Novell
Open Enterprise Server

www.novell.com

NCP™ SERVER FOR LINUX
ADMINISTRATION GUIDE

December 23, 2005

Novell®

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

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

Novell Trademarks

Third-Party Materials

Contents

About This Guide

This guide includes information on Novell® NCP™ Server Services for Linux, which enables users to access data on a Linux server using the same methods as they do on a NetWare server using Novell Client™ software.

The following topics are included in this documentation:

- Chapter 1, “NCP Server for Linux Overview,” on page 9
- Chapter 2, “What's New,” on page 11
- Chapter 3, “NCP Server for Linux Installation and Setup,” on page 13
- Chapter 4, “NCP Server Performance and Security,” on page 23
- Appendix A, “Documentation Updates,” on page 27

Audience

This guide is intended for intended for anyone involved in installing, configuring, and managing NCP Server.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments 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

The latest version of this *NCP Server Administration Guide* is available on the OES documentation Web site (http://www.novell.com/documentation/lg/oes).

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.

NCP Server for Linux Overview

1

With this release of Novell® Open Enterprise Server (OES), the great services provided by Novell NetWare® Core Protocol (NCP™) on NetWare are now available on Linux. This means that Windows* and Linux workstations running Novell Client™ software can now access data and manage file sharing using the same methods as they do on NetWare servers. NCP is included with OES and, by default, is installed on Linux servers.

1.1 How NCP Server Works

NCP has been used for years to manage access to the primary NetWare server resources. NCP makes procedure calls to the NetWare File Sharing Protocol (NFSP) that services requests for NetWare file and print resources. NCP is the principal protocol for transmitting information between a NetWare server and its clients.

NCP handles login requests and many other types of requests to the file system and the printing system. NCP is a client/server LAN protocol. Workstations create NCP requests and use TCP/IP to send them over the network. At the server, NCP requests are received, unpacked, and interpreted.

Services included with NCP are file access, file locking, security, tracking of resource allocation, event notification, synchronization with other servers, connection and communication, print services and queue management, and network management.

Novell Client software must be used to initiate a connection between a Windows or Linux workstation running Novell Client software and a Linux server running NCP Server services. Security and authentication issues require that linking clients to servers be a client/server application. Intelligence at both ends of the connection work together to verify that clients are who they claim to be, and that file controls are followed when using shared server files.

1.2 Benefits of NCP Server

NCP and Novell Client software together more than match the level of security and utility found in Windows, Macintosh*, UNIX, or Linux networking; in fact, they far exceed all those examples. NCP and Novell Client software offer great benefits in ways that appeal to users and to managers.

If you look at the list of file attributes provided by NCP and NSS and then compare those to the file attributes in Windows, Macintosh, UNIX, or Linux networks you will find that NCP and NSS provide much more control over files.

Some of the benefits provided by NCP Server on Linux include:

- Users can log in to the Linux network from their Novell Client workstation just like they do with NetWare. This means that for users familiar with a NetWare environment, there is no need to re-educate or retrain. There is also no need to reconfigure Novell Client workstations to access your Linux network.
- Users and administrators can map drives to volumes and directories on Linux servers just like they do on NetWare.
- NetWare-style login scripts can be created for users to automate drive mappings and other network functions.

- The file and directory attributes and rights that exist on NetWare are now available and configurable on Linux.
- Directory limits for individual users can be set and administered on Linux.
- All the functions provided by the red N on the taskbar for Windows clients running Novell Client software are now also available on Linux.

1.3 What's Next

For information on installing and configuring NCP server on Linux, see Chapter 3, “NCP Server for Linux Installation and Setup,” on page 13.

What's New

2

The following changes and enhancements were added to NCP Server for Linux for Novell Open Enterprise Server (OES) Support Pack 2.

- The ability to change the Inherit POSIX Permissions option and set the archive bit for files using Novell Remote Manager (NRM). See Section 3.3.5, “Setting Volume Definition Flags,” on page 18.
- File share modes have been added to cross protocol locking. See Section 3.3.10, “Enabling and Disabling Cross Protocol Locks,” on page 19.

NCP Server for Linux Installation and Setup

3

NCP™ Server for Linux is by default installed during the Open Enterprise Server (OES) installation. You can optionally choose to install NCP Server for Linux after the OES installation. SUSE ® Linux Enterprise Server (SLES) 9 is installed with the OES installation. This section contains information to help you install, set up, and configure NCP Server for Linux.

NSS can be installed with NCP Server, but is not required.

3.1 Installing NCP Server after the OES Installation

If you did not install NCP Server during the OES installation, you can install it later by installing the Novell NCP Server selection using Linux console commands or YaST. See "Installing or Configuring OES Components on an Existing Server" for more information.

3.2 Setting Up NCP Server

After installing NCP Server for Linux, you might need to create and mount NCP volumes on your Linux server. NCP volumes on Linux can be created on the NSS file system using the same utilities as on NetWare®, or you can create NCP volume mount points on any Linux file system using NCPCON commands or Novell® Remote Manager (NRM). A SYS NCP volume mount point is automatically created and mounted when NCP Server is installed. The path to the this mount point is `/usr/novell/sys`. This volume contains the same login and public directories that exist on NetWare. These directories let Novell clients run commands for logging in, mapping drives, etc., as well as providing the means for client commands to be run from login scripts.

3.2.1 Creating NCP Volumes

If you want to make traditional Linux file system files and directories on a Linux server accessible to workstations running Novell Client™ software, you must create one or more NCP volumes on that Linux server. Creating an NCP volume on a Linux server (traditional Linux file system) creates an NCP volume name and associates it to a path for a mount point. Novell clients can then access files and folders on that NCP volume just like they do on NetWare.

Creating an NCP Volume Using NCPCON

At the Linux Server console, type `ncpcon create volume` *`ncp_volume_name path`*.

Replace *ncp_volume_name* with the name you want to assign to the new volume. Volume names are not case sensitive. Replace *path* with the path to the directory on your Linux server where you want the mount point to be created. For example, if volume name is vol1 and the path is `/home/novell/vol1`, then you would type

```
ncpcon create volume vol1 /home/novell/vol1
```

This command does not remove or delete data. It only adds the NCP volume mount information to `/etc/opt/novell/ncpserv.conf`.

NOTE: You can also type `ncpcon` at the Linux server console to access the ncpcon utility and then enter NCP console commands without prefacing them with ncpcon in the command. Type `help` while in the ncpcon utility to get a list of and descriptions for available commands.

Creating an NCP Volume Using Novell Remote Manager

1. Access Novell Remote Manager by pointing your browser to the URL of the server where NCP Server is running.

   Do this by entering the following in the address (URL) field:

   ```
   http://server's_TCP/IP_address:8008 or
   other_configured_port_number
   ```

   For example:

   http://172.16.123.11:8008
2. On the Novell Remote Manager main page in the left column under *Manage NCP Services*, click *Manage Shares*, then click *Create New Share*.
3. Enter the name of the NCP volume you want to create, and if desired, select the *Inherit POSIX Permissions* and *Enable Archive Bit* check boxes. Then click *OK*.

   The share name you specify is the volume name NCP clients will see. It will be associated to a path on your Linux server.

   See Section 3.3.5, "Setting Volume Definition Flags," on page 18 for more information on the options to inherit POSIX permissions and enable the archive bit.
4. Enter the path to the share name, then click *OK* to confirm the creation of the volume (share).

   This creates a mount point to the volume (share) name you specified and "mounts" it to make it accessible to NCP clients.

Using Novell Remote Manager or NCPCON to create an NCP volume does not create an NSS volume. This method applies to file systems other than NSS. If you want to create an NSS volume on your OES server, you must have the NSS component of OES installed. You can then use NSSMU or iManager to create NSS partitions, pools, and volumes.

Novell clients (Windows or Linux machines running Novell Client software) can access NSS files on a Linux server if

- You have NCP Server installed on your OES Linux server (installed by default with OES).
- You have created an NSS partition, pool, and volumes.
- You have made the appropriate volume trustee assignments (for non-admin users).

3.2.2 Mounting NCP Volumes

After creating an NCP volume, you must mount it to make it accessible to Novell clients. Any NCP volume that has been dismounted must also be mounted before it can be accessed by Novell clients.

If you created an NCP volume using Novell Remote Manager, the volume is automatically mounted when it is created.

Mounting an NCP Volume Using NCPCON

At the Linux Server console, type `ncpcon mount` *`ncp_volume_name`*.

Replace *ncp_volume_name* with the name of the volume you want to mount. For example, if volume sys was dismounted and you wanted to mount it, you would type

```
ncpcon mount sys
```

Mounting an NCP Volume Using Novell Remote Manager

On the Novell Remote Manager main page in the left column under *Manage NCP Services*, click *Manage Shares*, then click the *Mount* button next to the NCP volume you want to mount.

3.3 Managing NCP Server

After you have installed NCP Server and created and mounted NCP volumes for your specific needs, some additional information can be useful to help you effectively manage NCP Server. This information consists of instructions for dismounting, removing and purging NCP volumes, and viewing NCP Server information.

3.3.1 Viewing NCP Server Information

You can view information on NCP server configuration and volumes using either the NCPCON utility or Novell Remote Manager.

Viewing NCP Server Information Using NCPCON

Enter `ncpcon` at the Linux server console, and then use any of the following NCPCON commands to view NCP server information:

Table 3-1 *Viewing NCP Server Information Using NCPCON Commands*

Command	Description
config	Displays the NCP server configuration.
stats	Displays NCP statistics such as bytes read, bytes written, and NCP requests.
volume	Displays a list of currently mounted NCP volumes. You can also specify a specific volume name with the command to get information about that volume

Viewing NCP Server Information Using NRM

On the Novell Remote Manager main page in the left column under *Manage NCP Services*, click *View Server Information*. You can also click *View Diagnostic Information* to view NCP server diagnostic information. This can help you troubleshoot NCP server problems. You can click the pid value to access additional pages for process information and to change file attributes for specific NCP-related program files.

3.3.2 Managing NCP Server Volumes

After creating and mounting an NCP volume on your Linux server, there might be occasions when you want to dismount the volume, purge deleted files from the volume, or remove the volume mount point.

Dismounting an NCP Volume Using NCPCON

Enter `ncpcon` at the Linux server console, and then enter the following command:

```
dismount volume_name
```

Replace *volume_name* with the name of the volume you want to dismount. This command removes NCP client accessibility to the mount point represented by the volume name. You can also replace *volume_name* with *all* to dismount all NCP volumes on the server.

Dismounting an NCP Volume Using Novell Remote Manager

On the Novell Remote Manager main page in the left column under *Manage NCP Services*, click *Manage Shares*, then click the *Unmount* button next to the NCP volume you want to dismount.

Dismounting an NCP volume makes it inaccessible to NCP clients.

Purging Deleted NSS Files Using NCPCON

Enter `ncpcon` at the Linux server console, and then enter the following command:

```
purge volume volume_name
```

Replace *volume_name* with the name of the NSS volume you want to purge. This command purges or permanently removes deleted files from an NSS volume. This command only works with NSS volumes.

Purging Deleted NSS Files Using Novell Remote Manager

Purging deleted NSS files using Novell Remote Manager is currently not possible. You can purge and undelete NSS files on your Linux server using NetStorage. For more information, see “Purging and Salvaging Deleted NSS Files” in the OES NetStorage Administration Guide for Linux.

Removing an NCP Volume Using NCPCON

Enter `ncpcon` at the Linux server console, and then enter the following command:

```
remove volume volume_name
```

Replace *volume_name* with the name of the volume you want to remove. This command does not remove or delete data. It only removes the NCP volume mount point (path and association) that was created when you created the NCP volume.

If you have removed an NCP volume and want to restore it, you must create the volume again like you did when you first created it.

Removing an NCP Volume Using Novell Remote Manager

1. On the Novell Remote Manager main page in the left column under *Manage NCP Services*, click *Manage Shares*, then click *Delete Existing Share*.
2. Enter the name of the NCP volume you want to remove, click *OK*, then click *OK* again to confirm the volume removal.

   This removes the NCP volume and path association. This does not remove or delete data from the directory; it only removes the volume mount point that was created.

3.3.3 Managing NCP Server Connections

You can view a list of NCP server connections as well as get specific information for each connection. Using Novell Remote Manager, you can also clear specific NCP connections and send a broadcast message out to current NCP connections.

Viewing NCP Connection Information Using NCPCON

Enter `ncpcon` at the Linux server console, then enter the following command:

```
connection
```

You can also enter `connection list` to get more detailed information on NCP connections, or specify the connection number to get detailed information on a specific NCP connection. For example, you would enter `connection 1` to get specific information on that NCP connection.

Viewing NCP Connection Information Using Novell Remote Manager

On the Novell Remote Manager main page in the left column under *Manage NCP Services*, click *Manage Connections*.

Use this page to view NCP server connection statistics and the list of connections. You can also broadcast a message to all currently connected users and clear selected connections.

To broadcast a message to all NCP connections, type the message you want broadcast and click *Send*.

To clear specific NCP connections, check the boxes next to the connections you want to clear and then click *Clear ALL Marked Connections*.

3.3.4 Disabling and Enabling Opportunistic Locking

Opportunistic locking (Oplocks) improves file access performance and is enabled by default in NCP Server. Oplocks provides a way to cache file data at the client. It allows the client to read and write data using its local cache and interact with the file server only when necessary. Oplocks improves both client and network performance by reducing the amount of traffic on the network.

There are two levels of oplocks available with NCP Server. You can set oplocks to either of these levels or disable oplocks completely. By default, oplocks is set to level 2, which includes both level 1 and level 2 functionality.

To disable oplocks, edit the `etc/opt/novell/ncpserv.conf` file and add the following line:

```
OPLOCK_SUPPORT_LEVEL 0
```

To set oplocks to level 1, edit the `etc/opt/novell/ncpserv.conf` file and add the following line:

```
OPLOCK_SUPPORT_LEVEL 1
```

There is no need to add a line to the ncpserv.conf file to set oplocks to level 2, because it is by default set to that level.

For more information on Oplocks with NCP Server, see Section 4.1, “Opportunistic Locking and NCP,” on page 23.

3.3.5 Setting Volume Definition Flags

There are two options that can be added to provide NetWare-like functionality to non-NSS NCP volumes on Linux. These are the Enable Archive Bit option and the Inherit Posix Permissions option. Both options are disabled by default. The Enable Archive Bit option turns on support for the DOS archive bit on files. NCP, like Samba, uses the user-execute mode bit to save this information. For more information on the Inherit Posix Permissions option, see Section 4.2, “NCP on Linux Security,” on page 24.

Setting Volume Definition Flags Using Novell Remote Manager

Adding these options using Novell Remote Manager can only be done during the volume creation. See Step 3 on page 14 for information on adding these options using Novell Remote Manager.

Setting Volume Definition Flags Using Ncpserv.conf

To add either or both of these options, edit the `etc/opt/novell/ncpserv.conf` file and add the following flag(s) to the end of the volume definition line for the volume you want to add the options to.

```
Enable_Archive_Bit

Inherit_Posix_Permissions
```

The following sample volume definition lines provide examples for adding each option individually and together:

```
VOLUME TEST1 /usr/Novell/TEST1 Inherit_POSIX_Permissions

VOLUME TEST2 /usr/Novell/TEST2 Enable_Archive_Bit

VOLUME TEST3 /usr/Novell/TEST3 Enable_Archive_Bit
Inherit_POSIX_Permissions
```

3.3.6 Monitoring NCP Server

You can monitor NCP Server connections, communications, volumes, and diagnostics using NCPTOP. NCPTOP is a monitoring utility that has the look of the NetWare Monitor utility, and is an interactive, real-time reporting utility. It is part of the novell-ncpserv RPM.

After NCP Server has been installed, you can start NCPTOP by entering `ncptop` at the Linux server console. Different statistic monitoring functions of NCPTOP can be accessed using the F1 through F5 function keys. The purpose of each function key is displayed within the NCPTOP utility.

3.3.7 Changing the NCP Server Code Page

NCP Server by default uses the code page corresponding to the Linux server's default language. For example, if the Linux server is installed as a Japanese server, NCP Server will by default use shift-JIS as its local code page. If the Linux server is installed as a French server, NCP Server will by default use CP850 as its local code page. NCP Server can automatically detect and use most commonly used code pages.

If you want NCP Server to use a code page that is different than the one that is set by default, you must specify that code page in the `/etc/opt/novell/ncpserv.conf` configuration file.

Open the `/etc/opt/novell/ncpserv.conf` configuration file and add the following line

```
LOCAL_CODE_PAGE Code_Page
```

Replace *Code_Page* with the code page you want. Some examples are CP437, CP850, CP737, CP866, CP874, CP949, SJIS, BIG5, and GBK. For a complete list of available code pages, type `iconv --list | more` at the linux command line.

3.3.8 Disabling Sendfile Support

The Linux sendfile() API improves the performance for file reads. Samba has had problems in the past with sendfile(). Sendfile() support is enabled by default. If you experience problems with Samba and sendfile(), you can turn sendfile() off by adding the following line to the `/etc/opt/novell/ncpserv.conf` configuration file.

```
SENDFILE_SUPPORT 0
```

You can also replace the 0 with a 1 to turn sendfile() back on.

3.3.9 Enabling and Disabling the Execute Only File Attribute

The Execute Only file attribute is enabled by default. You can disable it by adding the following line to the `/etc/opt/novell/ncpserv.conf` configuration file.

```
EXECUTE_ATTRIBUTE_SUPPORT 0
```

If this option is enabled, volume archive bit support is turned off automatically.

You can also replace the 0 with a 1 to enable the Execute Only file attribute.

3.3.10 Enabling and Disabling Cross Protocol Locks

Cross-protocol locks are disabled by default. Enabling cross-protocol locks turns on the cross-protocol checking for physical record locks This lets you run applications from Samba and NCP clients concurrently; and each will recognize when the other has the file in use. Enabling cross-protocol locks also enables file share modes. File share modes allow an application to specifiy whether or not it allows other clients to read and/or write the file while it is using it. Commonly, this is used to allow other clients to read the same file but not write to it while the primary client is using it. Without share modes, applications incorrectly assume that they have exclusive access to a file.

You can enable cross-protocol locks by adding the following line to the `/etc/opt/novell/ncpserv.conf` configuration file.

```
CROSS_PROTOCOL_LOCKS 1
```

You can also replace the 1 with a 0 to disable cross-protocol locks.

3.4 NCP Server Directory and File Attributes and Trustee Rights

Directory and File Trustee Rights

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

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

Directory and File Attributes

NCP Server for Linux supports the same file and directory attributes for NSS on Linux as NSS on NetWare. These are the same attributes that exist for the NSS file system on NetWare. See the File Systems Management Guide for OES (http://www.novell.com/documentation/oes/index.html?page=/documentation/oes/stor_filesys/data/bs3fkbm.html) for information on NSS file and directory attributes.

The following file and directory attributes are supported for traditional Linux file systems on Linux.

- Read Only
- Hidden
- Shareable

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

Even though the other NSS file and directory attributes appear to be supported on traditional Linux file systems, and might also appear to be settable, those file and directory attributes are not supported, and will be ignored if files are accessed through NCP. For example, it might appear that you have set the copy inhibit attribute for a specific file, but that file can still be copied if it's accessed through NCP.

NOTE: File attribute and NCP support tend to get mixed together in the minds of NetWare administrators. It is important to remember that file and directory attributes are supported and enforced by the file system that underlies an NCP volume, not by the NCP server.

3.4.1 Changing NCP File System Rights

The NCPCON utility lets you view, add, or remove file and directory rights for both NSS and traditional Linux file systems.

Viewing File and Directory Rights

To view file or directory rights, enter `ncpcon` at the Linux server console and then enter the following:

```
rights view path
```

Replace *path* with the directory path to the file or directory that you want to view trustee rights for. This lets you view the trustee assignments that have been specifically made for that file or directory. Effective rights are not displayed using this command.

Adding File and Directory Rights

To add file or directory rights, enter `ncpcon` at the Linux server console and then enter the following:

```
rights add path fdn mask
```

Replace *path* with the directory path to the file or directory that you want to add trustee rights to.

Replace *fdn* with the fully distinguished name of the user or object that you want to grant rights to.

Replace *mask* with the rights that you want to grant to the user or object.

For example, if you wanted to grant Read and File Scan rights to the users:bob directory for user Bob, and Bob's context is bob.acme, you would enter the following after starting the NCPCON utility:

```
rights add users:bob bob.acme RF
```

Removing File and Directory Rights

To remove file or directory rights, enter `ncpcon` at the Linux server console and then enter the following:

```
rights rem path fdn
```

Replace *path* with the directory path to the file or directory that you want to remove trustee rights from.

Replace *fdn* with the fully distinguished name of the user or object that you want to remove rights from.

For example, if you wanted to remove trustee rights to the `users:bob` directory from user Bob, and Bob's context is bob.acme, you would enter the following after starting the NCPCON utility:

```
rights rem users:bob bob.acme
```

3.5 Additional Information

Although hard links are supported with NCP Server for Linux, soft links are intentionally not supported because they create security problems.

For more information on features provided by NCP Server for Linux, see the Novell Client for Windows Installation and Administration Guide and the Novell Client for Linux Installation and Administration Guide.

NCP Server Performance and Security

4

This section contains information to help you understand Opportunistic Locking (Oplocks) for NCP™ and the differences in the NCP security models.

4.1 Opportunistic Locking and NCP

Oplocks, or opportunistic locks, are a way to cache file data at the client. This allows the client to read and write data using its local cache and interact with the file server only when necessary. Oplocks are acquired after a normal NCP file handle has been obtained. Oplocks should help both client and network performance by reducing the amount of traffic on the network.

When a server requires a client to release its oplock, it sends it a tickle packet. Tickle packets are very similar to broadcast packets. The main difference is that they include a dollar sign ($) character instead of an exclamation point (!) character for the control information. Tickle packets also contain the file handle, so the client knows which oplock to release.

There are two types of oplocks: L1 (level 1) and L2 (level 2).

L1 oplocks give the client exclusive access to the file. The client can cache reads and writes locally. The client can even close the file without notifying the server; this is useful for when the client application opens and closes the same file over and over.

L1 oplocks can be acquired by using NCP to open the file and then setting the corresponding oplock request bits. If another connection has the file open, the L1 oplock is denied — you can't get an oplock on a file that is currently shared with another client.

If another connection tries to access (open, rename, or delete) an L1 oplocked file, the owner of the oplock is notified with a tickle packet that the lock needs to be broken. The client then

1. Acknowledges the tickle packet. For protocols like IPX™ and UDP, this lets the server know that the client received the tickle packet.
2. Flushes any dirty cache buffers to the server.
3. Acquires any cached physical record locks if it plans on keeping the file open.
4. Performs one of the following four operations:
    - Clears the oplock
    - Refuses to clear the oplock

      Note that the Novell® client doesn't ever do this.
    - Downgrades the oplock to an L2 shared lock
    - Closes the file

With all L1 oplocks, the server waits for the client holding the L1 oplock to respond before allowing the new access request to continue. Because NCP allows only one outstanding request for a client connection, the server must be careful never to send a tickle packet to the client making the initial access request.This avoids a deadlock situation.

L2 oplocks give the client shared read access to the file. Multiple clients can have L2 oplocks for the same file. Not all clients accessing the same shared file require L2 oplocks; some might not have an oplock at all. The L2 oplock entitles the client to cache file data locally for reads, but not for writes. This is useful when the client reads the same data over and over. L2 oplocks should be released when the client application closes a file, because the server won't notify the client when another connection wants exclusive access to that file (delete, rename, exclusive open, etc.).

When a client writes to a file that has L2 oplocks for other clients, all the other clients are sent a tickle packet to notify them that their local cache for that file is no longer valid. When the client receives this tickle packet, it

1. Acknowledges the tickle packet.
2. Invalidates its local cache for the file.
3. Clears its oplock for the file.

The server does not grant an L2 oplock for a file that has been written to recently by a client other than the one requesting the lock.

Oplock support can be turned off or on at the client or at the server. The server lets the user enable only L1 oplocks or both L1 and L2 oplocks.

Oplocks are automatically released when a file is closed.

A client can't open, rename, or delete a file while another client has an L1 oplock on it. The request causes a tickle packet to be sent to the client holding the oplock; the server then waits for a reply from that client and then continues based on the client's response.

When a client has an L1 oplock for a file, it doesn't need to send physical record lock requests to the server for that file. It can track the locks locally. If the client later needs to release the oplock, it will need to acquire any outstanding physical record locks from the server before continuing. For L2 oplocks, physical record locks should be managed at the server instead of the client to avoid deadlocks.

If a client tries to open, rename, or delete a file that it already has L1 oplocked, the open will fail because the server can't delay the request and wait for notification from the client that it has cleared the oplock.

4.2 NCP on Linux Security

The NetWare® and Linux security models are quite different. The basic NetWare security model assumes that users have no rights until they are granted specific rights. Those rights are inherited by the user to all child subdirectories. That way, a single trustee assignment can give a user rights to a large number of subdirectories and files. A user's home directory will be set up so that only the user and the system administrator have rights there. A user's files are secure. If a user wants to share his files with others, he can grant them rights through trustee assignments on the individual files or the user can create a shared subdirectory and assign trustees to it. When a user is given a trustee assignment to a file or directory, he can automatically see each parent directory along the path up to the root. However, the user can't see the contents of those directories, just the path to where he has rights.

The POSIX/Linux security model takes a different approach. The POSIX permissions are specified for each file and subdirectory, and nothing is inherited. If a user is to have access to all the files in a subdirectory, the permissions (UID, GID, and mode bits) must be set for each file in a manner that gives the user the appropriate access. This can't be done with a simple trustee assignment to the parent subdirectory. In order for a user to use the `dir` or `ls` command, the user must have the read and execute rights in that directory and all its parent directories up to the root. Because of this, users usually have read rights by default across most of the system, and then the rights for everyone are masked for areas that need to be private. This means that the default for POSIX is open and shared rather than private. In POSIX, files are private when you make them private rather than private by default.

These differences can become problems when you try to share files between NCP users and Linux users that rely on the POSIX rights for their access (Local, SSH, and Samba users). In order for the Linux/POSIX users to access files, they need to be granted r and x rights through the group and other mode bits for subdirectories along the path up to the root of the volume. This gives them the right to see and read all files in those directories up to the root. This is unlike NCP rights on NetWare, where users see only the subdirectory path to the locations where they have been granted trustee rights. For shared volumes, NetWare users should be aware that Linux/POSIX users might have more rights to files and subdirectories than NCP users do.

Because the NetWare model is secure/private until granted specific rights, all files and subdirectories created by NCP clients have the following POSIX security permissions:

- The UID will be that of the user (or root if the user isn’t LUM enabled)
- The GID will be root
- The mode bits will be rwx --- ---

This way, by default, the only person who can access a file or subdirectory from a LINUX environment is root and the creator of the file or subdirectory. An option is included with OES that lets a volume be configured such that the permissions (GID and mode bits) are inherited from the parent directory. This lets shared areas be more easily created and managed. This option is not enabled by default. The more secure model of the OES release is still the default. See Section 3.3.5, “Setting Volume Definition Flags,” on page 18 for more information.

Because NSS is not a POSIX file system, NSS rights don’t behave like standard POSIX rights. NSS volumes keep track of trustee assignments; all trustee assignments are synchronized between NCP and NSS. For NSS volumes, access is based on trustee rights for the user (UID) rather than the permissions (UID, GID, and mode bits). This makes things simpler in that Linux/POSIX-based users (Local, SSH, and Samba) do not have more rights than the same user would have if he were accessing files through NCP. This makes NSS easier to manage.

Documentation Updates

A

This *NCP Server Administration Guide* has been updated with the following information on December 23, 2005:

A.1 December 23, 2005 (Open Enterprise Server SP2)

Location	Change
Entire guide.	Page design reformatted to comply with revised Novell® documentation standards.
"Creating an NCP Volume Using Novell Remote Manager" on page 14	Options for inheriting POSIX permissions and enabling the archive bit can now be performed using Novell Remote Manager. The change is reflected in this section.
Section 3.3.10, "Enabling and Disabling Cross Protocol Locks," on page 19	Cross-protocol locks now include file share modes. Information on file share modes has been added to this section.

Additional NCP Server Commands and Options

B

The following NCP Server commands, command line options, and configuration file options should not be used except under direction from Novell.

B.1 Configuration File Options

The following configuration file options apply to the `ncpcon.conf`, `ncpserv.conf,` and `ncp2nss.conf` configuration files.

LOG_TIMESTAMPS [Yes|No] *Default is No*

LOG_MAX_FILE_SIZE size *Default is 4194304 (4MB)*

B.2 NCP2NSS Command Line Options

`--d` *Used to start daemon as a foreground process instead of background daemon.*

`--h` *Help*

B.3 NCPCON Command Line Options

`--@filename` *Use file for ncpcon input processing*

`--h` *Help*

`--ncpservername` *Used with bind/unbind command*

`--ipaddress` *Used with bind/unbind command*

`--volid` *Used with bind/unbind command*

Hidden Commands

`log` *For more information type help log*

`diag` *For more information type help diag*

`flush volume` *For more information type help flush volume*

`nss resync`

B.4 NCPTOP Command Line Options

`--d` *Output logging information to ncptop.log*

`--h` *Help*