and select the Traditional volume you want to delete, then click Delete
2. Click OK to confirm your choice.

Dismounting a Traditional Volume

To repair a Traditional volume, you need to dismount that volume.

1. From NRM, open the tree you want.
2. Right-click the server object and select Properties.
3. Click Media > Traditional Volumes.
4. Select the volume you want to dismount, then click Dismount.

   The option changes to Mount.

Repairing a Traditional Volume

Typically, you cannot mount a Traditional volume if it has even minor damage. Occasionally, a damaged volume mounts and causes errors in the process.

Dismount the volume (see "Dismounting a Traditional Volume" on page 21), then use the Vrepair utility to correct volume problems or to remove name space entries from File Allocation Tables

(FATs) and Directory Entry Tables (DETs). For instructions, see "VREPAIR" in the *NetWare 6.5 Utilities Reference*.

You can run the Vrepair utility on a damaged volume while other volumes are mounted. Following are typical instances when the Vrepair utility can help:

- A hardware failure either prevented a volume from mounting or caused a disk read error.

  NOTE: Although the Vrepair utility cannot fix hardware problems, it can sometimes fix related volume damage.

- A power failure caused a corrupted volume.
- The server console displays a mirroring error when the server boots.

  This mirroring refers to the two copies of FATs and DETs that the operating system keeps (if disks are mirrored, NetWare keeps four copies).

If a volume fails to mount as the server is booting, the Vrepair utility loads automatically and attempts to repair the volume.

When the Vrepair utility autoloads, it uses the default options. If you want to use an alternate option, load the Vrepair utility manually and set the alternate option before running the Vrepair utility.

NOTE: If you do not want the Vrepair utility to automatically repair a volume that fails to mount, use the "SET" parameter named Automatically Repair Bad Volumes to change the default.

Prerequisites

❑ The volume you want to repair must be dismounted.

❑ If the volume to be repaired has name space support, the corresponding Vrepair name space module (v_*namespace*.nlm) must be located in either the sys:system directory or in a search path directory.

Example modules include v_mac.nlm and v_long.nlm.

Procedure

1 At the server console prompt, enter

```
vrepair [volume_name] [logfile_name]
```

(Optional) Replace *volume name* with the name of the volume to repair. If there is only one volume that is dismounted, you don't need to specify this parameter, because the Vrepair utility will attempt to repair that volume.

(Optional) If you want to save the error log, replace the *logfile_name* with the name of the file you want the Vrepair utility to create. The Vrepair utility creates a log of errors it finds. It displays the errors on screen and will write them to a file if you specify a filename.

When you launch the Vrepair utility, an Options menu is displayed.

2 Accept the default options, or select alternate options, as appropriate.

The first time you try to repair a volume, accept the default options. If the default options fail to repair the volume, select alternate options.

2a To accept the default options, continue with Step 3.

2b To set alternate options at the Options menu, choose Set VRepair Options, then select Option 2.

3. To begin the repair process, choose Repair A Volume from the Options menu.

   - If more than one volume is dismounted, select the volume to repair from those listed.
   - If only one volume is dismounted, the Vrepair utility assumes it is the volume that needs repairing and begins the repair.

   As the volume is being repaired, the server console screen displays a message indicating Vrepair activity.

4. (Optional) Modify error log settings after the repair has started.

   If the Vrepair utility finds many errors during the repair process, you might want to change some of the run-time error settings. To modify these settings after the repair has started, press F1 to display the Current Error Settings menu.

   - Select Option 1 if you do not want the Vrepair utility to pause after each error.
   - Select Option 2 if you want the Vrepair utility to log errors in a text file.
   - Select Option 3 to stop the volume repair.
   - Select Option 4 to continue with a volume repair after you have stopped it.

5. When the repair is complete, answer Y when prompted to write repairs to the disk.

6. If the Vrepair utility has found errors, run vrepair again by repeating Step 2 through Step 5. Repeat until the Vrepair utility finds no errors.

   If you are unable to mount the volume after running the Vrepair utility several times, you must delete the volume, then re-create the volume using NRM.

Salvaging and Purging Files

Files deleted from the NetWare server remain on the disk until the deleted files are purged. Deleted files can be salvaged any time before they are purged.

Purging frees the space used to store the deleted files on the server's server disk. If a disk runs out of free space, NetWare automatically purges the files that were deleted first. For instructions on salvaging and purging deleted files, see "Salvaging and Purging Deleted Files on NetWare Volumes" in the *ConsoleOne 1.3.x User Guide*.

Protecting Data: Disk Mirroring and Duplexing

NetWare allows you to protect your data with disk mirroring or duplexing. For information, see Chapter 4, "Using Software RAID-1 Devices for Data Fault Tolerance," on page 31.

For information on partitions, see "Creating a Traditional NetWare Partition" on page 17.

Using Directory Map Objects

A Directory Map object represents a particular directory in the file system. If you create a Directory Map object to point to an application, users can access the application by mapping a drive to the Directory Map object.

Directory Map objects can be especially useful in login scripts by indicating directories that contain applications or other frequently used files. For instructions on creating Directory Map Objects, see "Creating a Directory Map Object" in the *ConsoleOne 1.3.x User Guide*.

If you have a directory that contains a word processor, you will probably map a network-search drive to that directory in any login scripts you create. If you should later upgrade the word processor and rename the directory, you would have to change the mapping in every login script where that search mapping appears.

By using a Directory Map object, you could avoid making changes to the login scripts.

First, using ConsoleOne, you could create a Directory Map object called current_wpr that points to the word processor directory (sys:public\wpr\80).

Then, with a Map command in your login scripts, map a search drive to the Directory Map object, rather than to the specific directory:

```
map ins s2:=.current.wpr.sales.novell_us
```

For a general description of the Map command, see "MAP" in the *Utilities Reference*.

When users log in, their network-search drive is mapped to the current_wpr Directory Map object, which points to the directory containing WPR8.0.

Later, if you upgrade to WPR9.0 and change the directory's name to sys:public\wpr\90, you would change only the Directory Map object to indicate the new path.

You would not change the Map command in the login script because the Map command still indicates the correct Directory Map object.

Copying Data from Traditional to NSS Volumes

For information on copying data from Traditional volumes to NSS volumes, see "Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade" in the *Novell Storage Services File System Administration Guide for NetWare 6.5*.

3 Conserving Disk Space

This section discusses how to optimize file system performance for your Novell® NetWare® 6.5 Traditional File System storage and file management systems.

- "Saving Disk Space with File Compression" on page 25
- "Saving Disk Space with File Purging" on page 28

Saving Disk Space with File Compression

One way to conserve disk space is to compress files. If you set the File Compression attribute for a Traditional volume, NetWare compresses files that have been inactive for a period of time. Compression occurs typically at non-peak hours.

NetWare maintains the original version of a file during compression. When compression completes, NetWare replaces the original with the compressed version of the file, if no errors occurred. If errors do occur during compression, NetWare leaves the original version intact.

This section discusses the following topics:

- "Planning for File Compression" on page 25
- "Enabling File Compression" on page 26
- "Disabling File Compression" on page 27
- "Setting File Compression Attributes" on page 27
- "Suspending File Compression" on page 27

Planning for File Compression

To effectively use file compression for your Traditional volumes, you must understand several key concepts:

Only Inactive Files Are Candidates for Compression

Files automatically pass in and out of their compressed state as they are unused, then used. It is not necessary to separate application files from data files for file compression because NetWare compresses files based on the interval of time that a file remains inactive. Most application files are used regularly.

Use the Set command to preclude compression of frequently used applications. For instructions on how to use the Set command, see "SET" in the *NetWare 6.5 Utilities Reference*.

Decompression Activity Depends on Available Space

Compressed files are uncompressed as they are needed, then remain uncompressed until they are inactive for an extended period. For a file to be uncompressed, there must be enough free space on the volume to accommodate the uncompressed file size.

Immediate Compression Impacts CPU Performance

Compression is usually a low priority process thread because of compression's impact on performance. If you flag an item for immediate compression during peak system usage, performance may deteriorate.

Files Remain Compressed during Backup and Restore

Backup applications that use Novell Storage Management Services™ (SMS™) can back up and restore files in their compressed state. Other applications may decompress them.

Compressed Volumes Remain Compressed

The File Compression attribute can be turned on when you create the Traditional volume or at any time afterwards. However, after you enable file compression for a Traditional volume, you cannot turn it off. Instead, you can suspend the compression activity, as needed.

If you want to turn off file compression, you must back up the volume in its uncompressed state, then restore the data to a new volume on which the File Compression attribute is not set.

How to Monitor Compression Activity

Monitor compression activity via the Set command's Compress Screen parameter. For instructions on how to use the Set command, see "SET" in the *NetWare 6.5 Utilities Reference*.

Enabling File Compression

You choose to compress files when you create volumes by setting the File Compression attribute.You can also set the File Compression attribute later. However, after you enable file compression for a volume, you cannot turn it off.

IMPORTANT: Do not use file compression on a volume on a CD drive.

There are several parameters that affect how file compression behaves:

- Days Untouched Before Compression
- Minimum Percentage Compression Gain

Days Untouched Before Compression

Use the Set command's parameter named Days Untouched Before Compression to set this interval of inactivity. This parameter specifies the number of days that must pass without access to a file before the file can be compressed. The parameter uses the date the file was last accessed to gauge whether a file should be compressed.

Minimum Percentage Compression Gain

To avoid the overhead of uncompressing files that do not compress well, the system calculates the compressed size of a file before actually compressing it. If no disk space will be saved by compression, or if the size difference does not meet the value specified by the set command's parameter named Minimum Percentage Compression Gain, the file is not compressed. For a general description, see "SET" in *NetWare 6.5 Utilities Reference*.

For instructions on setting file compression for volumes, directories, and files, see "Setting File Compression Attributes" on page 27.

For instructions on enabling or disabling file compression, see "Creating and Mounting a Traditional Volume" on page 18.

Disabling File Compression

File compression is enabled and disabled at the volume level.

If you do not enable the File Compression attribute when you create a volume, you can subsequently enable it using the Set command. However, after it is enabled, file compression cannot be disabled on the volume unless you re-create the volume.

You can temporarily suspend file compression using the set command's Enable File Compression parameter. See "SET" in *NetWare 6.5 Utilities Reference*.

Setting File Compression Attributes

Use the Set command to set the File Compression attribute for an entire volume. File compression Set parameters do not affect the volume's file compression if the attribute is disabled for that volume.

IMPORTANT: Do not use file compression for volumes on CD drives.

To change Set command's parameters, execute the Set command at the server console prompt.

The following list identifies set command parameters that affect file compression. The settings apply to all files and directories in compression-enabled volumes on the server. For information on the function and range of values associated with each Set command's parameter, see "SET" in the *NetWare 6.5 Utilities Reference*.

- Compression Daily Check Stop Hour
- Compression Daily Check Starting Hour
- Minimum Compression Percentage Gain
- Enable File Compression
- Maximum Concurrent Compressions
- Convert Compressed to Uncompressed Option
- Decompress Percent Disk Space Free To Allow Commit
- Decompress Free Space Warning Interval
- Deleted Files Compression Option
- Days Untouched Before Compression

Suspending File Compression

Use the Set command's Enable File Compression parameter to temporarily suspend file compression for a volume. For instructions, see "SET" in *NetWare 6.5 Utilities Reference*.

While file compression is suspended, files that would have been compressed are queued and compressed when compression is re-enabled.

You can also use the Monitor utility to change file compression parameters. For a general description, see "Monitor" in the *NetWare 6.5 Utilities Reference*.

Saving Disk Space with File Purging

To save disk space, consider changing how your NetWare system treats salvageable files and the purging feature:

- "Salvageable Files" on page 28
- "File Purging" on page 28

Salvageable Files

You can conserve disk space by purging salvageable files from volumes. Salvageable files are files saved by NetWare, after being deleted by users, that can be salvaged (recovered).

Salvageable files are usually stored in the directory they were deleted from. If a user deletes that directory, the salvageable files are saved in the sys:deleted.sav directory, located in the volume's root directory.

You can view a list of deleted files in a directory and recover files by using NRM. For more information on salvaging files, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*. Recovered files contain information about who deleted the files and when they were deleted.

Deleted files are saved until the administrator deliberately purges them or until the NetWare server runs out of disk allocation blocks on the volume.

File Purging

Salvageable files are usually stored in the directory they were deleted from. If a directory is deleted, NetWare moves the salvageable files from the deleted directory to the deleted.sav directory.

When the NetWare server runs out of blocks, it purges deleted files. It deletes the files in the order that they were deleted (first in, first out) in any of the salvageable areas. Purged files cannot be salvaged.

To purge files and directories as they are deleted, use one of these methods:

- Use the Set command at the NetWare server console to disable the salvageable file feature.

  By default, the Immediate Purge of Deleted Files parameter is set to Off. By default, files are salvaged when they are deleted instead of being purged immediately.

  To purge Traditional files as they are deleted: Set the parameter named Immediate Purge of Deleted Files to On. This increases performance, but at the cost of losing the salvageable file feature. For instructions on how to use Set, see "SET" in the *NetWare 6.5 Utilities Reference*.

- Set the Purge attribute for individual files and directories.

  If a file is flagged with the Purge attribute, the file is purged when it is deleted.

If a directory is flagged with the Purge attribute, NetWare purges all files in that directory when the directory is deleted. Purged files and directories cannot be recovered.

- Use NRM to manually purge individual files and directories. For instructions, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

4 Using Software RAID-1 Devices for Data Fault Tolerance

Because NetWare® 6.5 Traditional File System volumes can span multiple disks, a single server disk failure can cause all of the volumes that have segments on that disk to fail. To increase the data fault tolerance of your server with a Traditional file system, you can mirror the data from a Traditional NetWare partition on one disk to Traditional NetWare partitions on other disks.

This section discusses the following:

- "Planning Your Software RAID-1 Device" on page 31
- "Managing Traditional Software RAID-1 Devices" on page 33

Planning Your Software RAID-1 Device

Mirroring is a software RAID-1 technique that writes data in parallel to multiple separate devices. If one device fails, the other member devices remain available.

You can create a software RAID-1 device with up to four member partitions, including the original partition and up to three mirrored partitions. Each member partition resides on a separate server disk.

As contrasted to a hardware RAID-1 device, the server operating system controls the mirroring activity in a software RAID-1 device, which can slightly impact the CPU performance for the server. Adding additional mirrors after the first contributes to availability, but it also incrementally impacts CPU performance.

Typically, you write only to the original partition and send duplicate writes to the mirrored partitions. However, you can read from all member partitions. This improves the read performance of your Traditional volumes that contain volume segments in member partitions of the RAID.

This section discusses the following considerations for achieving fault tolerance:

- "Fault Tolerance for Traditional Volumes" on page 31
- "Key Concepts for Mirroring Traditional NetWare Partitions" on page 32
- "Improving Fault Tolerance for Software RAID-1 Devices with Duplexing" on page 32
- "Example Software RAID-1 Solution for Fault Tolerance of Traditional Volumes" on page 32

Fault Tolerance for Traditional Volumes

If you mirror one partition, you do not necessarily provide data protection for the entire volume. To create software RAID-1 devices for Traditional NetWare partitions, you must keep in mind the relationship between Traditional NetWare partitions, volumes, and volume segments. (For information about these key concepts, see Chapter 1, "Overview of Traditional File System," on page 11.)

NetWare partitions consist of up to 8 volume segments. Each segment can be allocated separately as a member of a different Traditional volume. If you mirror a partition, the volume segments it contains are mirrored on the mirror partition. For a Traditional volume that spans multiple server disks, only its volume segments in that particular partition get mirrored. The volume segments on other partitions on the same or different server disks remain unprotected. To fully protect your Traditional volume, you must create a RAID-1 device for each Traditional NetWare partition that contains one of the volume's segments.

Key Concepts for Mirroring Traditional NetWare Partitions

The following are important concepts for mirroring Traditional NetWare partitions:

- All member partitions of a software RAID-1 device must be of the same type. A Traditional NetWare partition can only be mirrored to other Traditional partitions.
- Each member partition in the software RAID-1 device must be compatible in data area size.

  The new partition must be at least the same size or slightly larger than the other partitions in the group. The physical size of the partition must be at least 100 kilobytes (KB), but no more than 120 megabytes (MB) larger than the data size of the existing partitions in the mirror group.
- All member partitions in the software RAID-1 device must have the same sharable status. Either all are sharable for clustering, or all are not.
- Partitions you add to the software RAID-1 device cannot be members of any other software RAID device. They must be standalone partitions.
- Only partitions marked with the Mirror attribute can be used as a software RAID-1 mirrored partition. You must set the Mirror attribute for partitions when you create them; you cannot add the option later.
- Although you can mirror one partition to as many as four other partitions, mirroring two partitions is typically sufficient fault tolerance for most systems.
- If a mirrored disk fails and cannot be accessed by the server, you can unmirror the server's partitions on the functional disk, then salvage the lost volume segments.
- If you want to remove a hot-plug mirrored disk without bringing down the server, you must unmirror the disk first.

Improving Fault Tolerance for Software RAID-1 Devices with Duplexing

Mirroring stores the same data on separate disks on the same controller channel. If you mirror partitions on separate disks over different controller channels or host bus adapters, this is called *duplexing*. Duplexing can also concurrently use two instances of a driver for the channels. Duplexing is the recommended method for fault tolerance because two channels rarely fail simultaneously.

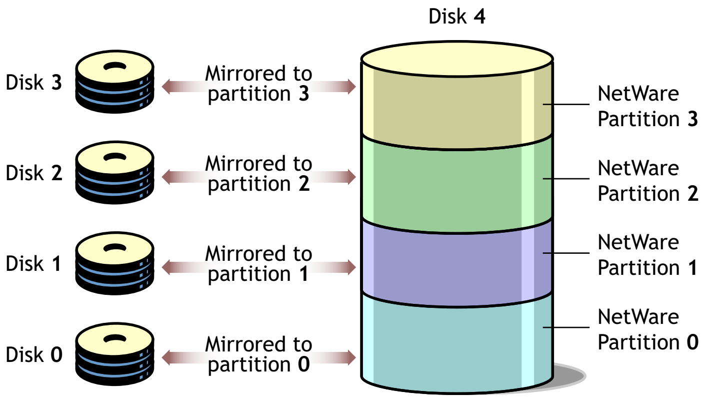
The process for mirroring and duplexing is the same. The term mirroring is used in all menus in NRM to refer to both mirroring and duplexing.

Example Software RAID-1 Solution for Fault Tolerance of Traditional Volumes

As an example, consider a server that has five server disks. Four of the disks (0, 1, 3, and 4) are under 4 gigabytes (GB) and each disk contains a single partition the size of the disk. The fifth disk (5) is 20 GB and contains four partitions of 4 GB each; the remaining 4 GB capacity are unused free space. Each physical NetWare partition is further subdivided into eight volume segments of about 500 MB each. The first four disks contain 32 volume segments that can be allocated to up to 32 separate Traditional volumes. (4 disks x 1 partition per disk x 8 volume segments per partition = 32 volume segments) You choose to create 8 Traditional volumes, each with 4 segments that span the four disks.

For data fault tolerance, you create four software RAID-1 mirrored partitions on the fifth server disk, where each the other device's partition are mirrored separately. In Figure 1, single partitions on several smaller disks are mirrored to similarly-sized partitions on one larger disk. In this configuration, if any of the small disks fail, the data on the volume segments can be recovered from the mirrored partition. However, if the large server disk fails, all of the mirrored partitions would also fail. The original data would not be harmed.

Figure 1 Mirroring Small Disks to Partitions on One Large Disk



Managing Traditional Software RAID-1 Devices

This section discusses the following management tasks:

- "Mirroring Partitions" on page 33
- "Unmirroring Partitions" on page 34
- "Recovering Data from an Out of Sync Disk" on page 34

Mirroring Partitions

You set the Mirror attribute for a partition when you create it.

1. In NRM, click Manage Server > Partition Disks.
2. Locate the device that you want to create the partition on, then click Create.
3. In the Partition Type drop-down list, select the type of partition you want to create.

   For example, Traditional NetWare partition.
4. Click Create Partition and Volume.
5. Specify the size of the partition in bytes (B), kilobytes (KB), megabytes (MB), or gigabytes (GB).

   If you plan to make this a mirrored partition, it must be compatible in data area size with other partitions you plan to use. The physical size of the partition must be at least 100 KB, but no more than 120 MB larger than the data size of the existing partitions in the mirror group.

6. (Conditional) To create a partition that can be mirrored, select Mirror and select one of the following options:

   - **Create New Mirror:** This option means you are making the partition capable of being part of a mirror group. You do not actually create the group until you add another mirrored partition to the partition you are creating.
   - **Existing Mirror Group:** (If you select this option, also select the ID of the mirrored partition.) This shows a list of existing mirror groups that are compatible in data area size. This option lets you add this new partition to one of the mirror groups in the list.

7. Complete the required fields, click Create, then click OK to confirm your decision.

   If this is a mirrored partition, NetWare displays the status as “100% mirrored” when the mirroring is complete.

Unmirroring Partitions

You must unmirror mirrored partitions before you can delete a partition or conduct surface tests on a disk.

To unmirror a partition, locate the partition you want to unmirror, then click Remove.

This removes the partition from the mirror group. You can now delete the partition.

Recovering Data from an Out of Sync Disk

After a server disk is unmirrored, its status is listed as either Not Mirrored or Out of Sync on the Disk Partition Mirroring Status list.

To check the mirror status: At the server console command prompt, enter

```
mirror status
```

When a server disk is listed as Out of Sync, the operating system does not recognize any volume information on it. Use this procedure to recover data from an Out of Sync partition.

To resynchronize the mirror: At the server console command prompt, enter:

```
remirror partition id
```

Substitute the actual partition ID for *id*. For example, if the device is 0X1e, enter

```
remirror partition 1e
```

This initiates the resynchronization process for the mirror group that contains the partition you selected. Check the mirror status to confirm the resynchronization.

5 Using Software RAID-0 Devices to Enhance Disk I/O Performance

For a heavily used volume, disk response time can be slow. Even though NetWare® 6.5 Traditional File System volumes can comprise segments from multiple disks, the disks are not forced to distribute data evenly across the member disks. You can improve disk I/O performance by using a software RAID 0 device to use for the volume. A RAID 0 device evenly stripes data across its disks.

This section discusses the following:

- "Planning Your Software RAID-0 Device" on page 35
- "Managing Traditional Software RAID-0 Devices" on page 36

Planning Your Software RAID-0 Device

Striping is a software RAID technique that writes data concurrently to multiple separate devices. Consider the following guidelines before creating your RAID 1 device:

- A segment is the amount of storage space used from each disk you plan to use in the software RAID device. A software RAID-0 device can accommodate 2 to14 segments.
- A stripe is the amount of data the file system places on one device before moving to the next device. The stripe size ranges from 4 KB to 256 KB, in increments of 2 KB. The default stripe size is 64 KB.
- Each segment in the software RAID 0 configuration should come from a different device. You can obtain segments from the same device, but this will severely impede the performance of your file system on the RAID.
- It is best to use segments of the same size when you create your RAID device. The size of each segment must be compatible in data area size with other segments you plan to use. The minimum segment size is 100 KB. The maximum size must not be more than 120 MB larger than the size of other partitions. The size the RAID pulls from each segment is equivalent to the size of its smallest member segment.
- All member segments in the software RAID-0 device must have the same sharable status. Either all are sharable for clustering, or all are not. Set the segment's disk as Sharable or Not Shareable before you build the RAID.
- If one of the member disks fails, all volumes on the RAID device become unavailable. After you replace the disk, you must restore each volume from backup media. Each volume's data must be restriped across all segments in the RAID before you can use the volume again.
- If one of the member disks fails, the entire volume becomes unavailable. Therefore, you should mirror or duplex volumes built on RAID-0 devices. To mirror the software RAID 0 devices, the devices in the mirror must have no disks in common. This configuration creates a software RAID 10 Traditional volume.

Managing Traditional Software RAID-0 Devices

You must use Novell Storage Services™ Management Utility or the NSS Storage Management plug-in for iManager to create a software RAID 0 device. For instructions, see "Managing Software RAID Devices " in the *Novell Storage Services File System Administration Guide for NetWare 6.5*.

After you create the RAID 0, use NRM to create a Traditional volume on the device. Make sure to use the RAID 0 for your segment. For information on creating a Traditional volume, see "Creating and Mounting a Traditional Volume" on page 18.

To create a RAID 10 Traditional volume, mirror the volume you just created. For information on mirroring Traditional volumes, see Chapter 4, "Using Software RAID-1 Devices for Data Fault Tolerance," on page 31.

6 Optimizing Disk and Cache Performance for Traditional Volumes

NetWare® provides several methods for improving the performance of your NetWare Traditional File System:

- "Optimizing Storage Disk Capacity for Traditional Volumes" on page 37
- "Improving Disk Reads on Traditional Volumes" on page 39
- "Improving Disk Writes for Traditional Volumes" on page 40
- "Configuring SET Parameters for the Traditional File System" on page 41
- "Configuring Common File System SET Parameters for NetWare" on page 43

For instructions on using the SET utility, see "SET" in the *NetWare 6.5 Utilities Reference*.

Optimizing Storage Disk Capacity for Traditional Volumes

There are several options for increasing the capacity of your storage disks:

- "Saving Disk Space with Block Suballocation" on page 37
- "Disable Read-After-Write-Verify" on page 38
- "For 16-Bit Disk Adapters, Increase the Number of Reserved Buffers Below 16 MB" on page 38
- "Use Drivers that Support Scatter/Gather Functionality" on page 38
- "Provide a Disk Large Enough for a Memory Core Dump" on page 38
- "Select Segments for Volumes from Different Disks" on page 38
- "Monitor Free Space in Volumes" on page 38

Saving Disk Space with Block Suballocation

Use block suballocation to enhance use of disk space.

Block suballocation divides any partially used disk block into suballocation blocks of 512 bytes. These suballocation blocks can be used by files to share what would otherwise be unavailable space.

You can set block suballocation only when creating a Traditional volume. For instructions on setting block suballocation on Traditional volumes, see "Creating and Mounting a Traditional Volume" on page 18.

Keep at least 1000 free blocks on each Traditional volume that has suballocation enabled. Free blocks are disk blocks that have no files stored in them. If the number of free blocks is low, the suballocation will increase server utilization. To view the number of free blocks, view the volume's details in iManager.

Disable Read-After-Write-Verify

Disable Read-After-Write-Verify in the Monitor utility if your hard disk provides this capability.

Read-After-Write-Verify is almost always provided by the hard disk itself. Use the Read-After-Write-Verify feature only if your hardware does not provide this feature but does support software-controlled Read-After-Write-Verify.

For information, see "Turn Off Read-After-Write Verification" on page 41.

For 16-Bit Disk Adapters, Increase the Number of Reserved Buffers Below 16 MB

If you have a 16-bit disk adapter, make sure you increase the number of reserved buffers below 16 MB. Use the Set command or Monitor utility to set the Reserved Buffers Below 16 MB parameter to its upper limit, 300. The parameter is found in Monitor > Available Options > Server Parameters > Memory. For instructions, see "SET" in the *NetWare 6.5 Utilities Reference*.

Remember that too many reserved buffers can prevent large volumes from mounting in a Traditional file system. As soon as possible, upgrade the system to a newer board that can access higher memory.

Use Drivers that Support Scatter/Gather Functionality

Scatter/gather is an I/O technique to organize the read and write calls from multiple data buffers that are separated in memory. The purpose is to lower the overhead associated with each call by reducing the number of calls that need to be made.

Provide a Disk Large Enough for a Memory Core Dump

Provide at least one device large enough to hold a core dump of the server's memory. A core dump cannot span devices.

Select Segments for Volumes from Different Disks

If a volume comprises two or more segments, each segment should be on a different disk. If the volume is made of more than one segment on one disk, the volume spans between the two segments, slowing performance.

Monitor Free Space in Volumes

Keep at least 10% free space in any NetWare volume, except for the sys: volume, where there should be 20% free space.

WARNING: Do not fill up your sys: volume. This could damage your entire file system. The Transaction Tracking System^{TM}, which protects Novell eDirectory$^{®}$, shuts down, compromising the eDirectory replicas on the server.

To keep enough free space on volumes, try the following suggestions:

- Regularly monitor each volume's disk space.
- Use the Volume Low Warning Threshold parameter to specify when you are warned that a volume is running out of disk space.
- Move any user files or print queues to another volume.

- Do not store replicas on servers with low disk space.
- Limit the size of auditing files on Traditional NetWare partitions.

Improving Disk Reads on Traditional Volumes

On a server that is read-intensive, the following procedures can improve the speed of disk reads on your NetWare Traditional volumes.

- "Change Concurrent Disk and Directory Writes for Faster Reads for Traditional Volumes" on page 39
- "Change the Turbo FAT Wait Time for Faster Reads of Traditional Volumes" on page 39

Change Concurrent Disk and Directory Writes for Faster Reads for Traditional Volumes

Use this procedure if your server is slow to respond to read requests.

NOTE: This procedure requires that you decrease the values of the Maximum Concurrent Disk Cache Writes parameter and the Maximum Concurrent Directory Cache Writes parameter. Although decreasing these values increases the speed of read requests, it might decrease the speed and efficiency of write requests.

Modify the following parameters using "SET" in the *NetWare 6.5 Utilities Reference*.

- Decrease the value of Maximum Concurrent Disk Cache Writes.

  If the parameter is currently set to the default value of 50, try setting the value to 10.
- Decrease the value of Maximum Concurrent Directory Cache Writes.

  If the parameter is currently set to the default value of 10, try setting the value to 5.
- Increase the value of Directory Cache Buffer Non Referenced Delay.

  This parameter specifies how long a directory entry must be cached before it can be overwritten. Increasing this value causes the system to allocate more directory cache buffers and thus speeds up directory access.

  If the parameter is currently set to the default value of 5.5 seconds, try setting the value to 60 seconds.

Change the Turbo FAT Wait Time for Faster Reads of Traditional Volumes

When a program randomly accesses a file that contains more than 64 file allocation table (FAT) entries, the file system builds a turbo FAT index for the file so that the information in the file can be accessed quickly.

The Turbo FAT Re-Use Wait Time parameter specifies how long a turbo FAT index remains in memory after the indexed file is closed. When the turbo FAT index is in memory, files can be opened and information accessed faster.

If network users frequently access files larger than 64 blocks, increase the value of FAT Re-Use Wait Time, using "SET" in the *NetWare 6.5 Utilities Reference*. You must specify the value in seconds.The new setting is persistent through a server reboot. If the parameter is currently set to the default value of 329.5 seconds (5 minutes 29.6 seconds), try setting the value to 600 seconds (10 minutes).

Improving Disk Writes for Traditional Volumes

For a write-intensive server, the following procedures can improve the speed of disk writes:

- "Increase the Number of Concurrent Writes" on page 40
- "Change Disk and Directory Caching for Faster Writes" on page 40
- "Turn Off Read-After-Write Verification" on page 41

Increase the Number of Concurrent Writes

You can increase the speed and efficiency of disk cache writes by increasing the number of write requests that can be executed at one time.

To determine whether you need to increase the number of concurrent writes, first compare the number of dirty cache buffers to the total number of cache buffers. These statistics are found on the General Information screen in the Monitor utility. Dirty cache buffers contain data that has not yet been written to disk.

The ratio of dirty cache buffers to total cache buffers is an indicator of the efficiency of disk cache writes. If the number of dirty cache buffers is greater than 70% of total cache buffers, increase the number of concurrent write requests.

NOTE: Increasing the number of concurrent disk cache writes slows disk cache reads. You might want to balance the speed of disk writes and reads to meet the needs of users. If your server's processing load is write-intensive, you can favor disk writes. If it is read-intensive, favor disk reads.

Increase the value of Maximum Concurrent Disk Cache Writes, using "SET" in the *NetWare 6.5 Utilities Reference*. The new setting is persistent through a server reboot. If the parameter is currently at the default value of 50, try increasing it to 100.

Change Disk and Directory Caching for Faster Writes

Change Disk and Directory Caching for faster writes if network users frequently make many small write requests and the server is slow to respond to the requests. Use "SET" in the *NetWare 6.5 Utilities Reference* to modify the following parameters:

- Increase the value of Dirty Disk Cache Delay Time.

  This parameter specifies how long the system waits before writing a not-completely-dirty cache buffer to disk.

  If the value is low, the system writes to disk more frequently, but writes fewer requests each time. If the value is high, the system waits longer before writing to disk, but executes more write requests with each operation. A higher value provides greater efficiency in writing to disk.

  If the parameter is currently at the default value of 3.3 seconds, try increasing the value to 7 seconds.

- Increase the value of Dirty Directory Cache Delay Time.

  This parameter specifies how long the system keeps a directory table write request in memory before writing it to disk.

  IMPORTANT: Increasing the parameter provides slightly faster performance, but can increase the chance of directory tables becoming corrupted.

  If the parameter is currently at the default value of 0.5 seconds, try increasing the value to 2 seconds.

- Increase the value of Maximum Concurrent Directory Cache Writes.

  This parameter determines how many write requests from directory cache buffers are executed at one time. Increasing this value increases the efficiency of directory cache write requests.

  Increasing the number of concurrent directory cache writes decreases the speed of directory cache reads. Balance the speed of writes and reads to meet the needs or your users.

  If the parameter is currently at the default value of 10, try increasing the value to 25. The changed value is now persistent.

Turn Off Read-After-Write Verification

Read-after-write verification is almost always provided by the hard disk. If your hard disk provides read-after-write verification, you might want to disable the software version of read-after-write verification in order to nearly double the speed of disk writes.

WARNING: Turning off read-after-write verification can increase the risk of data corruption on the server's hard disk. You should use the following procedure only if your disks provide read-after-write verification and are reliable, or if your disk subsystem provides data fault tolerance through mirroring or appropriate RAID level.

Prerequisite

□ Hard disks that provide their own means of read-after-write verification.

Procedure

Use "SET" in the *NetWare 6.5 Utilities Reference* to disable the Disk Read After Write Verification parameter.

Configuring SET Parameters for the Traditional File System

The following are the default settings in NetWare 6.5 for the Traditional file system SET parameters.

SET Parameters for the Traditional File System	Default Value
Volume Log File State	1
Volume TTS Log File State	1
Volume Log File Overflow Size	4194304
Volume TTS Log File Overflow Size	4194304
Auto TTS Backout Flag	On
TTS Abort Dump Flag	Off
TTS UnWritten Cache Wait Time	1 minute 5.9 seconds
TTS Backout File Truncation Wait Time	59 minutes 19.2 seconds
Dirty Directory Cache Delay Time	0.5 seconds
Directory Cache Allocation Wait Time	2.2 seconds
Directory Cache Buffer NonReferenced Delay	5.5 seconds

SET Parameters for the Traditional File System	Default Value
Maximum Directory Cache Buffers	2000
Minimum Directory Cache Buffers	500
Maximum Number Of Internal Directory Handles	100
Maximum Number Of Directory Handles	20
Maximum Record Locks Per Connection	500
Maximum File Locks Per Connection	2500
Maximum Record Locks	20000
Maximum File Locks	200000
Read Ahead Enabled	On
Read Ahead LRU Sitting Time Threshold	10 seconds
Minimum File Cache Buffers	20
Maximum Concurrent Disk Cache Writes	750
Dirty Disk Cache Delay Time	3.3 seconds
Minimum File Cache Report Threshold	20
Automatically Repair Bad Volumes	On
File Delete Wait Time	5 minutes 29.6 seconds
Allow Deletion Of Active Directories	On
Maximum Percent of Volume Space allowed for Extended Attributes	10
Maximum Extended Attributes per File or Path	16
Purge Files On Dismount	Off
Fast Volume Mounts	On
Maximum Percent Of Volume Used By Directory	13
Maximum Subdirectory Tree Depth	25
Volume Low Warn All Users	On
Volume Low Warning Reset Threshold	256
Volume Low Warning Threshold	256
Turbo FAT Re-Use Wait Time	5 minutes 29.6 seconds
Allow Unowned Files To Be Extended	On
Auto Mount Mirrored Volume Containing Inactive Device	Off

Configuring Common File System SET Parameters for NetWare

The SET parameters for Common File System are shared by NSS and Traditional file systems. The following are the default settings in NetWare 6.5 for the Common File System SET parameters.

IMPORTANT: When modifying Common File System SET parameters, ensure that your planned settings satisfy the requirements for both your NSS and Traditional volumes.

Common File System SET Parameters	Default Value
Maximum Transactions	10000
Maximum Concurrent Directory Cache Writes	75
Minimum File Delete Wait Time	1 minute 5.9 seconds
Immediate Purge Of Deleted Files	Off
Compression Daily Check Stop Hour	6
Compression Daily Check Starting Hour	0
Minimum Compression Percentage Gain	20
Enable File Compression	On
Maximum Concurrent Compressions	2
Convert Compressed To Uncompressed Option	1
Decompress Percent Disk Space Free To Allow Commit	10
Decompress Free Space Warning Interval	31 minutes 18.5 seconds
Deleted Files Compression Option	1
Days Untouched Before Compression	14

7 Troubleshooting

This section presents various troubleshooting procedures for resolving problems with Traditional volume including the following:

Resolving File I/O Errors

To resolve a file I/O error, try one or more of the following:

- Make sure that the volume (especially volume sys:) is mounted.
- If the volume is out of disk space, error messages will appear on the Logger Console screen indicating that the volume is almost out of disk space. Check this screen for messages.
- Check how much space remains on the sys: volume. If it is low, increase the size by adding free space.

To increase the amount of free space, do one or more of the following:

- Delete extraneous files (if you can log in from a workstation).
- At the server console prompt, enter `set immediate purge of files = on`, then retry the action.
- If you have an additional disk, increase the size of the volume by creating an additional segment of the volume on the disk.

Resolving Volume I/O Errors

To resolve a volume I/O error on Traditional volumes, try one or more of the following:

- Make sure that all devices that contain the volume are online. (Volumes can span multiple devices.)
- Repair the volume using the Vrepair utility.
- Make sure that the volume is visible.

If you have tried all of the above without success, contact a Novell Support Provider or the disk drive manufacturer.

Resolving Problems When the Server Hangs after Mounting the Last Volume

To diagnose problems when the server stops processing after mounting the last volume, identify whether the following conditions exist:

- Make sure the server network board is installed or seated correctly and is initializing when the server is started.
- Make sure that the server network board is configured correctly.
- Check the network board configurations of the boards in the server and the settings shown on the server and make sure that the settings match.
- Make sure that all server and workstation network boards are seated properly and that cabling and connections are attached securely.
- Make sure that the terminators on cables have the right ohm rating and are installed correctly. The IBM PC Cluster sends a broadcast message during initialization, then stops processing if the network is not cabled or terminated properly.
- Check the network boards in all workstations for correct node address settings.

Resolving Problems When No Volumes Mount

The sys: volume contains the NetWare system files and the NLM™ programs.

If the sys: volume does not mount when the server is booted, then the autoexec.ncf file does not execute, LAN drivers do not load, and the volume does not become part of the eDirectory tree.

To diagnose problems when no volumes mount, identify whether the following conditions exist:

- The sys: volume is corrupted.
- The server disk containing volume sys: volume has failed.
- The cable or power to the external server disks has malfunctioned.

To resolve problems when no volumes mount, do the following:

- Repair the volume using the utilities that are appropriate for the volume type.
- Check the cabling and power to the external server disks. Replace any faulty components.
- Replace the server disk containing the sys: volume.
  - Create the partitions and the sys: volume.
  - Restore the data from a backup copy.

Resolving Problems When Only Some Volumes Mount

To diagnose problems when only some volumes mount, identify whether the following conditions exist:

- The server does not have enough RAM
- The disk driver for external drives are not be loaded

To resolve problems when only some volumes mount, do the following:

- Add more RAM.
- Verify which drivers are loaded.

Resolving Disk Error Problems When a Volume Is Mounting

To diagnose problems when disk errors occur while a Traditional volume is mounting, identify whether the following conditions exist:

- The server does not have enough memory to mount the volume.
- The operating system is experiencing directory sector mismatching. This mismatching can be caused if the media is defective or if the server is turned off without the Down command.

To resolve disk error problems that occur while a volume is mounting:

- Check the status of the available cache buffers. If the available cache buffers are fewer than 20%, add more memory to your server.
- Minor errors usually correct themselves through normal network use. For example, if a FAT entry is wrong, the entry is updated and corrected the next time the table is written to. If errors do not correct themselves, repair the volume using the Vrepair utility.

Resolving Memory Errors When a Volume Is Mounting

To diagnose memory error problems when a Traditional volume mounts, identify whether the following conditions exist:

- Volumes take more memory to mount than they require after being mounted because the mounting process performs consistency checks (for example, the duplicate copies of all the tables are checked).
- Volumes and directory entries grow dynamically. Therefore, if your server is using most of the RAM (file cache buffers are close to 20% of the memory) and you dismount a volume, you might not be able to remount the volume unless additional memory is available.
- Each additional name space support that you add to a volume increases the size of the file allocation tables and directory entry tables. Adding name space support can cause the tables to grow so large that the server does not have enough RAM to mount the volume.

To resolve memory errors when a volume mounts, perform the following actions or ensure that the following conditions exist:

- Check the status of the available cache buffers. If the cache buffers are fewer than 20%, add more RAM to your server.
- Free up memory by unloading resources.

- On volumes using the Traditional file system, streamline the directory structure. Each subdirectory takes at least one directory block (by default, a 4 KB block of memory). Therefore, subdirectories with only one file require as much memory as directories with 32 files. Check the 4 KB size.

  If you combine directories so that most directories have about 32 files and you then purge the deleted subdirectories and files, you will free up memory.
- Calculate how much memory you need and add memory to the server.
- Remove any recently added name space support.

  WARNING: This is a destructive step that destroys all the extended file information. Before taking this step, try to free up enough memory so that the volume mounts and you can back up the data.

  Have all users log out, then unload all NLM programs except the volume's disk drivers. Dismount any mounted volumes.

  To remove the name space on a Traditional volume, load the Vrepair utility, select Set VRepair Options, then select the Remove Name Space Support from the Volume and Write All Directory and FAT Entries Out to Disk options. Exit to the main menu, then run VRepair > Repair a Volume on the volume that would not mount.

Resolving Volume Mounting Problems Because of Corrupted Directory Entry Tables or File Allocation Tables

To diagnose problems when mismatches exist in the duplicate copies of the FAT and directory entry table (DET) on Traditional volumes, identify whether the following conditions exist:

- A power failure has occurred and the server has not been shut down with the down command.
- A server disk has failed.
- A disk channel error has occurred.
- A volume does not dismount when you enter the dismount command.
- Directory information in cache is not completely written to disk.

To resolve problems when mismatches exist in the duplicate copies of the FAT and DET, do the following:

- Use the Vrepair utility to repair the disk.
- Add a UPS system so that the server is shut down automatically when a power failure occurs.
- Replace faulty disks or controllers.

Resolving Volume Mounting Problems Because of Name Space Module

After a volume has been configured to support more than the DOS naming convention, the name space NLM program must be loaded before the volume can be mounted.

To diagnose problems when a Traditional volume cannot mount because the name space NLM program is not loaded, identify whether the following conditions exist:

- The command to load the name space NLM is not in the startup.ncf file.
- The NLM to load the name space has not been copied to the boot directory of the server.

To resolve problems when a Traditional volume cannot mount because the name space NLM program is not loaded, do the following:

- Load the name space NLM program, then mount the volume. Copy the name space NLM to the server boot directory and add the load command to the startup.ncf file. The NLM then loads automatically whenever the server is booted.
- Delete the name space configuration from the volume.

  WARNING: This is a destructive step that destroys all of the extended file information.
- Back up all non-DOS files.
- Load the Vrepair utility, select Set VRepair Options, then select the Remove Name Space Support from the Volume and Write All Directory and FAT Entries to Disk options. Exit to the main menu, then run Vrepair > Repair a Volume on the volume that would not mount.

Other Troubleshooting Information

For other troubleshooting information on the Traditional file system and server operating system, see "Troubleshooting the NetWare Server" in the *NetWare 6.5 Server Operating System Administration Guide*.

8 Planning Your Directory Structure

This section presents a simple example of a network directory structure to help you plan your file system. Based on the example and the accompanying information, you can begin to design a directory hierarchy suitable to your own needs.

IMPORTANT: We recommend that you create separate volumes for applications and user data, reserving the sys: volume for the operating system and its extensions.

This section discusses the following topics:

- "Directories" on page 51
- "Drive Mappings" on page 54
- "Organizing Directory Structures Based on Access Requirements" on page 56
- "Managing Directory Structures for Network Applications" on page 56
- "Designing Application Directory Structures" on page 57
- "Designing Data Directory Structures" on page 59
- "Designing Home or User Directory Structures" on page 59
- "Access Rights and Organization of Your Directory Structure" on page 59

Directories

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

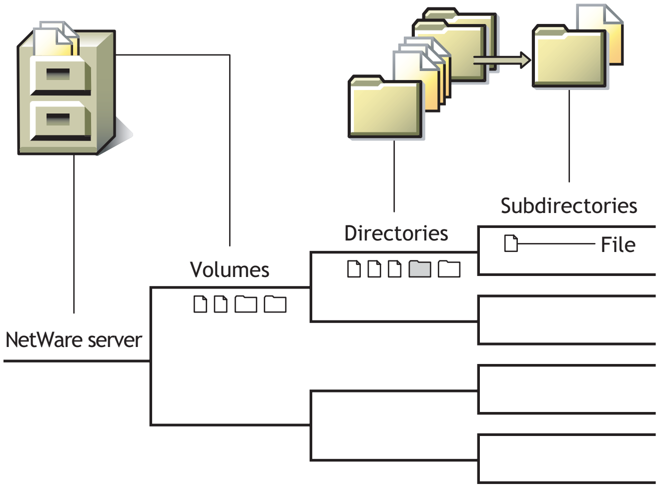
A directory is a logical separation within a volume where you store files and subordinate directories, called subdirectories. The directory is a special type of file that contains a list of its files and subdirectories. It can also contain metadata about the directory, such as who can access it and its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

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

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

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

Figure 2 Sample File Directory Structure



There is no one best solution for organizing files with directories. You can use a combination of approaches, such as by geographic location, applications, business units, projects, or owners.

To control who can access directories and files on your NSS and Traditional NetWare file systems, you must assign file system trustees, trustee rights, and inherited rights filters.

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

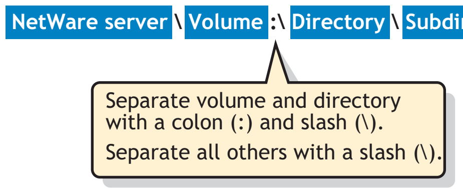
This section contains the following topics:

- "Directory Path" on page 52
- "Root Directory" on page 53
- "Fake Root Directory" on page 53
- "Directory Map Objects" on page 54

Directory Path

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

Figure 3 Directory Path Conventions


NetWare server \ Volume :\ Directory \ Subdirectory \ Filename
Separate volume and directory with a colon (:) and slash (\).
Separate all others with a slash (\).

If your network uses more than one client operating system, keep in mind the conventions of the different systems. For example, NetWare allows 255 characters in a directory path (counting the drive letter and delimiters), but DOS permits only 127 characters.

Also, some applications restrict the number of characters in the directory path. For more information, check the application's documentation.

Root Directory

The root directory is the base directory in the volume. The root is typically represented by a backslash (\).

The root directory of a volume typically contains only directories. Storing files at this level is possible, but it can be a security risk. Granting rights to files at the root of the volume necessitates granting rights to the entire volume.

To avoid this security risk, create Fake Roots for applications that want to write files to the root directory. For information, see "Fake Root Directory" on page 53.

Fake Root Directory

A fake root is a subdirectory that functions as a root directory.

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

NetWare allows you to map a drive to a fake root. This allows you to place applications in a subdirectory and assign rights to them there. For information about drive maps, see "Drive Mappings" on page 54.

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

Creating a Fake Root Directory

To use an application that must be installed at the root, load the files in a subdirectory, then designate the subdirectory as a fake root directory in the login script by using the Map Root command.

For example, suppose you have an application in a directory named *myapp* that must reside in the root directory of drive P:, but you do not want to put the application in the root directory for security reasons. You can map a fake root to the directory and map a search drive to it at the same time by adding the following line to the Novell Client login script:

```
map root s16:=p:= apps:devapps\myapp
```

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

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

Directory Map Objects

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

If you create a Directory Map object to point to an application, users can access the application by mapping a drive to the Directory Map object. If the application's location in the directory structure changes, you can update the object instead of changing all users' drive mappings.

Using a Directory Map Object

Directory Map objects can be especially useful in Novell Client login scripts to point to directories that contain applications or other frequently used files. In Novell Client login scripts, you can map a drive to a Directory Map object instead of to the directory. If the application's location in the directory structure changes, you can update the path in the Directory Map object instead of changing the related drive maps in numerous login scripts. For information about Map commands, see "Login Script Commands and Variables" in the *Novell Login Scripts Guide*.

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

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

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

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

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

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

Additional Information

For information, see "Object Classes and Properties" in the *Novell eDirectory 8.7.3 Administration Guide*.

Drive Mappings

A drive mapping is a pointer to a location in the file system, represented as a letter assigned to a directory path on a volume. The directory path includes the volume, directory, and any subdirectories leading to the file. A drive map assigns a letter to a path so that the letter can be used instead of the complete path name.

Drive mappings can be temporary or permanent:

- **Permanent Mappings:** To make drive mappings permanent so you can use them every time you log in, place Map commands in your Novell Client login script, or use the mapping functionality of your client operating system to make them permanent, so they will be reconnected every time you log in.
- **Temporary Mappings:** To map a drive so you can use it during your current session, use the NetWare Map command from a DOS prompt, or use the mapping functionality of your client software. If you use the Map command from a DOS prompt, the mapping is only valid until you log out.

For instructions on creating drive mappings, see "Creating eDirectory Objects to Facilitate File Management" in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

NetWare recognizes three types of drive mappings:

- Local Drive Mappings
- Network Drive Mappings
- Network-Search Drive Mappings

For information about how to use the NetWare Map command, see Map (http://www.novell.com/documentation/nw65/utlrfenu/data/h7onc376.html) in the *NetWare 6.5 Utilities Reference* or see "Login Script Commands and Variables" in the *Novell Login Scripts Guide*.

Local Drive Mappings

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

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

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

```
lastdrive=Z
```

Network Drive Mappings

Network drive mappings point to volumes and directories on the network. Normally, drives F: through Z: are used for network mappings. Each user can map drive letters to different directories.

To create a network drive mapping, use the Map command. For information, see the Map command in the *NetWare 6.5 Utilities Reference*.

Network-Search Drive Mappings

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

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

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

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

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

Organizing Directory Structures Based on Access Requirements

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

Organizing the Directory Structure

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

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

Grouping the User Community

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

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

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

Managing Directory Structures for Network Applications

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

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

For information, see “Fake Root Directory” on page 53.

- After you install the application:
  - Designate Novell eDirectory organization, role, and user objects as file system Trustees for the application directory and its contents.
  - Assign access rights for each trustee.
  - Configure attributes for the directory and its files.
- To allow users to access network-based applications, map search drives to the directories that contain these applications. For information, see “Network-Search Drive Mappings” on page 55.

  To make the mapped search drives permanent, place them in login scripts, which are executed when users log in. For information, see the *Novell Login Scripts Guide*.
- You can create a Directory Map object that points to an application directory.

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

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

Designing Application Directory Structures

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

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

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

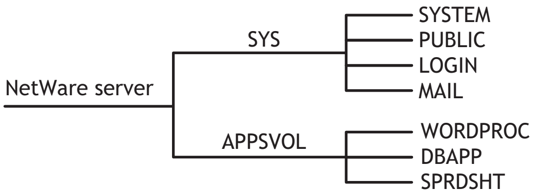
This section describes the following examples of application directory structures:

- “Application Volume with Separate Application Directories Off Its Root” on page 58
- “Sys: Volume with a Parent Application Directory Off Its Root” on page 58
- “Sys: Volume with Separate Application Directories Off Its Root” on page 58
- “Sys:public Directory with a Parent Application Directory” on page 58

Application Volume with Separate Application Directories Off Its Root

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

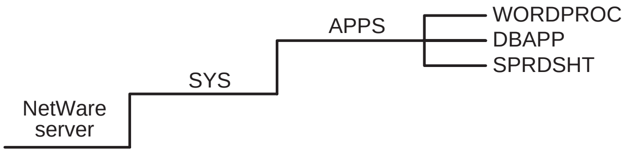
Figure 4 Application Volume with Separate Application Directories Off Its Root



Sys: Volume with a Parent Application Directory Off Its Root

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

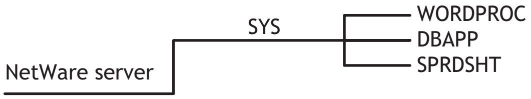
Figure 5 Sys: Volume with a Parent Application Directory Off Its Root



Sys: Volume with Separate Application Directories Off Its Root

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

Figure 6 Sys: Volume with Separate Application Directories Off Its Root

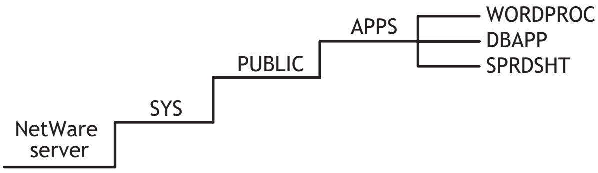


Sys:public Directory with a Parent Application Directory

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

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

Figure 7 Sys:public Directory with a Parent Application Directory



Designing Data Directory Structures

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

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

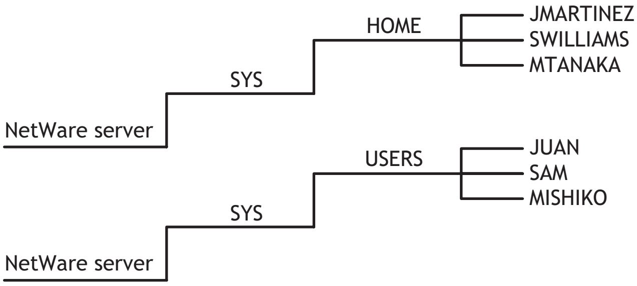
Designing Home or User Directory Structures

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

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

If you decide to use the sys: volume, create a parent directory in volume sys:, such as home or users. Within the parent directory, the name of each subdirectory should be the username. Usernames can be up to 47 characters, but DOS displays only 8 characters in a one-level directory name.

Figure 8 Home or User Directory Structure



Access Rights and Organization of Your Directory Structure

Security is one of the most important aspects of file system organization. Novell eDirectory™ rights and the file system's directory and file attributes allow you to determine who can access what, and whether that access amounts to being able to merely read a file or modify it. For information, see "Security: Granting Trustee Rights to Directories and Files" on page 68.

Organizing the Directory Structure

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

For example, you can structure the hierarchy of directories in such a way as to take advantage of the inheritance aspect of rights.

Rights can be associated with volumes, directories, and files as a safeguard against deletion or modification by users. Directory and file attributes can also be used to control what users can do.

Grouping the User Community

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

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

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

9 Configuring and Managing Directories and Files

The procedures in this section focus on the following system administration tasks:

Identify the task you want to complete and find an appropriate procedure. Then, use links associated with the procedure for more information about ways in which applications and utilities can be used.

This section focuses primarily on setting up directories, files, drives, and security. For instructions on creating Traditional partitions and volumes, see "Configuring and Managing Traditional File System" on page 15. System administrators are concerned with all of these aspects of the file system. Users will be concerned with drive mapping and with some of the file and directory procedures.

Creating a Directory

You create directories in Novell Remote Manager, Novell NetStorage, the Novell Client™ for Windows 2000/XP, or by mapping a drive from your workstation to the network volume with CIFS.

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

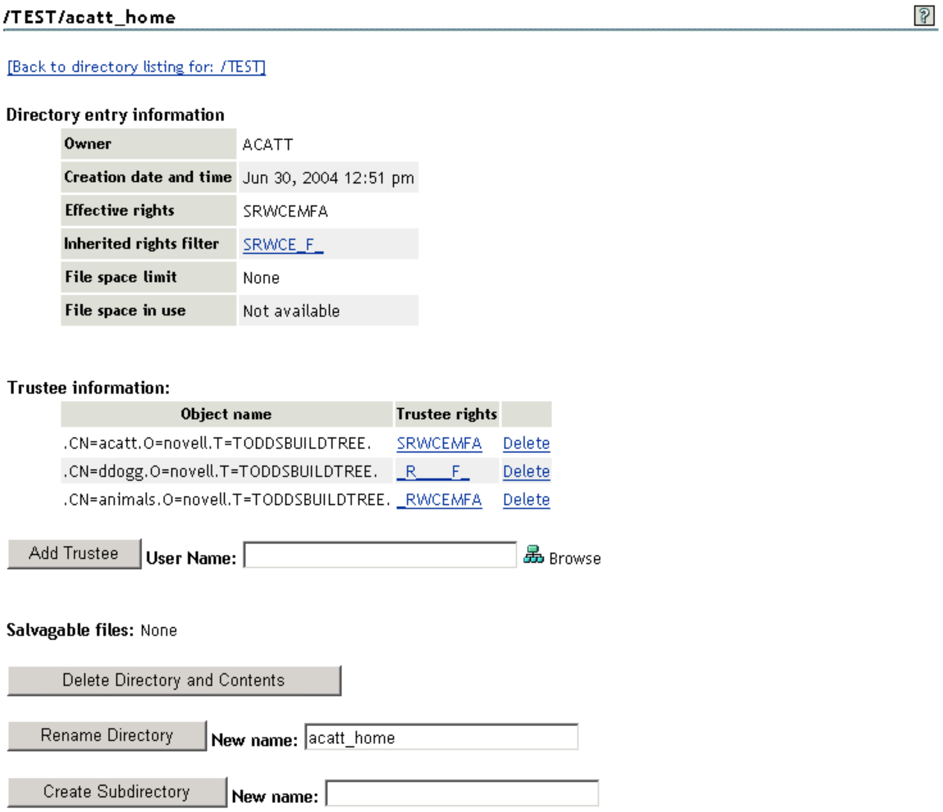
1 In your Web browser, log in to Novell Remote Manager on the NetWare server where you want to create a directory in an NSS volume. The general form of the URL is

   http://*192.168.1.1*:8008

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

2 Click Manage Server > Volumes.

3 Click the Properties icon next to the Volume you want to manage.



/TEST/acatt_home

[Back to directory listing for: /TEST]

Directory entry information

Owner	ACATT
Creation date and time	Jun 30, 2004 12:51 pm
Effective rights	SRWCEMFA
Inherited rights filter	SRWCE_F_
File space limit	None
File space in use	Not available

Trustee information:

Object name	Trustee rights	
.CN=acatt.O=novell.T=TODDSBUILDTREE.	SRWCEMFA	Delete
.CN=ddogg.O=novell.T=TODDSBUILDTREE.	_R____F_	Delete
.CN=animals.O=novell.T=TODDSBUILDTREE.	_RWCEMFA	Delete

User Name:

Salvagable files: None

New name: acatt_home

New name:

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

Viewing Directory and File Information

You can see extended information about a directory or file by using Novell Remote Manager, Novell NetStorage, or the Novell Client. For instructions on viewing directory and file information, see "Viewing Details of Directories or Files and Performing Specific Actions on Them" in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

You can view file information such as

- Owner and trustees
- Attributes, effective rights, and the Inherited Rights Filter (IRF)
- Name space

- File size
- Creation, access, archive, and modify dates

You can view directory information such as

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

Copying or Moving Directories and Files

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

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

To move a directory's subdirectories and files, you must also have the Erase right to the source directory, because moving files includes deleting them from the source directory. For instructions, see "Viewing Details of Directories or Files and Performing Specific Actions on Them" in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Creating a Fake Root Directory with the Map Root Command

If your application must be installed at the root, load the files in a directory, then use the Map Root command in the login script to designate the directory as a fake root directory. For information about using the Map command in a login script, see "Login Script Commands and Variables" in the *Novell Login Scripts Guide*.

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

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

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

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

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

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

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

For more information, see the *Novell Login Scripts Guide*.

Creating and Configuring a Directory Map Object

A Directory Map object represents a particular directory in a file system. For example, Directory Map objects can point to directories that contain frequently used files such as applications.

If you create a Directory Map object to point to an application, users can access the application by mapping a drive to the Directory Map object.

1 In your Web browser, log in to Novell iManager on the NetWare 6.5 server where you want to create the Directory Map object. The general form of the URL is

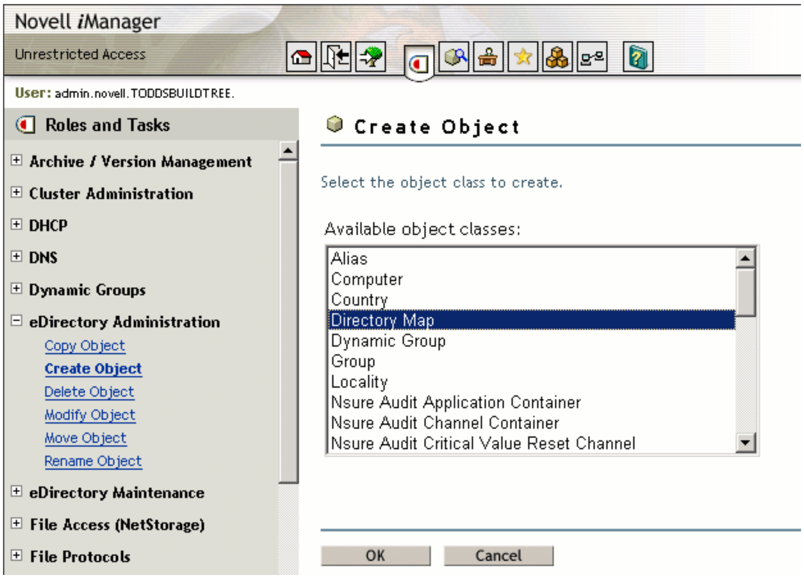
http://*192.168.1.1*/nps/iManager

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

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

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

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



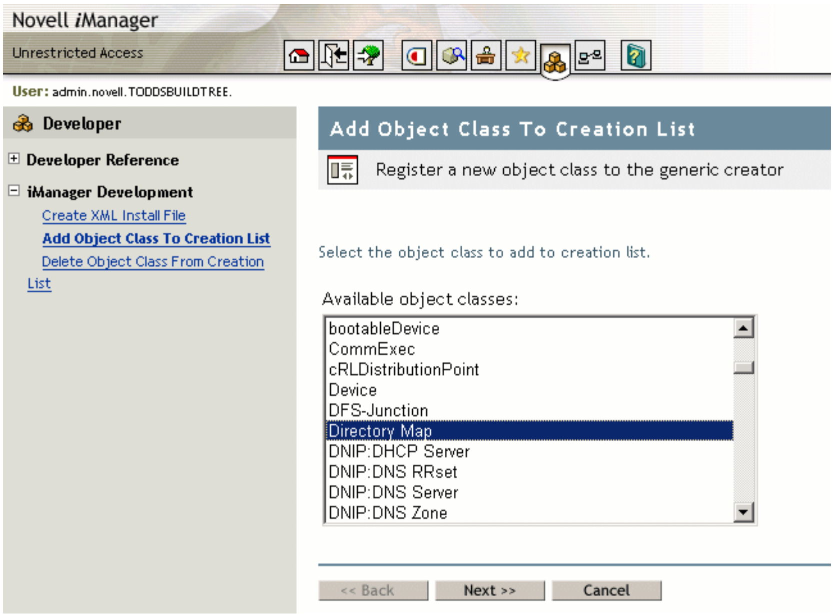
3 (Conditional) If Directory Map is not one of the Available Object Classes, you must add the Directory Map object class to the list.

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

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

3a In iManager, click the Developer icon.

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



Novell *i*Manager

Unrestricted Access

User: admin.novell.TODDSBUILDTREE.

Developer

⊞ Developer Reference

⊟ iManager Development

Create XML Install File

Add Object Class To Creation List

Delete Object Class From Creation List

Add Object Class To Creation List

Register a new object class to the generic creator

Select the object class to add to creation list.

Available object classes:

bootableDevice
CommExec
cRLDistributionPoint
Device
DFS-Junction
Directory Map
DNIP:DHCP Server
DNIP:DNS RRset
DNIP:DNS Server
DNIP:DNS Zone

<< Back | Next >> | Cancel

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

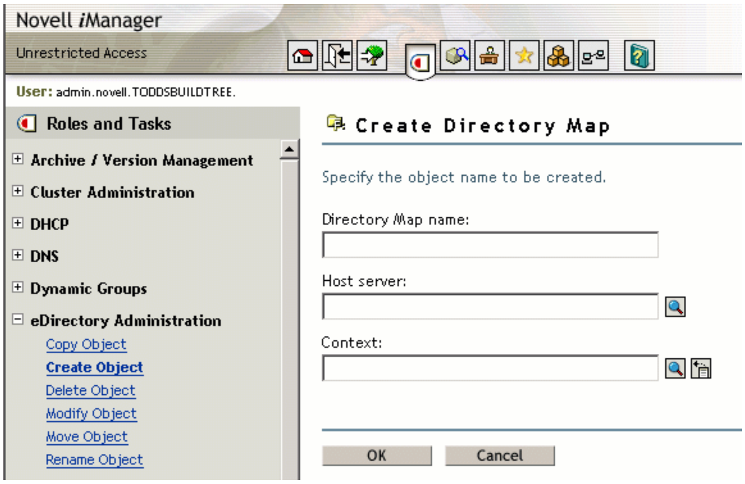
3d At the summary page, verify that the value of the <class-name> entry is com.novell.emframe.fw.GenericCreator, click Finish, then click OK.

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

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

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

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



Novell *i*Manager

Unrestricted Access

User: admin.novell.TODDSBUILDTREE.

Roles and Tasks

⊞ Archive / Version Management

⊞ Cluster Administration

⊞ DHCP

⊞ DNS

⊞ Dynamic Groups

⊟ eDirectory Administration

Copy Object

Create Object

Delete Object

Modify Object

Move Object

Rename Object

Create Directory Map

Specify the object name to be created.

Directory Map name:

Host server:

Context:

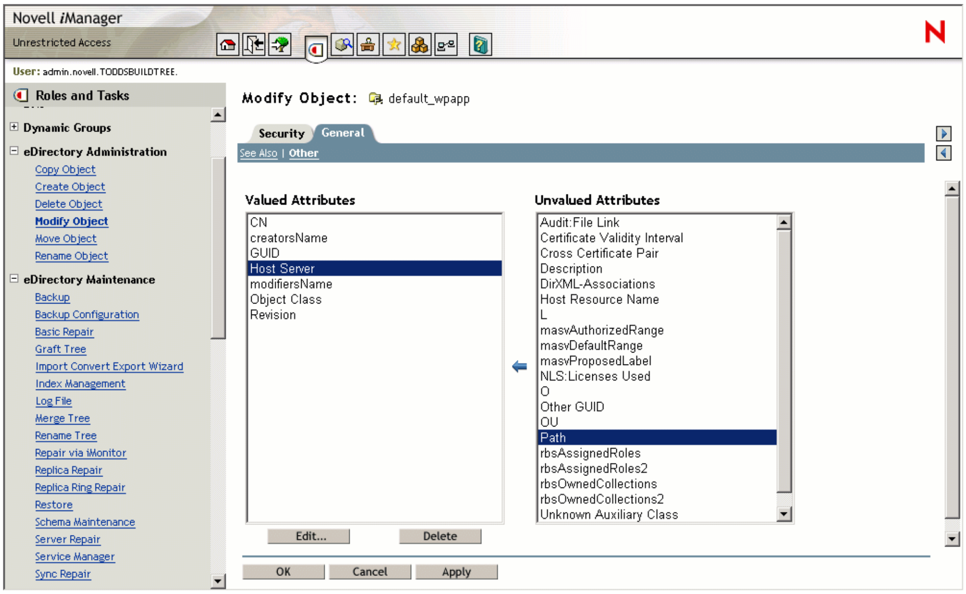
OK | Cancel

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

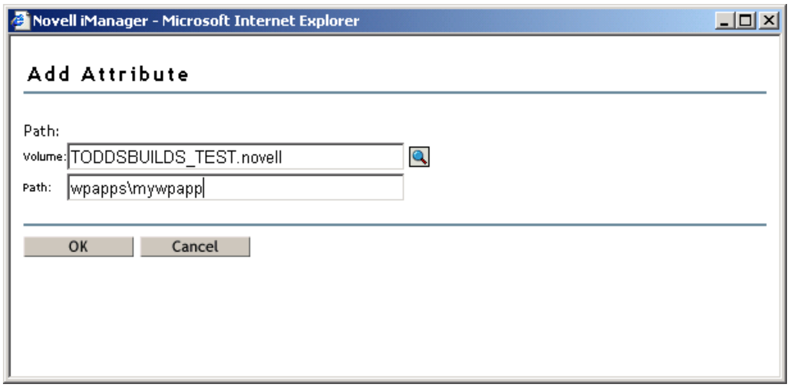
- **Directory Map Name:** Type the common name that represents this Directory Map object for use in Map and Map Root commands.
- **Host Server:** Select the NetWare 6.5 server where the directory resides.

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

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



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



Volume: TODDSBUILDS_TEST.novell

Path: wpapps\mywpapp

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

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

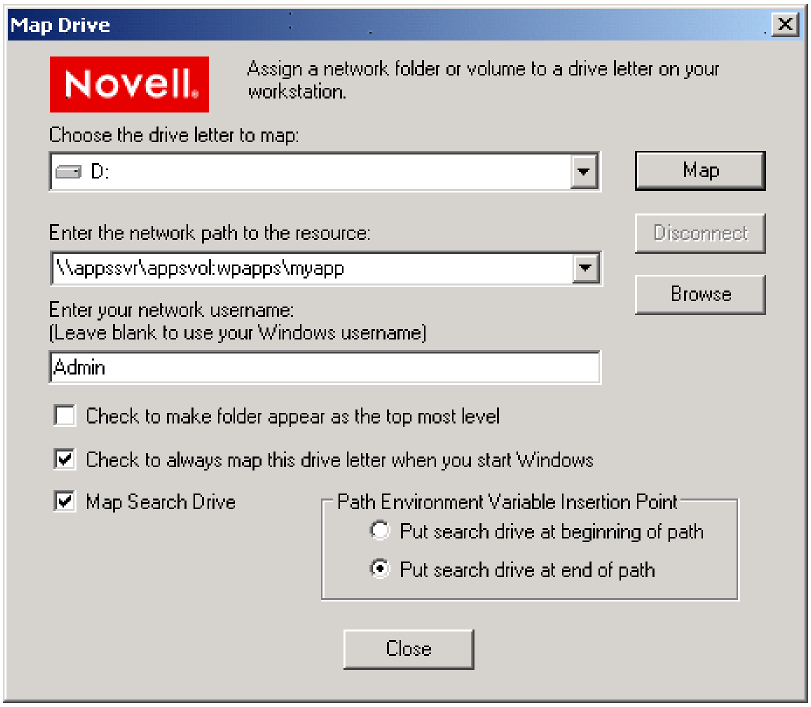
9 (Conditional) If the path you specified for the Directory Map object does not exist on the NetWare 6.5 server, create the specified path.

For more information about creating a Directory Map Object, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

For an example of how you could use Directory Map objects to reduce maintenance of login scripts, see "Using Directory Map Objects" on page 23.

Mapping Network Drives

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



Map Drive

Assign a network folder or volume to a drive letter on your workstation.

Choose the drive letter to map: D:

Enter the network path to the resource: \\appssvr\appsvol:wpapps\myapp

Enter your network username:
(Leave blank to use your Windows username)
Admin

☐ Check to make folder appear as the top most level

☑ Check to always map this drive letter when you start Windows

☑ Map Search Drive

Path Environment Variable Insertion Point

○ Put search drive at beginning of path

● Put search drive at end of path

2. Specify a drive letter to map.
3. Type or browse to the path to the network resource where you want to map a drive.
4. Specify the login name to use for the map.

   If none is provided, the client uses your Windows logon username. If necessary, the client later prompts you for the password that matches the server login username you provide.
5. (Optional) Enable the Check to Make Folder Appear as the Top-Most Level option.
6. (Optional) Enable the Check to Always Map This Drive Letter When You Start Windows option.
7. (Optional) Enable the Map Search Drive option. Specify whether to put the search drive at the beginning or end of the path.
8. Click Map.

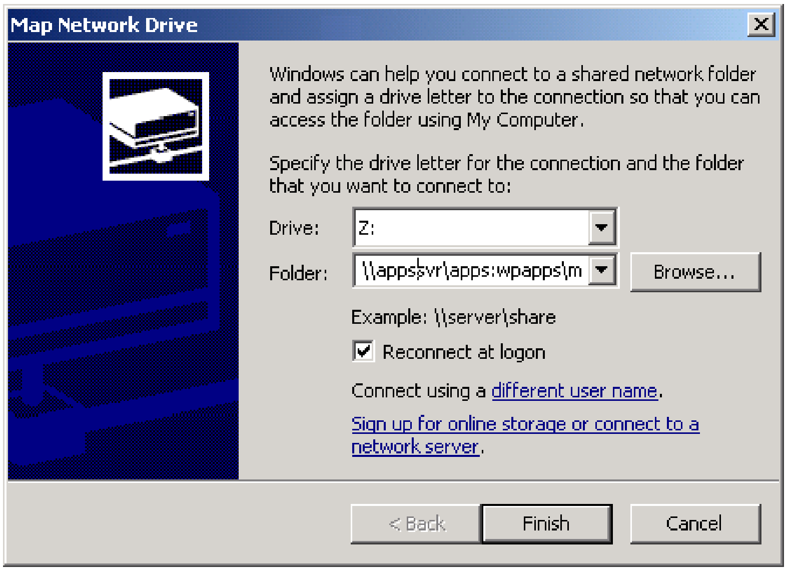
For more information, see "Common Networking Tasks" in the *Novell Client for Windows Installation and Administration Guide*.

You can also map network drives by placing commands in the Novell Client login scripts. For information, see the *Novell Login Scripts Guide*.

Mapping Network Drives with Windows Explorer

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

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



Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\appssvr\apps:wpapps\m

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

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 recur for subsequent logins to the network, enable Reconnect at Logon.

5 Click Finish.

Mapping Network Drives on DOS Clients with the Map Command

You can also use native methods for mapping drives on your DOS client. Use the Map command to map drives and search drives to network directories. For a general description of the Map command, see "MAP" in the *NetWare 6.5 Utilities Reference*.

Security: Granting Trustee Rights to Directories and Files

File system security includes assigning trustee rights. To set up rights, see the following:

- "File System Trustee Rights" on page 68
- "Adding a Trustee to a Directory or File" on page 72
- "Viewing/Modifying the Inherited Rights Filter for Directories and Files" on page 73

For Windows information, see "NetWare File Security" in the *Novell Client for Windows Installation and Administration Guide*.

File System Trustee Rights

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

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

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

File system Trustee rights assigned to files and subdirectories redefine the rights that users inherit from directory rights.

Eight file system Trustee rights can be granted at either the directory or file level, as described in the table below:

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

Inherited Rights Masks

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

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

At each level, the IRM is applied to all rights inherited from the parent directory. Only those rights allowed by the mask are inherited by the child object. Rights for the various trustees explicitly assigned to the child are then collected. When a trustee inherits rights from above, the new rights replace the old ones (except the Supervisor right, which cannot be masked or removed by a new assignment to the same trustee).

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

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

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

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

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

Visibility Lists

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

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

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

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

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

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

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

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

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

Supervisor Trustee Rights

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

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

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

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

Trustee Assignments for a Volume

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

Default Trustee Rights

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

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

Inherited Trustee Rights

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

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

Public Trustee Rights

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

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

Example of Rights Needed for Typical Access Tasks

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

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

Adding a Trustee to a Directory or File

Prerequisite

- ❑ The Access Control right to the directory or file you want to add the trustee to.

Procedure

You can add, modify, or delete a trustee in a directory or file using ConsoleOne®. For instructions on adding, modifying, and deleting trustees, see "Managing Novell eDirectory" in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Viewing/Modifying the Inherited Rights Filter for Directories and Files

For instructions on viewing or modifying the Inherited Rights Filter, see "Managing Novell eDirectory" in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

The Connection Manager for NetWare

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

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

Connections to the NetWare Traditional File System

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

Connections to the NSS File System

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

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

If this fails to provide a method of access, NSS then checks the Visibility list to see if the requested object is a parent directory that requires visibility due to a rights assignment for a child directory. For information about the Visibility list, see "Visibility Lists" on page 70.

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

NSS does not directly access the connection table. However, it does make calls to read information from it to form its own connection table with GUIDs and file system Trustee rights.

Setting Directory or File Attributes

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

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

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

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

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

Attribute Code	Description	Applies to
A	Archive Needed identifies files that have been modified since the last backup. This attribute is assigned automatically.	Files only
Ci	Copy Inhibit prevents users from copying a file. This attribute overrides the trustee Read right and File Scan right.	Files only
Dc	Do Not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Directories and files
Di	Delete Inhibit prevents users from deleting a directory or file. This attribute overrides the trustee Erase right. When it is enabled, no one, including the owner and network administrator, can delete the directory or file. A trustee with the Modify right must disable this right to allow the directory or file to be deleted.	Directories and files
Dm	Do Not Migrate prevents directories and files from being migrated from the server's server disk to another storage medium.	Directories and files
Ds	Do Not Suballocate prevents data from being suballocated.	Files only
H	The Hidden attribute hides directories and files so they do not appear in a file manager or directory listing.	Directories and files
I	Index allows large files to be accessed quickly by indexing files with more than 64 File Allocation Table (FAT) entries. This attribute is set automatically.	Files only
Ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed.	Directories and files
N	Normal indicates the Read/Write attribute is assigned and the Shareable attribute is not. This is the default attribute assignment for all new files.	Directories and files
P	Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Directories and files
Ri	Rename Inhibit prevents the directory or file name from being modified.	Directories and files

Attribute Code	Description	Applies to
Ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Files only
Rw	Read/Write allows you to write to a file. All files are created with this attribute.	Files only
Sh	Shareable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Files only
Sy	The System attribute hides the directory or file so it does not appear in a file manager or directory listing. System is normally used with operating system files, such as DOS system files.	Directories and files
T	Transactional allows a file to be tracked and protected by the Transaction Tracking System™ (TTS™).	Files only
X	The Execute attribute indicates program files such as .exe or .com.	Files only

Tools for Managing File System Trustees and Attributes

- "Accessing Novell NetStorage" on page 75
- "Accessing the Novell Client for Windows 2000/XP" on page 76
- "Accessing Novell Remote Manager for NetWare (NetWare)" on page 76

Accessing Novell NetStorage

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

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

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

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

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

NetStorage uses Novell eDirectory™ for authentication. Log in with your administrator username and password to manage file system access for directories and files on NSS volumes. You can also log in as any username with equivalent rights to the administrator. This limititation 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.

Accessing the Novell Client for Windows 2000/XP

In combination with NCP Server on your NetWare server, the Novell Client™ for Windows 2000/XP 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 *Novell Client for Windows Installation and Administration Guide*.

Accessing Novell Remote Manager for NetWare (NetWare)

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

   http://*192.168.1.1*:8008

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

Generating a Server Security Report (NetWare)

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

To generate the Security report for your NetWare server:

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

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

- Trustee assignments for each volume

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

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

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

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

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

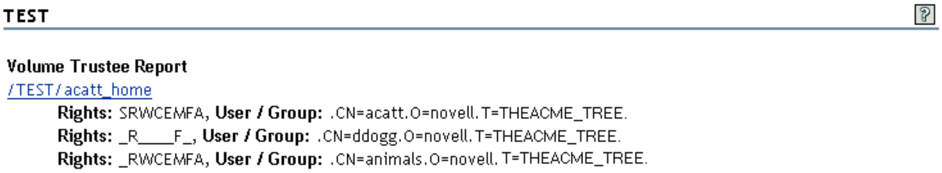
Viewing a File System Trustee Report for a Volume (NetWare)

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

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

2 Click the Info icon next to volume you are monitoring.

3 Scroll down the page, then click the Volume Trustee Report link.



TEST

Volume Trustee Report

/TEST/acatt_home

Rights: SRWCEMFA, User / Group: .CN=acatt.O=novell.T=THEACME_TREE.
Rights: _R____F_, User / Group: .CN=ddogg.O=novell.T=THEACME_TREE.
Rights: _RWCEMFA, User / Group: .CN=animals.O=novell. T=THEACME_TREE.

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

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

- "Using Novell NetStorage" on page 77
- "Using the Novell Client to Manage Trustees and Trustee Rights" on page 78
- "Using the Novell Client to Manage Inherited Rights and Filters" on page 79
- "Using Novell Remote Manager for NetWare (NetWare)" on page 80

Using Novell NetStorage

1 Open your Web browser to NetStorage and log in.

  For information, see "Accessing Novell NetStorage" on page 75.

2 Right-click the directory or file you want to manage, then select Properties.

3 Click the NetWare Info tab to view or modify attributes or the NetWare Rights tab to view or modify rights.

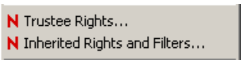
  Although the option label refers to NetWare, use the option for your NSS volumes on NetWare.

  For information, see "File System Trustee Rights" on page 68.

Using the Novell Client to Manage Trustees and Trustee Rights

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

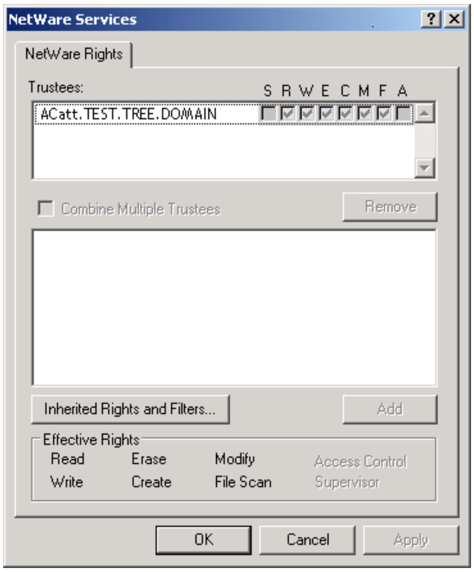
1 In a file manager, right-click the network directory or file, then select Trustee Rights.



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

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

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



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

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

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

Do one or more of the following:

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

Select one or more trustees from the Trusees 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.

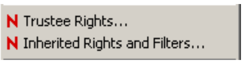
5 Click OK.

Using the Novell Client to Manage Inherited Rights and Filters

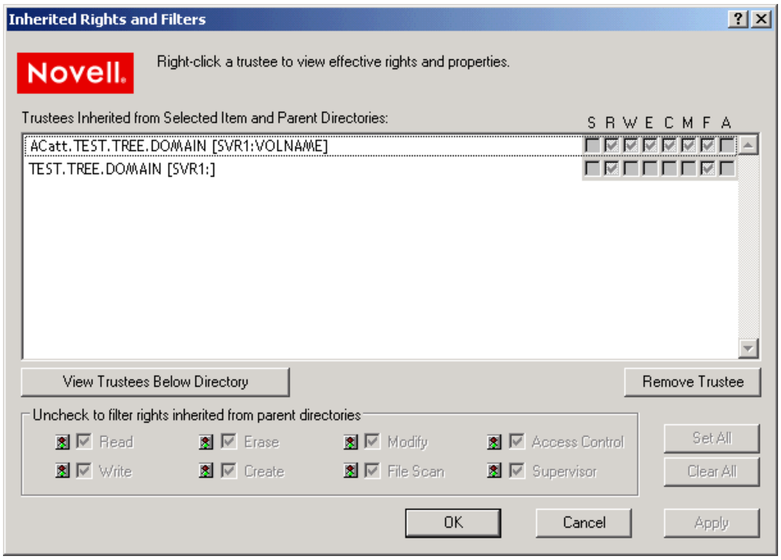
Administrators and users can manage file system inherited rights and filters for network directories and files, using the Novell Client on their workstations. For information about filtering inherited rights, see "Inherited Trustee Rights" on page 72.

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.



Inherited Rights and Filters

Right-click a trustee to view effective rights and properties.

Trustees Inherited from Selected Item and Parent Directories:

	S	R	W	E	C	M	F	A
ACatt.TEST.TREE.DOMAIN [SVR1:VOLNAME]	☐	☑	☑	☑	☑	☑	☑	☐
TEST.TREE.DOMAIN [SVR1:]	☐	☑	☐	☐	☐	☐	☑	☐

Uncheck to filter rights inherited from parent directories

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

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.

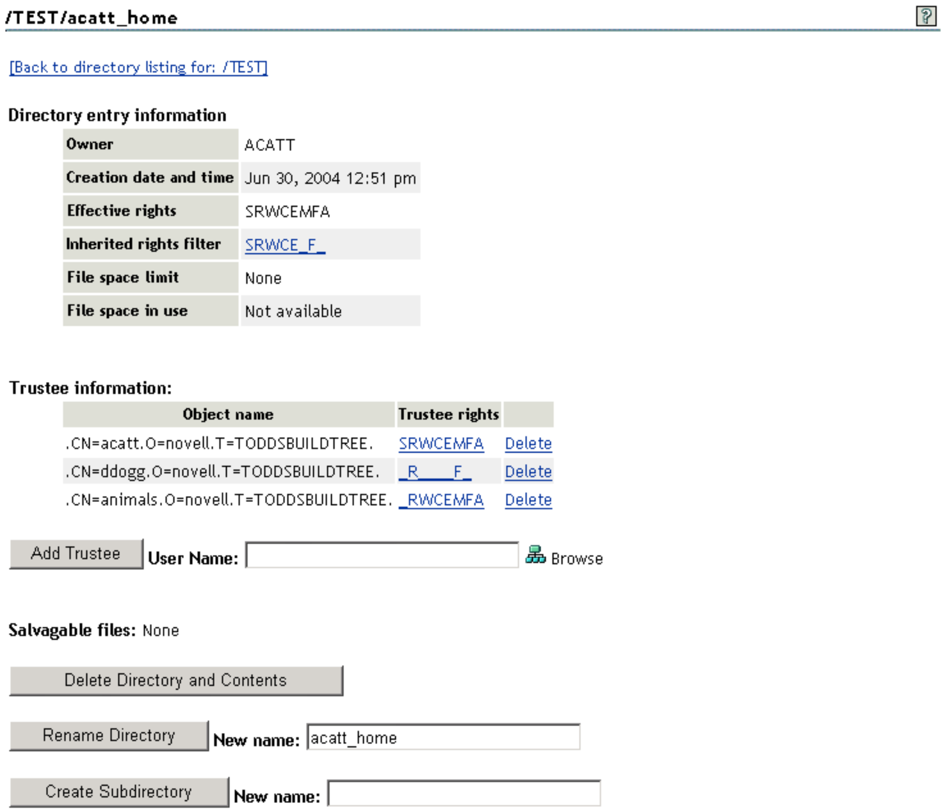
- **Delete a Trustee:** Select the trustee you want to manage from the Trustees Inherited from Selected Item and Parent Directories, then click Remove Trustee.

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.

Using Novell Remote Manager for NetWare (NetWare)

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

1. In Novell Remote Manager, click Manage Server > Volumes to open the Volume Management page.
2. Click the Volume link of the volume you want to manage.
3. Browse to the directory or file you want to manage.
4. Click the Properties icon to the left of the directory or file you want to manage.



/TEST/acatt_home

[Back to directory listing for: /TEST]

Directory entry information

Owner	ACATT
Creation date and time	Jun 30, 2004 12:51 pm
Effective rights	SRWCEMFA
Inherited rights filter	SRWCE_F_
File space limit	None
File space in use	Not available

Trustee information:

Object name	Trustee rights	
.CN=acatt.O=novell.T=TODDSBUILDTREE.	SRWCEMFA	Delete
.CN=ddogg.O=novell.T=TODDSBUILDTREE.	_R____F_	Delete
.CN=animals.O=novell.T=TODDSBUILDTREE.	_RWCEMFA	Delete

Salvagable files: None

New name: acatt_home

5. Do one or more of the following:
   - **Add a Trustee:** Type the full distinguished name or bindery name of the User object you want to add in the User Name field of the Trustee Information, or browse to the User object and select it, then click Add Trustee.
   - **Modify Trustee Rights:** Locate the User object name in the list of User objects under the Trustee Information, then click the Trustee Rights link next to the username. Select or deselect the check box for the trustee right you want to change, then click OK.
   - **Delete a Trustee:** Locate the User object name in the list of User objects under the Trustee Information, then click the Delete link next to the username.

- **Modify the Inherited Rights Filter:** Click the Inherited Rights Filter link in the directory or file information table. Select or deselect the check box for the rights you want to modify, then click OK.

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

Managing Attributes for Directories and Files

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

- "Using Novell NetStorage" on page 81
- "Using the Novell Client" on page 81
- "Using Novell Remote Manager (NetWare)" on page 82
- "Using the NetWare GUI (NetWare)" on page 83

For information about NetWare directory and file attributes and how to apply them, see "File System Trustee Rights" on page 68.

Using Novell NetStorage

1 Open your Web browser to NetStorage and log in.

  For information, see "Accessing Novell NetStorage" on page 75.

2 Right-click the directory or file you want to manage, then select Properties.

3 Click the NetWare Info tab to view or modify attributes for the selected directory or file.

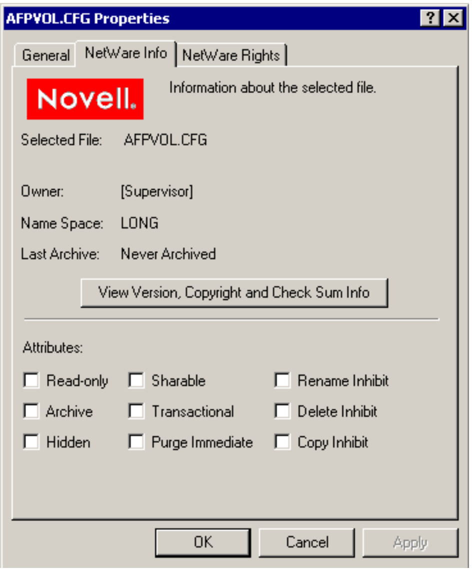
  Although the option label refers to NetWare, use the option for your NetWare NSS volumes.

  For information, see "File System Trustee Rights" on page 68

Using the Novell Client

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

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



Information about the selected file.

Selected File: AFPVOL.CFG

Owner: [Supervisor]

Name Space: LONG

Last Archive: Never Archived

Attributes:

☐ Read-only ☐ Sharable ☐ Rename Inhibit
☐ Archive ☐ Transactional ☐ Delete Inhibit
☐ Hidden ☐ Purge Immediate ☐ Copy Inhibit

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

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

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

3 Click OK.

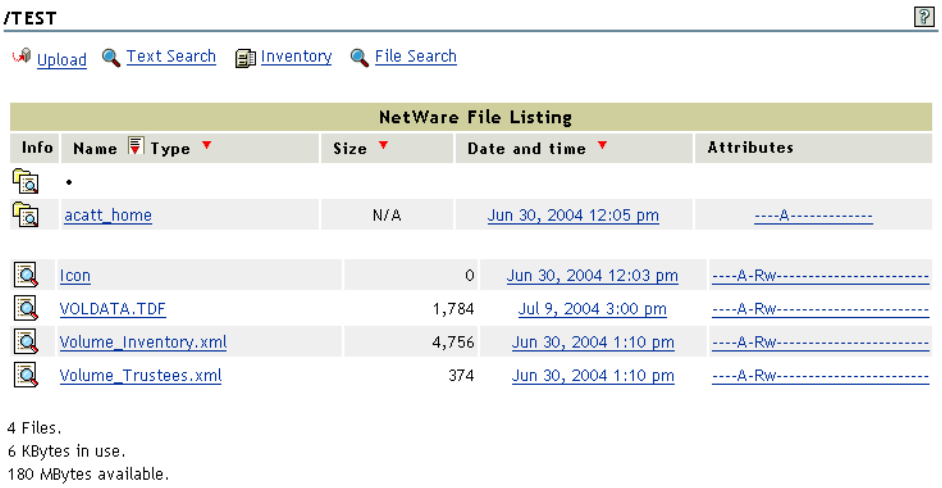
Using Novell Remote Manager (NetWare)

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

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

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

4 View the resource's attributes in the Attributes column.

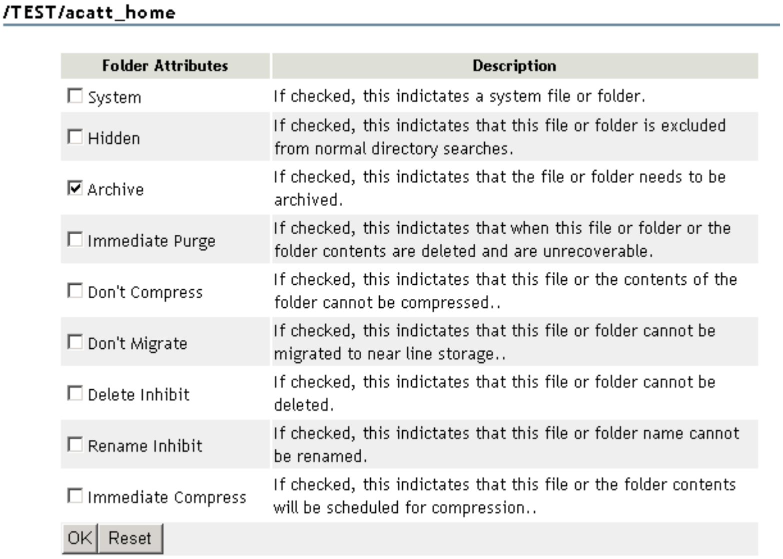


NetWare File Listing

Info	Name Type	Size	Date and time	Attributes
	.			
	acatt_home	N/A	Jun 30, 2004 12:05 pm	----A------------
	Icon	0	Jun 30, 2004 12:03 pm	----A-Rw----------------------
	VOLDATA.TDF	1,784	Jul 9, 2004 3:00 pm	----A-Rw----------------------
	Volume_Inventory.xml	4,756	Jun 30, 2004 1:10 pm	----A-Rw----------------------
	Volume_Trustees.xml	374	Jun 30, 2004 1:10 pm	----A-Rw----------------------

4 Files.
6 KBytes in use.
180 MBytes available.

5 To modify the attributes, click the Attributes link.



/TEST/acatt_home

Folder Attributes	Description
□ System	If checked, this indictates a system file or folder.
□ Hidden	If checked, this indictates that this file or folder is excluded from normal directory searches.
☑ Archive	If checked, this indictates that the file or folder needs to be archived.
□ Immediate Purge	If checked, this indictates that when this file or folder or the folder contents are deleted and are unrecoverable.
□ Don't Compress	If checked, this indictates that this file or the contents of the folder cannot be compressed..
□ Don't Migrate	If checked, this indictates that this file or folder cannot be migrated to near line storage..
□ Delete Inhibit	If checked, this indictates that this file or folder cannot be deleted.
□ Rename Inhibit	If checked, this indictates that this file or folder name cannot be renamed.
□ Immediate Compress	If checked, this indictates that this file or the folder contents will be scheduled for compression..

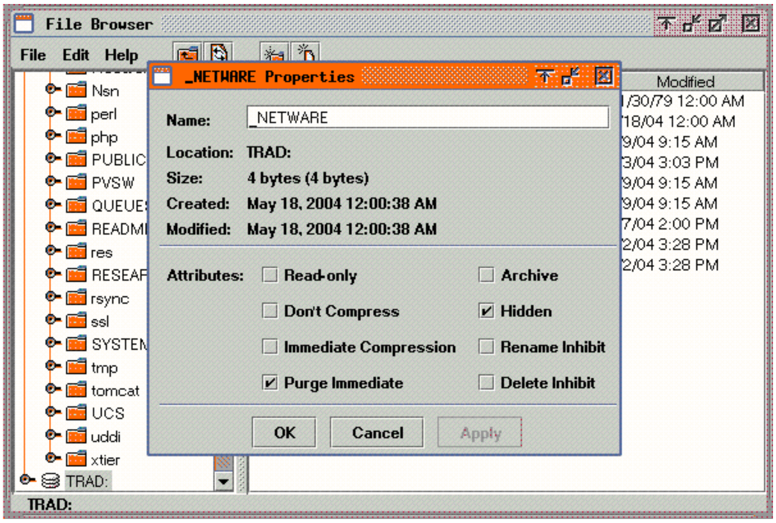
6 Select or deselect the check box for the attribute you want to set.

7 Click OK.

Using the NetWare GUI (NetWare)

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

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



Name: _NETWARE

Location: TRAD:

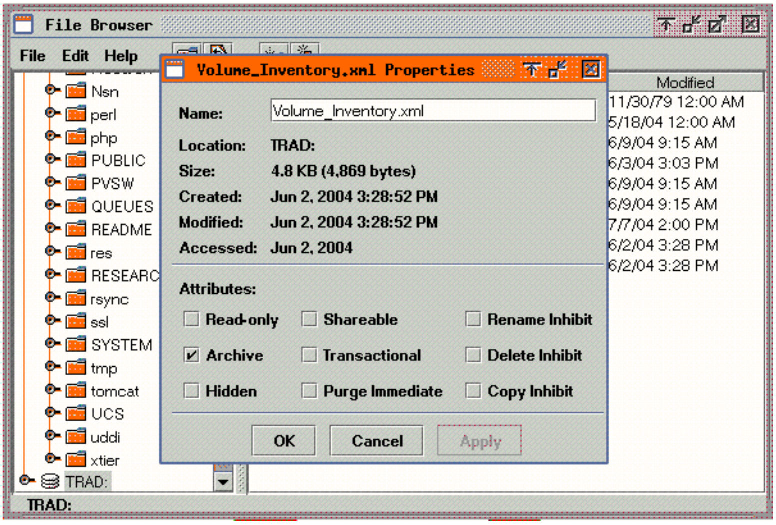
Size: 4 bytes (4 bytes)

Created: May 18, 2004 12:00:38 AM

Modified: May 18, 2004 12:00:38 AM

Attributes:

□ Read-only	□ Archive
□ Don't Compress	☑ Hidden
□ Immediate Compression	□ Rename Inhibit
☑ Purge Immediate	□ Delete Inhibit



Name: Volume_Inventory.xml

Location: TRAD:

Size: 4.8 KB (4,869 bytes)

Created: Jun 2, 2004 3:28:52 PM

Modified: Jun 2, 2004 3:28:52 PM

Accessed: Jun 2, 2004

Attributes:

□ Read-only	□ Shareable	□ Rename Inhibit
☑ Archive	□ Transactional	□ Delete Inhibit
□ Hidden	□ Purge Immediate	□ Copy Inhibit

3 View the attributes in the Attribute area.

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

5 Click OK.

Trustee Rights Utility for NetWare

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

Purpose

Use this utility iconiconat a workstation to

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

Syntax

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

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

RIGHTS Options

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

File and Directory Rights

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

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

Using RIGHTS

- If you use + (plus) to add rights, the rights you list are added to the existing rights.
- If you use - (minus) to remove rights, the rights you list are deleted from the existing rights.
- If you add and delete rights in the same command, group all added rights together and all deleted rights together.
- If you list rights without using + or -, the rights you list replace the existing rights.

- You must always specify a path. You can use a period (.) to represent your current directory.
- You can use wildcard characters.

Examples

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

  ```
  RIGHTS . R W F /NAME=JANICE
  ```

- To remove user ERNESTO from ALICE/SYS:USERS, type

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

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

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

FLAG (NetWare)

For NetWare, you can use the FLAG utility to set directory and file attributes from the command line. For information, see “FLAG” in the *Utilities Reference for OES*.

A Documentation Updates

This section contains information about documentation content changes made to the *Novell Traditional File System Administration Guide* since the initial release of NetWare® 6.5. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the front cover and the Legal Notices page, to determine the release date of this guide. For the most recent version of the *Novell Traditional File System Administration Guide*, see the Novell documentation Web site (http://www.novell.com/documentation/lg/nw65/trad_enu/data/front.html)

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

This document was updated on the following dates:

- "May 14, 2004" on page 87
- "July 2, 2004" on page 87
- "February 28, 2005" on page 88

May 14, 2004

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

- "Using Software RAID-0 Devices to Enhance Disk I/O Performance" on page 87
- "Appendix C: Documentation Updates" on page 87

Using Software RAID-0 Devices to Enhance Disk I/O Performance

The Using Software RAID-0 Devices to Enhance Disk I/O Performance section is revived in this release. This is not a new feature, it is information previously omitted in error.

Appendix C: Documentation Updates

The Documentation Updates section is new in this release.

July 2, 2004

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

- "Overview of Traditional File System" on page 88

- "Planning Your Directory Structure" on page 88
- "Configuring and Managing Directories and Files" on page 88

Overview of Traditional File System

The following changes were made to this section:

Location	Change
Directories	This topic was moved to Planning Your Directory Structure.
Drive Mappings	This topic was moved to Planning Your Directory Structure.

Planning Your Directory Structure

The following changes were made to this section:

Location	Change
Planning Your Directory Structure	This section moved to follow the volume management chapters.
Directories Created During NetWare Installation	This section was deleted because it contained obsolete information.
Designing Application Directory Structures	Application directories are storage areas where you install applications for convenient network access by groups and users. We recommend that you create separate volumes for applications and user data, reserving the sys: volume for the operating system and its extensions.

Configuring and Managing Directories and Files

This chapter was moved to follow the volume management chapters.

February 28, 2005

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

- "Planning Directories" on page 88
- "Configuring and Managing Directories and Files" on page 88

Planning Directories

Editorial updates were made to this section.

Configuring and Managing Directories and Files

Additional details were added to the procedures in this section.