Open Enterprise Server 2015 SP1

NCP Server for Linux Administration Guide

June 2016

Novell.

Legal Notices

Contents

About This Guide

Novell NCP Server services for Open Enterprise Server (OES) 2015 SP1 enable users to access data on Linux file systems with the Novell Client by using the Novell trustee model for access control.

The following topics are included in this documentation:

Audience

This guide is intended for administrators who install, configure, and manage NCP Server and NCP volumes.

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.

Documentation Updates

The latest version of the *OES 2015 SP1: NCP Server for Linux Administration Guide* is available on the OES documentation Web site (http://www.novell.com/documentation/oes2015).

Additional Information

For information on NCP features supported by NCP Server for Linux, see the *Novell Client 2 SP1 for Windows Administration Guide*, and the *Novell Client 2.0 SP3 for Linux Administration Guide*.

1 NCP Server for Linux Overview

On Open Enterprise Server (OES) 2015 SP1 servers, the NetWare Core Protocol (NCP) Server provides the same services that are available with NCP Server on NetWare. With NCP Server, you can define NCP volumes (NCP shares on Linux POSIX file systems) and use Novell Storage Services (NSS) volumes on Linux. Access to both types of volumes is controlled by using the Novell trustee model. Windows and Linux workstations running Novell Client software can access data and manage file sharing on OES 2015 SP1 servers just as they do on NetWare 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 works together to verify that clients are who they claim to be, and that file controls are followed when using shared server files.

1.1.1 Guidelines for Name Spaces

NCP recognizes only the DOS and LONG namespaces for an NSS volume on an OES server that is enabled to access via NCP.

However, NCP recognizes the DOS, AFP, NFS, and LONG namespaces for an NSS volume on a NetWare server that is enabled to access via NCP.

In OES, NCP does not support mounting a volume in a DOS name space.

However, an NCP verb request through the Novell Client to return the files and folders names in a DOS name space is supported.

1.2 Benefits of NCP Server

Using NCP and Novell Client software together exceeds the level of security and utility found in Windows, Macintosh, UNIX, or Linux networking. 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 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 the Novell Client workstation just like they do with NetWare. This means that for users familiar with a NetWare environment, there is no need to reeducate 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.
- Volume limits for individual users can be set and administered on Linux.
- Directory limits can be administered in the same way for all users.
- The Novell Client provides the same functions to users of OES 2015 SP1 servers as it does for users of NetWare servers.

1.3 What's Next

For information about enhancements to NCP Server in this release, see Chapter 2, “What’s New or Changed in NCP,” on page 15.

For information on installing and configuring NCP Server on Linux, see Chapter 3, “Installing and Configuring NCP Server for Linux,” on page 17.

2 What’s New or Changed in NCP

2.1 What’s New or Changed (OES 2015 SP1)

NCP in OES 2015 SP1 has been modified for bug fixes. There are no new features or enhancements in OES 2015 SP1.

2.2 What’s New or Changed (OES 2015)

This section describes enhancements and changes in NCP with the initial release Novell Open Enterprise Server (OES) 2015.

- “Augmented Size of NCP Verb Replies” on page 15
- “A New Option to Enhance the Readability of the ncpcon connection list Command” on page 15
- “Enabling or Disabling the Logging of eDirectory Object Rename or Delete Events” on page 15
- “Displaying Volume Size Details” on page 16
- “Support for NCP Volumes Greater than 16 TB” on page 16

Augmented Size of NCP Verb Replies

With the introduction of the ncpcon set parameter CONN_LBUF_POOL_SIZE, the reply size of the impacted NCP verbs have been augmented to 64K. This enables the client to get more detail in a single request, so that fewer requests are required for directory enumeration.

For more information, see “Augmented Size of NCP Verbs 87_20 and 89_20 Replies” in the *OES 2015 SP1: NCP Server for Linux Administration Guide*.

A New Option to Enhance the Readability of the ncpcon connection list Command

A new switch /h (`ncpcon connection list /h`) has been added to interpret the number of bytes read or written in human readable format. In other words as KB, MB, or GB, whichever fits best for the size reported.

For more information, see “connection list /h ” in the OES 2015 SP1: NCP Server for Linux Administration Guide.

Enabling or Disabling the Logging of eDirectory Object Rename or Delete Events

You can choose to disable or enable logging of object history events.

```
ncpcon set LOG_OBJECT_HISTORY = <value>
```

For more information, see “Enabling or Disabling Logging eDirectory Object Rename or Delete Events” in the OES 2015 SP1: NCP Server for Linux Administration Guide.

Displaying Volume Size Details

The command `ncpcon volume <volume name>` has been enhanced to display Used, Free, and Salvageable space, and the `ncpcon volume` command has been enhanced with the switch `/s` to display the size details of volumes.

See "Displaying NCP Volume Information" in the OES 2015 SP1: NCP Server for Linux Administration Guide.

Support for NCP Volumes Greater than 16 TB

- **Large Volume Support:** The NCP protocol has been extended to support volumes larger than 16 TB.
- **Novell Client Enhancements:** Novell Client for Windows has also been extended for accessing volumes larger than 16 TB.

  The Novell Client 2 SP4 for Windows with support for volumes larger than 16 TB is available on the Novell download site (http://download.novell.com/Download?buildid=fa_5vzOhcTo~).
- **Validation Against POSIX File Systems:** Increased size handling has been validated against BTRFS and XFS file systems in addition to NSS.

3 Installing and Configuring NCP Server for Linux

This section describes how to install and configure NCP Server for Linux on Open Enterprise Server (OES) 2015 SP1 server.

- Section 3.1, "Installation Requirements for NCP Server for Linux," on page 17
- Section 3.2, "Installing NCP Server," on page 22
- Section 3.3, "Updating NCP Server," on page 25
- Section 3.4, "Configuring Global NCP Server Parameters," on page 25
- Section 3.5, "Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon," on page 32
- Section 3.6, "Restarting the NetIQ eDirectory (ndsd) Daemon," on page 33
- Section 3.7, "Configuring the NCP Server Local Code Page," on page 33
- Section 3.8, "Configuring the Execute Only File Attribute for NCP Server," on page 34
- Section 3.9, "Configuring Sendfile Support for NCP Server," on page 35
- Section 3.10, "Configuring Opportunistic Locking for NCP Server," on page 36
- Section 3.11, "Configuring Cross-Protocol File Locks for NCP Server," on page 38
- Section 3.12, "Modifying the NCP File Server Name," on page 40
- Section 3.13, "Modifying the sys: Volume Mount Point," on page 41

3.1 Installation Requirements for NCP Server for Linux

Make sure your system satisfies the required software and configuration settings that are specified in this section.

- Section 3.1.1, "Supported Platforms," on page 18
- Section 3.1.2, "NCP Server and Dynamic Storage Technology," on page 18
- Section 3.1.3, "Static Hostname and the NCP File Server Name," on page 18
- Section 3.1.4, "64-Bit Support," on page 18
- Section 3.1.5, "NetIQ eDirectory 8.8 SP8," on page 18
- Section 3.1.6, "eDirectory Rights Needed by a Container Administrator," on page 18
- Section 3.1.7, "Novell Storage Services," on page 19
- Section 3.1.8, "Novell Samba," on page 19
- Section 3.1.9, "Linux User Management," on page 19
- Section 3.1.10, "Novell AFP," on page 20
- Section 3.1.11, "Novell Cluster Services for Linux," on page 20
- Section 3.1.12, "SLP," on page 20
- Section 3.1.13, "Novell iManager 2.7.7 for Linux," on page 21

- Section 3.1.14, “Novell Remote Manager for Linux,” on page 22
- Section 3.1.15, “SFCB,” on page 22
- Section 3.1.16, “Other OES 2015 SP1 Services,” on page 22

3.1.1 Supported Platforms

NCP Server for Linux supports OES 2 Linux and later.

3.1.2 NCP Server and Dynamic Storage Technology

NCP Server for Linux provides the NCP services for NSS volumes on Linux and for NCP volumes on Linux POSIX file systems. Dynamic Storage Technology (DST) is a component of NCP Server. Using DST is optional, but NCP Server must be installed and running for DST to work.

For information about managing Dynamic Storage Technology, see the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

3.1.3 Static Hostname and the NCP File Server Name

During the OES 2015 SP1 install, you assign a static IP address (IPv4), a host name, and a domain name to the server. NCP Server uses the server hostname (such as `server1`) as the NCP File Server Name, and generally considers that the hostname never changes. If you modify the host name after the installation, you must also modify the NCP File Server Name parameter. For information, see Section 3.12, “Modifying the NCP File Server Name,” on page 40.

IMPORTANT: Modifying the IP address or host name for an existing server impacts most services, not just NCP Server.

3.1.4 64-Bit Support

Selecting NCP Server as part of a 64-bit installation automatically installs 64-bit NCP server.

3.1.5 NetIQ eDirectory 8.8 SP8

NCP Server manages data access for NCP volumes, Dynamic Storage Technology (DST) shadow volumes, and NSS volumes. NCP Server restricts data access to users who have User objects defined in NetIQ eDirectory. For information about configuring eDirectory and users, see the *NetIQ eDirectory 8.8 SP8 What’s New Guide*.

IMPORTANT: The server’s `root` user is the only local user who can access data without authenticating in eDirectory.

3.1.6 eDirectory Rights Needed by a Container Administrator

A container administrator (or non-administrator user) needs the following eDirectory rights to install and manage the NCP and Dynamic Storage Technology service on an OES 2015 SP1 server:

- Object Create right on the container where the NCP Server objects are.
- Object Create right where the cluster container will be.

A container administrator (or non-administrator user) needs the following eDirectory rights to manage an NCP volume on an OES 2015 SP1 server:

- Object Write and Modify rights on the Volume object.

For example, to create an NCP volume `NCPVOL1` in the `sales.mycompany.com` container, the administrator must have Create right on the `sales` Container object and the Write and Modify rights on the NCPVOL1 Volume object.

The container administrator must be Linux-enabled with Linux User Management (LUM) and be added to the LUM `admingroup` for the server. For more information, see the *OES 2015 SP1: Installation Guide*.

NOTE: If the eDirectory administrator user name or password contains special characters such as #, +, and =, ensure that you escape each special character by preceding it with a backslash(\) when you enter credentials. You do not need a backslash for other special characters such as !,@,$,%,^,&,*,(,), and-.

3.1.7 Novell Storage Services

NSS requires NCP Server; however, NSS is not required for using NCP Server with NCP volumes on Linux file systems.

In its initial release, Dynamic Storage Technology supports only NSS volumes being used as shadow volumes. If you plan to use DST, you need to install NSS when you install NCP Server and Dynamic Storage Technology.

For information about installing NSS, see “Installing and Configuring Novell Storage Services” in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

3.1.8 Novell Samba

You can install and configure Novell Samba to provide file access for CIFS/Samba users to NCP volumes. For information about configuring Samba services, see the *OES 2015 SP1: Novell Samba Administration Guide*.

If both NCP users and Samba/CIFS users access the same NCP volume or NSS volume, you should enable cross-protocol file locking for NCP. For information, see Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,” on page 38.

NCP uses the `sambasharemodes.so` library file to support the cross-protocol file locking capability that coordinates access to files by NCP users and CIFS/Samba users. NCP updates that are released through the OES 2015 SP1 and later update channels and in support packs include the `sambasharemodes.so` library file that you need for NCP. Patches for Linux Samba are also released separately through the SUSE Linux Enterprise Server 11 SP2 and later update channels. For 64-bit OES 2 Linux and later, there is a risk of breaking the cross-protocol locks functionality if the `sambasharemodes.so` library file is modified from the version released with NCP.

3.1.9 Linux User Management

Users must be Linux-enabled with Linux User Management in order to access data via CIFS/Samba protocols. Linux User Management is selected and installed automatically when you install NCP Server and Dynamic Storage Technology. For information about Linux-enabling users with Linux User Management, see the *OES 2015 SP1: Linux User Management Administration Guide*.

3.1.10 Novell AFP

Cross-protocol file locking is supported for the Novell Apple Filing Protocol (AFP) service that provides AFP access for Macintosh users to NSS volumes. This allows NCP users and AFP users to access files on an NSS volume and prevents them from concurrently modifying files by locking the file across protocols. It requires the following setup:

- NCP Server for Linux is installed and running.
- NSS for Linux is installed and running.
- Novell AFP is installed and running.
- Linux Samba is installed. It can be running or not running.
- The NCP cross-protocol file locking attribute is enabled. For information, see Section 3.11, "Configuring Cross-Protocol File Locks for NCP Server," on page 38.

For information about installing and using Novell AFP for Linux, see the *OES 2015 SP1: Novell AFP for Linux Administration Guide*.

3.1.11 Novell Cluster Services for Linux

NCP Server supports the sharing of NSS volumes on Linux, NCP volumes on Linux POSIX file systems, and DST shadow volumes in clusters with Novell Cluster Services for Linux. NCP Server itself is not clustered, and must be installed and configured on each OES 2015 SP1 node in the cluster where you plan to fail over these volumes.

For information about configuring NCP volumes in cluster resources, see Chapter 11, "Configuring NCP Volumes with Novell Cluster Services," on page 105.

For information about configuring DST shadow volumes in cluster resources, see "Configuring DST Shadow Volume Pairs with Novell Cluster Services" in the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

For information about configuring NSS volumes in cluster resources, see "Configuring and Managing Cluster Resources for Shared NSS Pools and Volumes" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

For information about installing and managing Novell Cluster Services for Linux, see the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

3.1.12 SLP

SLP (Service Location Protocol) is a required component for Novell Cluster Services on Linux when you are using NCP to access file systems on cluster resources. NCP requires SLP for the `ncpcon bind` and `ncpcon unbind` commands in the cluster load and unload scripts. For example, NCP is needed for NSS volumes and for NCP volumes on Linux POSIX file systems.

SLP is not automatically installed when you select Novell Cluster Services. SLP is installed as part of the eDirectory configuration during the OES 2015 installation. You can enable and configure SLP on the eDirectory Configuration - NTP & SLP page. For information, see "Specifying SLP Configuration Options" in the *OES 2015 SP1: Installation Guide*.

When the SLP daemon (`slpd`) is not installed and running on a cluster node, any cluster resource that contains the `ncpcon bind` command goes comatose when it is migrated or failed over to the node because the bind cannot be executed without SLP.

The SLP daemon (`slpd`) must also be installed and running on all nodes in the cluster when you manage the cluster or cluster resources.

NCP Server re-registers cluster resource virtual NCP servers with SLP based on the setting for the eDirectory advertise-life-time (`n4u.nds.advertise-life-time`) parameter. The parameter is set by default to 3600 seconds (1 hour) and has a valid range of 1 to 65535 seconds.

You can use the `ndsconfig set` command to set the `n44.nds.advertise-life-time` parameter. To reset the parameter in a cluster, perform the following tasks on each node of the cluster:

1. Log in to the node as the `root` user, then open a terminal console.
2. Take offline all of the cluster resources on the node, or cluster migrate them to a different server. At a command prompt, enter

   ```
   cluster offline <resource_name>
   ```

   or

   ```
   cluster migrate <resource_name> <target_node_name>
   ```
3. Modify the eDirectory SLP advertising timer parameter (`n4u.nds.advertise-life-time`), then restart ndsd and slpd. At a command prompt, enter

   ```
   ndsconfig set n4u.nds.advertise-life-time=<value_in_seconds>

   rcndsd restart

   rcslpd restart
   ```
4. Bring online all of the cluster resources on the node, or cluster migrate the previously migrated resources back to this node.

   ```
   cluster online <resource_name>
   ```

   or

   ```
   cluster migrate <resource_name> <node_name>
   ```
5. Repeat the previous steps on the other nodes in the cluster.

OpenSLP stores the registration information in cache. You can configure the SLP Directory Agents to preserve a copy of the database when the SLP daemon (`slpd`) is stopped or restarted. This allows SLP to know about registrations immediately when it starts.

For more information about configuring and managing SLP, see “Configuring OpenSLP for eDirectory” in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

3.1.13 Novell iManager 2.7.7 for Linux

Novell iManager 2.7.7 for Linux is required for managing eDirectory users, Samba services, Universal Password, Linux User Management, Novell Storage Services, and Novell Cluster Services for Linux. It is not necessary to install iManager on every server, but it must be installed somewhere on the network. For information about installing and using Novell iManager, see the *NetIQ iManager Installation Guide*.

3.1.14 Novell Remote Manager for Linux

Novell Remote Manager for Linux is required for managing NCP Server services, NCP volumes, and Dynamic Storage Technology. It is installed by default when you install NCP Server and Dynamic Storage Technology.

For information about using Novell Remote Manager for Linux, see the *OES 2015 SP1: Novell Remote Manager Administration Guide*. For information about management options for NCP Server, see Section 7.1.4, “Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux,” on page 52.

3.1.15 SFCB

SUSE Linux Enterprise Server (SLES) 11 uses the open source CIMOM (or CIM server) from the SBLIM project called Small Footprint CIM Broker (SFCB). OES 2015 SP1 and SLES 11 provide SFCB as the default CIMOM and SFCC for CIM client functionality.

OpenWBEM, which was used as the CIMOM in OES 2, has been replaced by SFCB as the CIMOM.

For information, see “OES Services That Require LUM-Enabled Access” in the *OES 2015 SP1: Planning and Implementation Guide*

3.1.16 Other OES 2015 SP1 Services

Ensure that you install and configure additional OES 2015 SP1 services that might be required by each of the other services mentioned in this section. Refer to the individual guides for those services for information about how to install and manage them.

3.2 Installing NCP Server

- Section 3.2.1, “Preparing for the OES 2015 SP1 Install,” on page 22
- Section 3.2.2, “Installing NCP Server during OES 2015 SP1 Installation,” on page 23
- Section 3.2.3, “Installing NCP Server on an Existing OES 2015 SP1 Server,” on page 24

3.2.1 Preparing for the OES 2015 SP1 Install

Table 3-1 identifies settings for the OES 2015 SP1 server that are used as the default settings for NCP Server at install time, and are written to the `/etc/opt/novell/ncpserv.conf` file. This file specifies parameters that enable file systems on Linux to be available to workstations that connect to it via the Novell Client or the Microsoft NCP Client. It helps enforce the Novell trustee model of file access for NCP users and CIFS/Samba users.

You can change the settings for these parameters as needed to ensure that workstations on the network can access the server. If you later modify the settings for the server, you must also reconfigure them for NCP Server.

Table 3-1 Server Settings Used by NCP Server

Linux Server Setting	NCP Server Parameter Entry in `ncpserv.conf`	Reference
Server Hostname	`NCP_FILE_SERVER_NAME` *`hostname`*	Section 3.12, "Modifying the NCP File Server Name," on page 40
Server local code page	`LOCAL_CODE_PAGE` *`code`*	Section 3.7, "Configuring the NCP Server Local Code Page," on page 33
`SYS:` volume mount point	`VOLUME sys` *`/usr/novell/sys`*	Section 3.13, "Modifying the sys: Volume Mount Point," on page 41

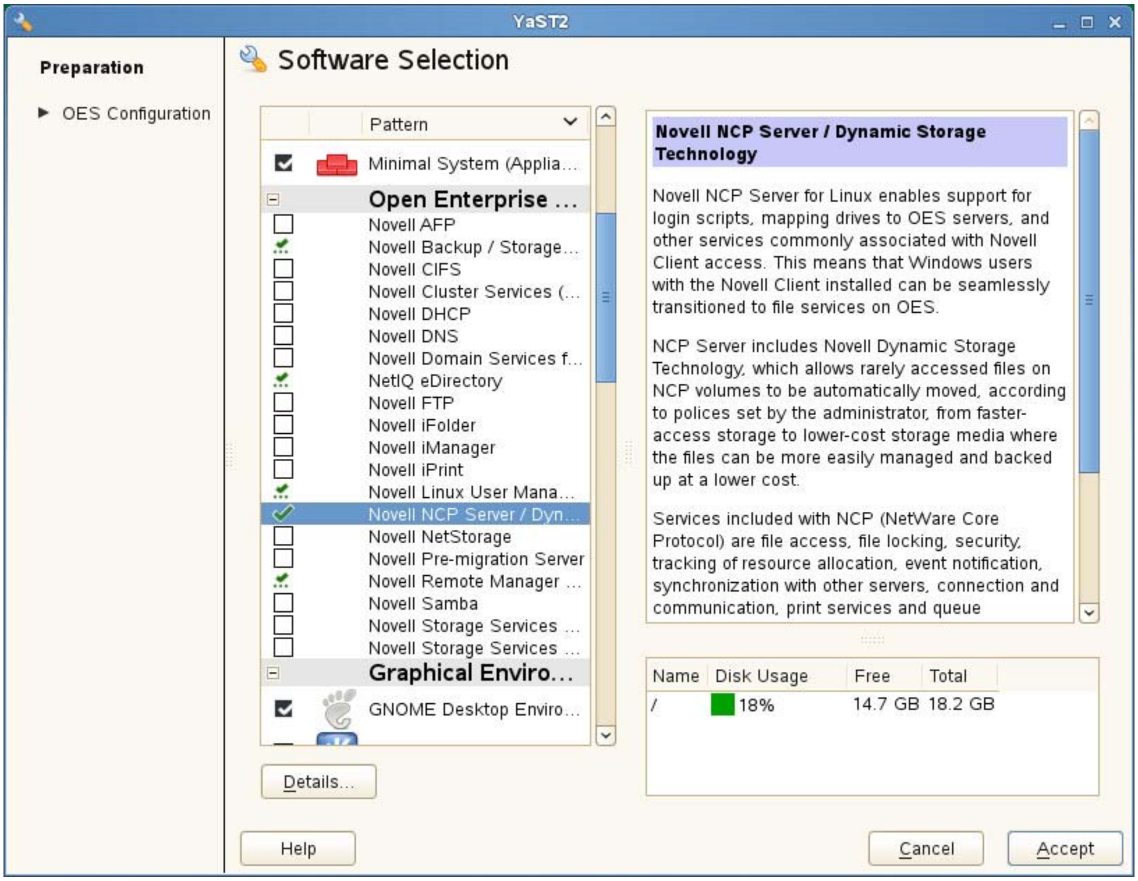
3.2.2 Installing NCP Server during OES 2015 SP1 Installation

NCP Server for Linux can be installed during OES 2015 SP1 installation. For general installation instructions, see the *OES 2015 SP1: Installation Guide*.

1. During the YaST install, on the **Install Settings** page, click **Software** to view details.
2. Select **NCP Server / Dynamic Storage Technology** option from the OES options.

   When you select **Novell NCP Server / Dynamic Storage Technology**, the following additional **OES Services** options are automatically selected:

   - **Novell Backup / Storage Management Services**
   - **NetIQ eDirectory**
   - **Novell Linux User Management**
   - **Novell Remote Manager (NRM) for Linux**



☑ Minimal System (Applia...

⊟ Open Enterprise ...

- □ Novell AFP
- ✓ Novell Backup / Storage...
- □ Novell CIFS
- □ Novell Cluster Services (...
- □ Novell DHCP
- □ Novell DNS
- □ Novell Domain Services f...
- ✓ NetIQ eDirectory
- □ Novell FTP
- □ Novell iFolder
- □ Novell iManager
- □ Novell iPrint
- ✓ Novell Linux User Mana...
- ✓ Novell NCP Server / Dyn...
- □ Novell NetStorage
- □ Novell Pre-migration Server
- ✓ Novell Remote Manager ...
- □ Novell Samba
- □ Novell Storage Services ...
- □ Novell Storage Services ...

⊟ Graphical Enviro...

☑ GNOME Desktop Enviro...

Novell NCP Server / Dynamic Storage Technology

Novell NCP Server for Linux enables support for login scripts, mapping drives to OES servers, and other services commonly associated with Novell Client access. This means that Windows users with the Novell Client installed can be seamlessly transitioned to file services on OES.

NCP Server includes Novell Dynamic Storage Technology, which allows rarely accessed files on NCP volumes to be automatically moved, according to polices set by the administrator, from faster-access storage to lower-cost storage media where the files can be more easily managed and backed up at a lower cost.

Services included with NCP (NetWare Core Protocol) are file access, file locking, security, tracking of resource allocation, event notification, synchronization with other servers, connection and communication, print services and queue

Name	Disk Usage	Free	Total
/	🟩 18%	14.7 GB	18.2 GB

3 If you plan to use NSS volumes, select **Novell Storage Services** from the **OES Services** options.

IMPORTANT: DST shadow volumes are supported only for Novell Storage Services volumes.

4 If you plan to provide access for CIFS/Samba users to NSS volumes on Linux, NCP volumes on Linux POSIX file systems, or DST shadow volumes, select **Novell Samba** from the **OES Services** options.

5 (Optional) Select **Novell iManager** from the **OES Services** options.

You must install Novell iManager somewhere in your network, but it is not necessary to install it on every server.

6 If you plan to configure NSS volumes on Linux, NCP volumes on Linux POSIX file systems, or DST shadow volumes on a cluster node, select **Novell Cluster Services (NCS)** from the **OES Services** options.

7 Click **Finish** to continue with the installation.

3.2.3 Installing NCP Server on an Existing OES 2015 SP1 Server

You can optionally install NCP Server for Linux at any time after the initial OES 2015 SP1 installation. Make sure to select the following options, just as you would for a new installation:

- **Novell Backup / Storage Management Services**
- **NetIQ eDirectory**
- **Novell Cluster Services (NCS)** (This is required only when installing NCP Server on a cluster node.)

- **Novell iManager** (If iManager is not installed on this server, you must install it somewhere in the network.)
- **Novell Linux User Management**
- **Novell NCP Server / Dynamic Storage Technology**
- **Novell Remote Manager (NRM) for Linux**
- **Novell Samba** (This is required only for CIFS/Samba users.)
- **Novell Storage Services** (This is required only where you are planning to use NSS volumes on Linux.)

For general instructions for installing and configuring OES 2015 SP1 components on an existing OES 2015 SP1 server, see "Installing or Configuring OES 2015 SP1 on an Existing Server" in the *OES 2015 SP1: Installation Guide*.

3.3 Updating NCP Server

NCP uses the `sambasharemodes.so` library file to support the cross-protocol file locking capability that coordinates access to files by NCP users and CIFS/Samba users. NCP updates that are released through the OES 2015 SP1 and later update channels and in support packs include the `sambasharemodes.so` library file that you need for NCP. Patches for Linux Samba are also released separately through the SUSE Linux Enterprise Server 11 SP2 and later update channels. For 64-bit OES 2 Linux and later, there is a risk of breaking the cross-protocol locks functionality if the `sambasharemodes.so` library file is modified from the version released with NCP.

3.4 Configuring Global NCP Server Parameters

NCP Server provides several global parameters for the SET utility that can be used to customize NCP Server for a given server. Initially, the parameters and default settings are in force, but the parameters are not explicitly added to the `/etc/opt/novell/ncpserv.conf` file. After you modify its default setting, an entry for the parameter and its new setting are added to the file. The parameter entry remains in the file even if you modify the setting back to the default.

IMPORTANT: If you use NCP Server in a cluster, make sure to set the same global policies on each OES 2015 SP1 node in the cluster where you plan to fail over the shared volumes.

There are three methods available for modifying parameter settings:

- **Novell Remote Manager:** You can view or modify server-level parameters by using Novell Remote Manager for Linux. Select **Manage NCP Services > Manage Server**, then select the **Parameter Value** link for the parameter in order to modify the setting. When you modify settings from Novell Remote Manager, NCP Server automatically restarts the NetIQ eDirectory daemon and the Novell NCP/NSS IPC daemon (if NSS is installed).
- **Command Line:** You can also modify the setting from its default value by using the `ncpcon set` command.

  ```
  ncpcon set parameter_name=value
  ```

  Replace *parameter_name* and *value* with the settings you want to change. NCP Server automatically restarts the NetIQ eDirectory daemon and the Novell NCP/NSS IPC daemon (if NSS is installed). These commands are dynamic.
- **Edit the Configuration File:** You can also modify the setting from its default value by adding the parameter to the `/etc/opt/novell/ncpserv.conf` file, then specifying the new value.

  If you modify the `/etc/opt/novell/ncpserv.conf` file, you must restart the NetIQ eDirectory daemon to make the changes go into effect. For information, see Section 3.6, "Restarting the NetIQ eDirectory (ndsd) Daemon," on page 33.

  When NSS is installed and running, and you modify values for any of the NCP Server parameters by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must manually restart `ncp2nss`. For information, see Section 3.5, "Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon," on page 32.

The following sections identify the global NCP Server parameters with their default values and valid options. For additional information about each parameter, see Section A.2, "NCPCON SET Parameters," on page 185.

- Section 3.4.1, "Directory Cache Management for NCP Server," on page 27
- Section 3.4.2, "Dynamic Storage Technology for NCP Server," on page 27
- Section 3.4.3, "Locks Management for File Access on NCP Server," on page 28
- Section 3.4.4, "Logs for NCP Server Events," on page 29
- Section 3.4.5, "NCP Communications," on page 29
- Section 3.4.6, "NCP Server Environment," on page 30
- Section 3.4.7, "NCP Volumes," on page 30
- Section 3.4.8, "NCP Volumes Low-Space Warning," on page 31
- Section 3.4.9, "TCP Connections," on page 31
- Section 3.4.10, "Managing Audit Settings," on page 32
- Section 3.4.11, "Managing NCP Threads," on page 32

3.4.1 Directory Cache Management for NCP Server

Table 3-2 *Server Parameter Information for Directory Cache Management*

Parameter Name and Description	Default Value	Value Options
MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY Controls the maximum number of file entries that can be cached by the system for a given folder in the directory cache.	10240	Minimum is 512 files.
MAXIMUM_CACHED_FILES_PER_VOLUME Controls the maximum number of file entries that can be cached by the system for a given volume in the directory cache.	256000	Minimum is 2048 files.
MAXIMUM_LAZY_CLOSE_FILES When a file is closed by the client, the NCP engine waits before closing the file just in case a client wants to reopen the file. This is called a “lazy close.” This parameter controls the maximum number of file handles that can be lazy closed in the directory cache.	4096	16 to 64000
MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME Controls the maximum number of folder entries that can be cached by the system for a volume in the directory cache.	102400	4096
LOG_CACHE_STATISTICS Controls whether cache statistics are logged in the `ncpserv.log` file.	0	0 - Disable 1 - Enable

3.4.2 Dynamic Storage Technology for NCP Server

For information about configuring global policies for DST, see the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

Table 3-3 *Server Parameter Information for Dynamic Storage Technology*

Parameter Name and Description	Default Value	Value Options
DUPLICATE_SHADOW_FILE_ACTION Controls how duplicate files conflicts are handled.	0	0 - Show duplicate shadow files (default) 1 - Hide duplicate shadow files 2 - Rename duplicate shadow files 3 - Delete duplicate files from shadow area 4 - Move duplicate shadow files to `/._DUPLICATE_FILES`

Parameter Name and Description	Default Value	Value Options
DUPLICATE_SHADOW_FILE_BROADCAST Controls whether broadcast messages are sent to NCP users whenever duplicate files conflicts occur.	1	0 - Disable 1 - Enable
REPLICATE_PRIMARY_TREE_TO_SHADOW Controls how the primary tree is replicated from the primary tree to the shadow tree. By default, it is disabled, and paths are replicated to the secondary storage area when data is actually moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location.	0	0 - Disable 1 - Enable
SHIFT_ACCESSED_SHADOW_FILES Controls whether files are moved from the secondary volume to the primary volume if the volume is accessed twice during a specified elapsed time. Use SHIFT_DAYS_SINCE_LAST_ACCESS to specify the time period. The file is moved after it is closed.	0	0 - Disable 1 - Enable
SHIFT_MODIFIED_SHADOW_FILES Controls whether files are moved from the secondary volume to the primary volume if the file is modified. The file is moved after it is closed.	1	0 - Disable 1 - Enable
SHIFT_DAYS_SINCE_LAST_ACCESS Specifies the number of elapsed days during which a file must be accessed twice before it is moved. This applies only if SHIFT_ACCESSED_SHADOW_FILES is enabled.	1	0 - Disable 1 to 365 (in days)

3.4.3 Locks Management for File Access on NCP Server

Table 3-4 *Server Parameter Information for Locks Management*

Parameter Name and Description	Default Value	Value Options
CROSS_PROTOCOL_LOCKS Controls cross-protocol file locking support with Samba. Cross-protocol locks help prevent the same file from being concurrently accessed for modifications from both a Samba and NCP client.	1	1 - Enable 0 - Disable
OPLOCK_SUPPORT_LEVEL Controls NCP opportunistic locking, which allows the client to cache file data for better performance.	2	0 - Disable 1 - Exclusive locks 2 - Shared and exclusive locks

Parameter Name and Description	Default Value	Value Options
LOCK_RANGE_MASK	1	By default this parameter is turned on. Setting the parameter value to 0 turns off this parameter and does not permit locking beyond the 0x7fffffffffffffff region.

3.4.4 Logs for NCP Server Events

Table 3-5 Server Parameter Information for Logging NCP Server Events

Parameter Name and Description	Default Value	Value Options
LOG_LEVEL Controls the nature and types of messages that are logged to the /var/opt/novell/log/ncpserv.log file.	WARN	Each level logs entries for its level and the levels above it. NOTHING ERROR WARNING INFO DEBUG ALL
LOG_CACHE_STATISTICS Controls whether cache statistics are logged in the ncpserv.log file.	0	0 - Disable 1 - Enable
LOG_IDBROKER_ERRORS Controls whether ID broker errors are logged in the ncpserv.log file.	0	0 - Disable 1 - Enable
LOG_MEMORY_STATISTICS Controls whether memory statistics are logged in the ncpserv.log file.	0	0 - Disable 1 - Enable

3.4.5 NCP Communications

Table 3-6 Server Parameter Information for Communications

Parameter Name and Description	Default Value	Value Options
FIRST_WATCHDOG_PACKET Controls how long to wait in minutes of inactivity before checking to see if an NCP connection is still alive.	0	0 - Disable 1-120 (minutes) - Enable
DISABLE_BROADCAST Controls the ability to broadcast messages from the NCP Server.	0	0 - Disable 1 - Enable

3.4.6 NCP Server Environment

***Table 3-7** Server Parameter Information for the NCP Server Environment*

Parameter Name and Description	Default Value	Value Options
LOCAL_CODE_PAGE Controls which base code page is used by the NCP Server. For more information, see Section 3.7, "Configuring the NCP Server Local Code Page," on page 33.	CP437	Valid language codes
NCP_FILE_SERVER_NAME This parameter is set by eDirectory when the NCP Server is installed, and must not be modified arbitrarily. For information, see Section 3.12, "Modifying the NCP File Server Name," on page 40.	Server hostname	This setting must match the server hostname, such as `server1`.

3.4.7 NCP Volumes

***Table 3-8** Server Parameter Information for Volume and File Management*

Parameter Name and Description	Default Value	Value Options
COMMIT_FILE	0	0 - Disable 1 - Enable
EXECUTE_ATTRIBUTE_SUPPORT	1	0 - Disable 1 - Enable
KEEP_NSS_FILE_DELETOR_IDS	1	0 - Disable 1 - Enable
SENDFILE_SUPPORT	0	0 - Disable 1 - Enable
SYNC_TRUSTEES_TO_NSS_AT_VOLUME_MOUNT Controls trustee resynchronization for an NSS volume when it is mounted for NCP.	0	0 - Disable 1 - Enable
VOLUME_GONE_WARN_USERS Controls whether a message is broadcast to warn users when the volume path is no longer present.	1	0 - Disable 1 - Enable

3.4.8 NCP Volumes Low-Space Warning

Table 3-9 Server Parameter Information for Volume Low-Space Warning

Parameter Name and Description	Default Value	Value Options
VOLUME_EMPTY_WARN_USERS Controls whether a message is broadcast to warn users when no volume space is available.	1	0 - Disable 1 - Enable
VOLUME_LOW_WARN_USERS Controls whether a message is broadcast to warn users when volume space is low.	1	0 - Disable 1 - Enable
VOLUME_LOW_WARNING_RESET_THRESHOLD Sets the high watermark threshold (in MB), which is the level where the low watermark threshold is reset, and users no longer receive the low-space message.	128	0 to 100000
VOLUME_LOW_WARNING_THRESHOLD Sets the low watermark threshold (in MB) that indicates space is low.	64	0 to 100000

3.4.9 TCP Connections

Table 3-10 Server Parameter Information for the TCP Connections

Parameter Name and Description	Default Value	Value Options
NCP_TCP_KEEPALIVE_INTERVAL Allows you to configure the keep-alive timeout for all TCP client connections accepted by the NCP server. The TCP keep-alive packet is sent by the server if the client is inactive for t this amount of time. This parameter also helps the NCP server to clear unwanted connections. The actual time taken to clear the unwanted NCP connections also depends on other system-wide TCP keep-alive parameters, like net.ipv4.tcp_keepalive_probes and net.ipv4.tcp_keepalive_intv. These parameters can be controlled by using the `sysctl` command.	8 minutes	Valid range: 3 minutes to 240 minutes
NCP_KEEPALIVE_INTERVAL If NCP_KEEPALIVE_INTERVAL=-1, then the behavior for NCP_TCP_KEEPALIVE_INTERVAL remains unaltered. If NCP_KEEPALIVE_INTERVAL > 0, whenever the client is idle then the connections remain open till the time mentioned for this parameter elapses provided FIRST_WATCHDOG_PACKET=0 or FIRST_WATCHDOG_PACKET > NCP_KEEPALIVE_INTERVAL.	-1	Valid Range: -1 and 3 minutes to 240 minutes

3.4.10 Managing Audit Settings

Table 3-11 Server Parameter Information for the Auditing Support

Parameter Name and Description	Default Value	Value Options
AUDITING_SUPPORT Indicates whether auditing support is enabled for NCP. The default value is 0, which indicates that auditing is turned off.	0	Valid values: 0 and 1

3.4.11 Managing NCP Threads

Table 3-12 Server Parameter Information for the NCP Thread

Parameter Name and Description	Default Value	Value Options
ADDITIONAL_SSG_THREADS Sets the number of additional SSG Threads (above the fixed 25 NCP threads) that can be used to serve incoming NCP file service requests. These threads are used when the 25 NCP threads are busy and taking more than the expected time to finish.	25	Valid range: 7 to 103
CONCURRENT_ASYNC_REQUESTS Sets the maximum number of the Async eDirectory NCP request threads that can be created.	25	Valid range: 15 to 256

3.5 Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon

If NSS is installed, NCP Server runs the Novell NCP/NSS IPC (`/etc/init.d/ncp2nss`) daemon in order to synchronize its settings with NSS. When you modify NCP Server settings by using Novell Remote Manager for Linux, NCP Server automatically restarts `ncp2nss` so that the new settings are immediately synchronized with NSS. If you modify values for any of the NCP Server parameters by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must manually restart `ncp2nss`.

1 On the OES 2015 SP1 server, open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, enter

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

If ncp2nss restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...

Exited

Starting the Novell NCP/NSS IPC daemon.
```

3.6 Restarting the NetIQ eDirectory (ndsd) Daemon

When you modify NCP Server settings by using Novell Remote Manager for Linux, NCP Server automatically restarts the NetIQ eDirectory daemon to apply the new settings. If you modify the `/etc/opt/novell/ncpserv.conf` file, you must restart the NetIQ eDirectory daemon to make the changes go into effect.

Use the following steps to stop and start `ndsd` when a single instance is running.

1. Use the following commands to stop `ndsd`:

   ```
   rcndsd stop
   ```

2. Use the following commands to start `ndsd`:

   ```
   rcndsd start
   ```

3.7 Configuring the NCP Server Local Code Page

NCP Server supports most commonly used code pages. NCP Server by default uses the code page corresponding to the code page used by the Linux server operating system that is specified at install time.

For example, if the Linux server is installed as a Japanese server, NCP Server uses the shift-JIS as its local code page. If the Linux server is installed as a French server, NCP Server uses the CP850 as its local code page.

Some examples of code page are CP437, CP850, CP737, CP866, CP874, CP949, SJIS, BIG5, and GBK. For a complete list of available code pages, open a terminal console, then enter

```
iconv --list | more
```

If you want NCP Server to use a code page that might be different than the one that is set for the Linux server, you must specify that code page in the `/etc/opt/novell/ncpserv.conf` configuration file. After you modify the initial setting, the code page for NCP Server does not change if you change the code page used for the Linux server. You must modify the settings separately as needed.

- Section 3.7.1, “Using Novell Remote Manager for Linux to Configure the Local Code Page,” on page 33
- Section 3.7.2, “Editing the /etc/opt/novell/ncpserv.conf File to Configure the Local Code Page,” on page 34

3.7.1 Using Novell Remote Manager for Linux to Configure the Local Code Page

To set the code page parameter by using Novell Remote Manager for Linux:

1. In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the `root` user.

   The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

   ```
   https://192.168.1.1:8009
   ```

2. Select **Manage NCP Services > Manage Server** to view the **Server Parameter Information**.
3. Click the link for the **LOCAL_CODE_PAGE** setting.

4 In **New Value**, type the new code value you want to use for NCP Server, then click **Change**.

5 On the Server Parameter Information page, verify that the new setting is displayed for the **LOCAL_CODE_PAGE** parameter.

3.7.2 Editing the /etc/opt/novell/ncpserv.conf File to Configure the Local Code Page

To manually edit the value in the `/etc/opt/novell/ncpserv.conf` file:

1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.

2 Add the following command line:

```
LOCAL_CODE_PAGE Code_Page
```

Replace *Code_Page* with the code page you want to use for NCP Server. It can be the same or different than the code page currently assigned.

3 Save the file.

4 Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

3.8 Configuring the Execute Only File Attribute for NCP Server

The NCP Execute Only attribute can be associated with the user mode execute bit on a file or subdirectory. With this setting turned on, NCP clients can set or clear this bit. The Novell Client for Linux uses this bit to represent the user mode execute bit on a file or subdirectory.

The Execute Only file attribute for NCP Server is enabled by default. You can enable or disable support for the attribute with the **Execute_Attribute_Support** option in the `/etc/opt/novell/ncpserv.conf` configuration file.

- Section 3.8.1, “Using Novell Remote Manager for Linux to Configure the Execute Attribute Support,” on page 34
- Section 3.8.2, “Editing the /etc/opt/novell/ncpserv.conf File to Configure the Execute Attribute Support,” on page 35

3.8.1 Using Novell Remote Manager for Linux to Configure the Execute Attribute Support

1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the `root` user.

The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```

2 Select **Manage NCP Services > Manage Server** to view the **Server Parameter Information**.

3 Click the link for the **EXECUTE_ATTRIBUTE_SUPPORT** setting.

4 In **New Value**, type a 0 (disable) or 1 (enable), then click **Change**.

5 On the Server Parameter Information page, verify that the new setting is displayed for the EXECUTE_ATTRIBUTE_SUPPORT parameter.

3.8.2 Editing the /etc/opt/novell/ncpserv.conf File to Configure the Execute Attribute Support

You can enable or disable support for the Execute Only attribute by manually editing the value for the EXECUTE_ATTRIBUTE_SUPPORT parameter in the `/etc/opt/novell/ncpserv.conf` file.

1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.

2 If the EXECUTE_ATTRIBUTE_SUPPORT parameter is not present, add the following line as the default setting of enabled:

```
EXECUTE_ATTRIBUTE_SUPPORT 1
```

3 You can optionally disable support, by changing the value from 1 to 0.

```
EXECUTE_ATTRIBUTE_SUPPORT 0
```

4 Save the file.

5 Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

```
rcndsd stop
```

```
rcdsd start
```

3.9 Configuring Sendfile Support for NCP Server

The Linux `sendfile()` API improves the performance for file reads. `Sendfile()` support is disabled by default.

Samba has had problems in the past with `sendfile()`. If you enable `sendfile()` and experience problems with Samba, you can disable `sendfile()` support in the `/etc/opt/novell/ncpserv.conf` configuration file.

- Section 3.9.1, “Using Novell Remote Manager for Linux to Configure Sendfile Support,” on page 35
- Section 3.9.2, “Editing the /etc/opt/novell/ncpserv.conf File to Configure Sendfile Support,” on page 36

3.9.1 Using Novell Remote Manager for Linux to Configure Sendfile Support

1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the `root` user.

The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```

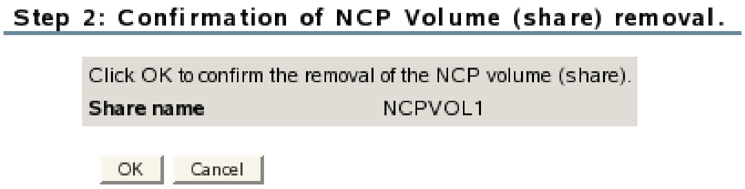
2 Select **Manage NCP Services > Manage Server** to view the **Server Parameter Information**.

3 Click the link for the **SENDFILE_SUPPORT** setting.

4 In **New Value**, type a 0 (disable) or 1 (enable), then click **Change**.

5 On the Server Parameter Information page, verify that the new setting is displayed for the SENDFILE_SUPPORT parameter.

Figure 3-1 Confirm Removal of NCP Volume



Step 2: Confirmation of NCP Volume (share) removal.

Click OK to confirm the removal of the NCP volume (share).

Share name NCPVOL1

3.9.2 Editing the /etc/opt/novell/ncpserv.conf File to Configure Sendfile Support

You can enable or disable `sendfile()` API support by manually adding or editing the value for the SENDFILE_SUPPORT parameter in the `/etc/opt/novell/ncpserv.conf` file.

1 On the OES 2015 SP1 server, log in as the `root` user.

2 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.

For example, to use `gedit`, open a terminal console, then enter

```
gedit /etc/opt/novell/ncpserv.conf
```

3 If the SENDFILE_SUPPORT parameter is not present, add the following line as the default setting of disabled:

```
SENDFILE_SUPPORT 0
```

4 You can optionally enable sendfile support by changing the value from 0 to 1.

```
SENDFILE_SUPPORT 1
```

5 Save the file.

6 Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

7 Synchronize the change with NSS by restarting `/etc/init.d/ncp2nss`. At a terminal console prompt, enter the following as the `root` user:

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

3.10 Configuring Opportunistic Locking for NCP Server

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

IMPORTANT: To use oplocks effectively, make sure users are running Novell Client 4.2 SP2 or later.

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.

For more information on oplocks with NCP Server, see Section 13.1, “Understanding Opportunistic Locking for NCP Connections,” on page 127.

- Section 3.10.1, “Using Novell Remote Manager for Linux to Configure Oplocks,” on page 37
- Section 3.10.2, “Editing the /etc/opt/novell/ncpserv.conf File to Configure Oplocks,” on page 37

3.10.1 Using Novell Remote Manager for Linux to Configure Oplocks

1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the `root` user.

  The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

  ```
  https://192.168.1.1:8009
  ```

2 Select **Manage NCP Services > Manage Server** to view the **Server Parameter Information**.

3 Click the link for the **OPLOCK_SUPPORT_LEVEL** setting.

4 In **New Value**, type a 0 (disable) or 1 (exclusive lock) or 2 (shared lock), then click **Change**.

5 On the Server Parameter Information page, verify that the new setting is displayed for the OPLOCK_SUPPORT_LEVEL parameter.

3.10.2 Editing the /etc/opt/novell/ncpserv.conf File to Configure Oplocks

You configure oplocks support in the `/etc/opt/novell/ncpserv.conf` configuration file. 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. However, you do need the line in order to change it back to the default of 2.

To disable oplocks support:

1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.

2 Add the OPLOCK_SUPPORT_LEVEL option with the value of 0 as follows:

  ```
  OPLOCK_SUPPORT_LEVEL 0
  ```

3 Save the file.

4 Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

  ```
  rcndsd stop
  ```

  ```
  rcndsd start
  ```

To set oplocks support to level 1 or 2:

1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.

2 Add the OPLOCK_SUPPORT_LEVEL option, and specify a level 1 (exclusive lock) or 2 (shared lock):

  ```
  OPLOCK_SUPPORT_LEVEL 1
  ```

or

```
OPLOCK_SUPPORT_LEVEL 2
```

3 Save the file.

4 Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

3.11 Configuring Cross-Protocol File Locks for NCP Server

Enabling cross-protocol locks turns on the cross-protocol checking for physical record locks. This lets you concurrently run applications from Samba clients, Novell AFP clients, Novell CIFS clients, and NCP clients, so each recognizes when the other has the file in use. Enabling cross-protocol locks enables file share modes. File share modes allow an application to specify 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.

NCP Server has an internal byte-ranging mechanism to prevent potential data corruption when files on NSS and NCP volumes are accessed by NCP clients. Cross-protocol file locking uses the Linux Advisory byte-range lock to prevent potential data corruption when files are accessed by non-NCP file access protocols and by other applications that directly access the files with POSIX APIs. By default, cross-protocol file locking is enabled (CROSS_PROTOCOL_LOCKS = 1) on OES 2015 SP1 servers. Cross-protocol file locking is enforced globally for all NCP and NSS volumes on the server.

Cross-protocol locks are enabled by default.

Non-NCP file access protocols include Novell Samba, Novell CIFS, and Novell AFP. Applications include any application or service that accesses data on an NCP volume or NSS volume, such as SSH, FTP, restore, scripts, antivirus, database, management tools, and so on.

For example, for any application that directly accesses files with POSIX APIs, you must enable CROSS_PROTOCOL_LOCKS in order for the Linux Advisory byte-range locks to work and prevent any potential data corruption.

NOTE: Disabling cross-protocol file locking can cause data corruption if any application or non-NCP file access protocol accesses the same data that is accessed via NCP. We recommend that you do not disable cross-protocol file locking, even if NCP is the only active file access protocol.

For better performance, you can disable cross-protocol file locking if you are not using non-NCP file access protocols and the files are not directly accessed by other applications. However, this is not recommended, because disabling cross-protocol file locking can cause data corruption.

- Section 3.11.1, “Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks,” on page 39
- Section 3.11.2, “Editing the /etc/opt/novell/ncpserv.conf File to Configure Cross-Protocol Locks,” on page 39

3.11.1 Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks

1. In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the `root` user.

   The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

   ```
   https://192.168.1.1:8009
   ```

2. Select **Manage NCP Services > Manage Server** to view the **Server Parameter Information**.
3. Click the link for the **CROSS_PROTOCOL_LOCKS** setting.
4. In **New Value**, type a 0 (disable) or 1 (enable), then click **Change**.
5. On the Server Parameter Information page, verify that the new setting is displayed for the CROSS_PROTOCOL_LOCKS parameter.

3.11.2 Editing the /etc/opt/novell/ncpserv.conf File to Configure Cross-Protocol Locks

You can enable or disable cross-protocol locks support in the `/etc/opt/novell/ncpserv.conf` configuration file. Support is enabled by default.

To enable cross-protocol locks:

1. Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
2. Add the CROSS_PROTOCOL_LOCKS option with the value of 1 as follows:

   ```
   CROSS_PROTOCOL_LOCKS 1
   ```

3. Save the file.
4. Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

   ```
   rcndsd stop
   ```

   ```
   rcndsd start
   ```

To disable cross-protocol locks:

1. Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
2. Modify the setting from 1 to 0 for the CROSS_PROTOCOL_LOCKS option as follows:

   ```
   CROSS_PROTOCOL_LOCKS 0
   ```

3. Save the file.
4. Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

   ```
   rcndsd stop
   ```

   ```
   rcndsd start
   ```

3.12 Modifying the NCP File Server Name

The NCP File Server Name parameter is set by default to the host name of the server at install time. Typically, the host name does not change because it affects so many installed services. It might be easier to reinstall the server than to discover and modify the host name setting for all services that include the host name in their configuration files.

If you modify the server host name, use the information in this section to modify the NCP File Server Name parameter.

- Section 3.12.1, “Understanding the NCP File Server Name,” on page 40
- Section 3.12.2, “Modifying the NCP File Server Name Parameter,” on page 41

3.12.1 Understanding the NCP File Server Name

- “NCP File Server Name” on page 40
- “Using Underscore Characters in the NCP File Server Name” on page 40
- “Linux Server Host name” on page 40

NCP File Server Name

NCP Server uses the server host name (such as `server1`) as the NCP File Server Name. The setting is initially based on the value you use for the OES 2015 SP1 server host name at install time. When installing OES 2015 SP1 on a virtual machine, this is the host name you give to the guest server, not the host name of the physical host server.

IMPORTANT: The NCP File Server Name parameter is included in the `ncpserv.conf` file for informational purposes only.

If you modify the server host name, you must also modify NCP_FILE_SERVER_NAME parameter by editing the `/etc/opt/novell/ncpserv.conf` file.

Using Underscore Characters in the NCP File Server Name

NCP Server allows the use of the underscore (_) character for the NCP File Server Name parameter.

Linux Server Host name

The Linux server host name is tied to a specified machine (physical or virtual) and is typically unique within a given network. The host name information is stored in the `/etc/hosts` file and the `/etc/HOSTNAME file`. The following simple rules are used for server host names to conform to accepted Internet standards:

- Host names can use alphabetic (a to z) characters, numeric (0 to 9) characters, and hyphens (-).
- Host names can begin and end with a letter or a digit, but cannot be only digits.
- Host names are case insensitive.

In the OES 2015 SP1 install and in YaST, underscores are treated as invalid characters for server host names and domain names, and cannot be set there. Any service, utility, or command that checks the host name for invalid characters might not work if you use underscores in the host name. However, many services, including BIND for the DNS Server, allow their check-names functions to be disabled or to ignore invalid characters in the host name.

3.12.2 Modifying the NCP File Server Name Parameter

1 On the OES 2015 SP1 server, open a terminal console, then log in as the `root` user.

2 Open the `/etc/opt/novell/ncpserv.conf` file in a text editor.

For example, to use gedit, enter

```
gedit /etc/opt/novell/ncpserv.conf
```

3 Locate the NCP_FILE_SERVER_NAME parameter.

For example, the entry for a server with a fully qualified host name of `server1.example.com` is set to a value of `server1` as follows:

```
NCP_FILE_SERVER_NAME server1
```

4 Type the new hostname. For example:

```
NCP_FILE_SERVER_NAME server-abc
```

5 Save the file.

6 Restart the NetIQ eDirectory (ndsd) daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

7 Restart the Novell NCP/NSS IPC daemon by entering

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

For information about why this is necessary, see Section 3.5, “Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon,” on page 32.

3.13 Modifying the sys: Volume Mount Point

At install time, OES 2015 SP1 sets up the `sys:` volume with the Linux path of `/usr/novell/sys`, and creates an NCP volume for it in the `/etc/opt/novell/ncpserv.conf` file. The `sys:` volume contains the same `login` and `public` directories that exist on NetWare. These directories let Novell clients run commands for logging in, mapping drives, and so on, as well as providing the means for client commands to be run from login scripts.

Typically, the mount path never changes. If you need to modify the path, use the following procedure:

1 On the OES 2015 SP1 server, open a terminal console, then log in as the `root` user.

2 Open the `/etc/opt/novell/ncpserv.conf` file in a text editor.

For example, to use gedit, enter

```
gedit /etc/opt/novell/ncpserv.conf
```

3 Locate the volume definition entry for the `sys:` volume.

The default path of the sys: volume is `/usr/novell/sys`, so its initial setting is:

```
VOLUME sys /usr/novell/sys
```

4 Type the new path. For example:

```
VOLUME sys /newpath/sys
```

5 Save the file.

6 Restart the NetIQ eDirectory (ndsd) daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

7 If NSS is installed on the server, restart the Novell NCP/NSS IPC daemon by entering

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

For information about why this is necessary, see Section 3.5, “Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon,” on page 32.

4 Migrating Data from NSS Volumes to NCP Volumes on Linux File Systems

This section describes migration and compatibility issues for migrating data from Novell Storage Services (NSS) volumes on NetWare 6.5 SP8 servers or OES 2015 SP1 servers to NCP volumes on Open Enterprise Server (OES) 2015 SP1 servers.

- Section 4.1, "Guidelines for Migrating Data from an NSS Volume on NetWare to an NCP Volume on Linux," on page 43
- Section 4.2, "Planning Your Migration," on page 45

4.1 Guidelines for Migrating Data from an NSS Volume on NetWare to an NCP Volume on Linux

Consider the guidelines in this section when planning your data migration from NSS volumes to NCP volumes by using the File System Migration Tool, or by using migration commands.

- Section 4.1.1, "Trustees and Trustee Rights," on page 43
- Section 4.1.2, "User Quotas," on page 43
- Section 4.1.3, "Deleted Files," on page 44
- Section 4.1.4, "Encryption," on page 44
- Section 4.1.5, "Distributed File Services," on page 44

4.1.1 Trustees and Trustee Rights

Both NSS volumes and NCP volumes use the Novell trustee model for controlling access to data. If you migrate data from an NSS volume on NetWare to an NCP volume, the trustees and trustee rights are enforced.

IMPORTANT: Make sure that the trustees are also authorized NetIQ eDirectory users of the destination server.

4.1.2 User Quotas

NCP Server does not provide a user quotas feature, so NCP volumes cannot support user quotas that are set on the NSS volume you are migrating. After the data is migrated, the quotas are not enforced in the NCP volume.

After the migration, you can use Linux tools to set user quotas on the Linux POSIX file system underneath the NCP share if the Linux file system being used under the NCP share supports user quotas and the Linux file system resides on a local, iSCSI, or Fibre Channel drive. All users of the NCP volume must be LUM enabled.

4.1.3 Deleted Files

NCP volumes do not support the deleted file salvage and purge that is available for NSS volumes. If you have deleted files on the NSS volume, they are not migrated. If you want to salvage deleted files, do it before you migrate the data. In addition, the Salvage (Undelete) and Purge options in the Novell Client, NetStorage, and the Files and Folders plug-in to iManager are disabled for NCP volumes on Linux file systems.

4.1.4 Encryption

NCP volumes do not support volume encryption. If you migrate data from an encrypted NSS volume, the data is not encrypted on the NCP volume. This would be a major security violation.

WARNING: We strongly recommend that you do not migrate data from an encrypted NSS volume to an NCP volume.

Consider migrating the device that contains the encrypted NSS volume from the NetWare server to the Linux server. For information on this scenario, see “Moving Non-Clustered Devices From NetWare 6.5 SP8 Servers to OES 2015 SP1” in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

4.1.5 Distributed File Services

Novell Distributed File Services is a feature of Novell Storage Services. If an NSS volume contains junctions or is a junction target, it affects how you migrate the data.

- “NSS Volumes That Contain Junctions” on page 44
- “NSS Volumes That Are Junction Targets” on page 45

NSS Volumes That Contain Junctions

DFS does not support junctions on NCP volumes on Linux file systems. If the original NSS volume contains junctions, its junctions are broken after migrating its data to an NCP volume. Instead of migrating data to an NCP volume, consider one of the following methods to move the data to an NSS volume on OES 2015 SP1:

- Use the File System Migration Tool to migrate the data from the NSS volume on NetWare to an NSS volume on OES 2015 SP1.
- Use the Novell Distributed File Services Move Volume task to move the NSS volume from NetWare to Linux. For information, see “Using DFS to Move NSS Volumes” in the *OES 2015 SP1: Novell Distributed File Services Administration Guide for Linux*.
- Move the devices that contain the pool from NetWare to Linux. For information, see “Migrating NSS Devices to OES 2015 SP1” in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

NSS Volumes That Are Junction Targets

NCP volumes can be the target of junctions on NSS volumes. If the original NSS volume is a junction target, it resides in a DFS management context. The Data Migration Tool uses the same Volume object for a volume when it is migrated within the same tree. This allows the volume to keep the same DFS GUID, so junctions that point to the volume are broken only until the VLDBs that are involved are repaired, as described in Table 4-1:

***Table 4-1** Post-Migration DFS Tasks*

Destination Server's DFS Management Context	Post-Migration DFS Tasks
Same	Run VLDB repair in the DFS management context.
Different	Run a VLDB repair in both the original and destination DFS management contexts.
None, but in the same tree	Create a DFS management context that contains the destination server. This creates a new VLDB that contains the destination volume information.

For information about running a VLDB repair, see "Repairing the VLDB" in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

4.2 Planning Your Migration

You can optionally use the File System Migration Tool to migrate data and trustee information from an NSS volume on NetWare to an NCP volume on an OES 2015 SP1 server. For information, see "Migrating File Systems to OES 2015 SP1" the *OES 2015 SP1: Migration Tool Administration Guide*.

- Section 4.2.1, "System Requirements for the OES 2015 SP1 Server," on page 45
- Section 4.2.2, "Supported Platforms for the Source NSS Volume," on page 46

4.2.1 System Requirements for the OES 2015 SP1 Server

The destination server is an OES 2015 SP1 server. The destination volume is an existing NCP volume on a Linux POSIX file system.

- NCP Server must be installed and running.
- Users of the data must be NetIQ eDirectory users. They will have the same trustee rights to the NCP volume on the destination server as to the original NSS volume.
- Linux User Management must be installed and enabled on the OES 2015 SP1 server if you plan to give access to CIFS/Samba users of the NCP volume.
- Use the NCP Server Console utility (`ncpcon`) to create the target NCP volume.
- Ensure that the user who performs the migration has Read/Write access rights to the POSIX path that corresponds to the NCP volume.

4.2.2 Supported Platforms for the Source NSS Volume

The File System Migration Tool supports migrating data from NSS volumes on the following platforms or later versions:

- OES 2015 SP1
- OES 2015
- OES 11
- OES 2
- NetWare 6.5 SP8

5 Using NCP Server and NCP Volumes in a Virtualized Environment

NCP Server works regardless of whether it is installed on a Open Enterprise Server (OES) 2015 SP1 server running on a physical server or on a virtual machine (VM) guest server (DomU). NCP Server is not supported on the Xen VM host environment (that is, it is not supported to run in Dom0).

To get started with Xen Virtualization, see the Virtualization with Xen documentation.

To get started with KVM Virtualization, see the Virtualization with KVM documentation.

To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product you are using.

For information on setting up virtualized OES 2015 SP1, see "Installing, Upgrading, or Updating OES on a VM" in the *OES 2015 SP1: Installation Guide*.

6 Planning for NCP Server and NCP Volumes

This section describes requirements and guidelines for using NCP Server and NCP volumes for Open Enterprise Server (OES) 2015 SP1 servers.

6.1 NCP Volumes on Linux

NCP volumes can be created on Linux POSIX file systems (such as Ext2, Ext3, btrfs, XFS, and Reiser) on an OES 2015 SP1 server.

By default, Novell Storage Services (NSS) volumes on Linux are NCP volumes. However, NSS volumes are managed through NSS management tools and commands.

IMPORTANT: Except where otherwise noted, “NCP volumes” refers only to NCP shares on Linux POSIX file systems.

NSS volumes are mounted by default in NSS and NCP Server on server restart. You can prevent an NSS volume from mounting automatically in NCP Server by modifying its NCP/NSS bindings so that the volume is not automatically mounted at server restart. For information, see Section 10.9, “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 94.

6.2 Security Issues

6.2.1 POSIX Permissions on the NSS File System

NSS users access the volumes with their eDirectory user names, not a local Linux identity. Access is granted by using the Novell trustee model of trustees, trustee rights, and inherited rights filters. The server’s `root` user is the only local user who has local access to the NSS file system.

NSS maps the file system settings for trustee rights to the POSIX file system, but it is not a one-to-one mapping. Many security features available in the Novell trustee model are not available in POSIX, so POSIX settings cannot be viewed in the same way that they might be for a non-NSS Linux file system. For information about how NSS maps file system rights and attributes, see “Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions” in the *OES 2015 SP1: File Systems Management Guide*.

6.2.2 POSIX Permissions on Linux File Systems

For NCP volumes on Linux POSIX file systems, make sure that the Inherit POSIX Permissions option is disabled (the default setting). When this setting is disabled, the local Linux environment access is restricted to the `root` user and the file owner or creator, which is the most secure configuration. For information, see Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,” on page 91.

Inherit POSIX Permissions is not allowed to be set on an NSS volume. There is an explicit check for this, and if it is an NSS volume, an Error 22 is returned. NSS has its own handling of POSIX permissions. For information, see Section 6.2.1, “POSIX Permissions on the NSS File System,” on page 49.

6.3 Novell Dynamic Storage Technology

Dynamic Storage Technology is a component of NCP Server on OES 2015 SP1. It is supported for use with NSS volumes on Linux. For information, see the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

6.4 User Quotas on Linux POSIX File Systems

NCP Server does not provide a user quotas feature for Linux POSIX file systems. User quotas are possible if the Linux file system being used under the NCP share supports user quotas and the Linux file system resides on a local, iSCSI, or Fibre Channel drive. All users of the NCP volume must be LUM enabled. Manage the user quotas by using the Linux file system tools.

7 Management Tools for NCP Server

This section describes the tools for managing NCP Server and NCP volumes on a Open Enterprise Server (OES) 2015 SP1 server.

- Section 7.1, "Novell Remote Manager for Linux," on page 51
- Section 7.2, "NCP Server Console (NCPCON) Utility," on page 57
- Section 7.3, "NCPTOP Quick Reference," on page 58

7.1 Novell Remote Manager for Linux

Use the NCP Server plug-in for Novell Remote Manager for Linux to manage NCP Server and NCP volumes on an OES 2015 SP1 server.

- Section 7.1.1, "Installing Novell Remote Manager for Linux," on page 51
- Section 7.1.2, "Accessing Novell Remote Manager," on page 51
- Section 7.1.3, "Starting, Stopping, or Restarting Novell Remote Manager on Linux," on page 52
- Section 7.1.4, "Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux," on page 52

7.1.1 Installing Novell Remote Manager for Linux

Novell Remote Manager for Linux is installed by default as part of your OES 2015 SP1 Server installation whenever any OES 2015 SP1 pattern is selected. For information about managing Novell Remote Manager for Linux, see the *OES 2015 SP1: Novell Remote Manager Administration Guide*.

7.1.2 Accessing Novell Remote Manager

1 Access Novell Remote Manager by pointing your browser to the URL of the server you want to manage.

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

```
http://server_IP_address:8008 or other_configured_port_number
```

For example:

```
http://192.168.123.11:8008
```

```
https://192.168.123.11:8009
```

2 Log in to Novell Remote Manager as the `root` user of the server or as the NetIQ eDirectory administrator user who has sufficient rights to manage the server.

The `root` user logs in as a local user of the server, not through eDirectory. If eDirectory, Linux User Management, or PAM are not working, the `root` user can still log in to Novell Remote Manager to manage the server. The `root` user can always log in directly to the server to manage it.

Novell Remote Manager is PAM-enabled, so any Linux-enabled user can log in. Depending on the user's trustee rights for the server, the user gets access only to the tasks the user has rights to perform.

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

Novell Remote Manager on Linux is installed and runs by default. If it hangs, you can use the `/etc/init.d/novell-httpstkd` script to get status or to stop, start, or restart `httpstkd`. For the latest information about `httpstkd`, see "Starting or Stopping HTTPSTKD" in the *OES 2015 SP1: Novell Remote Manager Administration Guide*.

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

Task	Command
Status	`rcnovell-httpstkd status`
Start	`rcnovell-httpstkd start`
Stop	`rcnovell-httpstkd stop`
Restart	`rcnovell-httpstkd restart`

7.1.4 Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux

- "NCP Volumes (NCP Shares)" on page 52
- "NCP Server Parameters" on page 53
- "NCP Server Connections" on page 54
- "NCP Trustee Reports" on page 54
- "NCP Logs and Audit Logs" on page 55
- "NCP Server Statistics" on page 55
- "NCP Server Diagnostics" on page 56
- "Dynamic Storage Technology" on page 56

NCP Volumes (NCP Shares)

Table 7-1 describes the management tasks available for the **Manage NCP Services > Manage Shares** task in Novell Remote Manager for Linux.

Table 7-1 Manage NCP Services > Manage Shares

Subtasks	Management Tasks
Share Name link	Browse files and directories. View and set file system attributes for files and directories on NSS volumes. View file information. View directory information.
Mount/Unmount	Mount NCP volumes and NSS volumes to make them available to NCP clients. Unmount NCP volumes and NSS volumes to make them unavailable to NCP clients.
Info icon	NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics. Open files listed for each NCP connection. Add a shadow volume for the NCP volume. For unmounted DST shadow volumes, click the **Info** icon to remove the shadow volume relationship. Removing a shadow volume removes the entry in the `ncpserv.conf` file, but does not delete the volumes that make up the shadow volume.
Create new share	Creates an NCP volume name (share) on a Linux POSIX file system (Ext3, XFS, or Reiser), and associates it to a path on your server. You are prompted for a volume (share) name and a path to the volume. This creates a mount point to the volume you specify and makes it accessible to NCP clients. **IMPORTANT:** You cannot use this method to create an NSS volume. You must use NSS tools to create and manage NSS volumes on Linux.
Delete existing share	Removes the NCP volume and path association for NCP volumes on Linux POSIX file systems (Ext3, XFS, or Reiser). This does not remove or delete data from the directory; it removes only the volume mount point that was created for the NCP share.
NCP/NSS bindings	View or modify whether NSS volumes are NCP accessible. If they are not accessible, the `EXCLUDE_VOLUME` *`volumename`* command is added to the `/etc/opt/novell/ncp2nss.conf` file. Use this option for NSS volumes on clusters where the load script handles NCP mount of NSS volumes. Use this option for NSS volumes that you want to use as the secondary storage area in a Dynamic Storage Technology shadow volume.

NCP Server Parameters

Table 7-2 describes the management task available for the **Manage NCP Services > Manager Server** task in Novell Remote Manager for Linux.

***Table 7-2** Manage NCP Services > Manage Server*

Subtasks	Management Tasks
Server Parameter Information	View NCP Server parameters for the `SET` command and their current values. Click the **Parameter Value** link to modify the value. For a list of parameters and their default values, see Section 3.4, "Configuring Global NCP Server Parameters," on page 25.

NCP Server Connections

Table 7-3 describes the management tasks available for the **Manage NCP Services > Manage Connections** task in Novell Remote Manager for Linux.

***Table 7-3** Manage NCP Services > Manage Connections*

Subtasks	Management Tasks
Connection information	View connection statistics. Clear all **Not Logged In** connections.
Connection listing	View a list of connections. Click the name link for the connection to view statistics for the connection and a list of its open files. Clear selected connections.
Name link for the connection	View statistics for the connection. View the network address, status, privileges, and security equivalence for a logged-in-user. Send a message to the selected connection.
Broadcast messages to everyone	Broadcast messages to all logged-in NCP users. The `DISABLE_BROADCAST` parameter must be disabled (value of 0) in order for broadcast messages to be sent. Users must be using a Novell Client version that supports receiving broadcast messages, and the client must be configured to receive messages.

NCP Trustee Reports

Table 7-4 describes the management tasks available for the **Manage NCP Services > View Trustee Reports** task in Novell Remote Manager for Linux.

Table 7-4 *Manage NCP Services > View Trustee Reports*

Subtasks	**Management Tasks**
Generating an NCP Trustee report for NSS volumes	View the NCP Trustee Report. A volume's trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.
Viewing a saved NCP Trustee report	View the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.

NCP Logs and Audit Logs

Table 7-5 describes the management tasks available for the **Manage NCP Services > View Logs** task in Novell Remote Manager for Linux.

Table 7-5 *Manage NCP Services > View Logs*

Subtasks	**Management Tasks**
Logs	Download and view the `ncpserv.log` and `ncp2nss.log`.
Audit logs	Download and view the following audit logs: ◆ `ncpserv.audit.log` All the operations performed by NCP Engine are logged into this file in XML format. For example, add trustee, remove trustee, volume mount and dismount, NSS event handler startup/shutdown, add/remove volume, create shadow volume, security sync, and kill NCP connections. No file operations are logged in this file. ◆ `ncp2nss.audit.log` The following ncp2nss events are logged into this file: Open command file, write command file, ncp2nss daemon halted, ncp2nss daemon running, NSS not detected, domain socket not created, domain socket not accessible, uneb not started, failed to import uneb symbols, failed to create uneb processing thread, ndp library not started, failed to import ndp library symbols, and failed to initialize ndp library. ◆ `SYS.audit.log` ◆ *`volumename`*`.audit.log` (an audit log is listed for each NSS volume)

NCP Server Statistics

Table 7-6 describes the management tasks available for the **Manage NCP Services > View Statistics** task in Novell Remote Manager for Linux.

Table 7-6 *Manage NCP Services > View Statistics*

Subtasks	Management Tasks
Server information	View server name, server version, and product version. View the number of connections.
Server statistics	View server statistics such as up time, traffic, and caching memory use.

NCP Server Diagnostics

Table 7-7 describes the management tasks available for the **Manage NCP Services > View Diagnostic Information** task in Novell Remote Manager for Linux.

Table 7-7 *Manage NCP Services > View Diagnostic Information*

Subtasks	Management Tasks
NCP engine	View statistics for NCP events. Click the **Process ID** (**PID**) link to view information about the currently running process.
NSS interface daemon	View statistics for NSS events. Click the **Process ID** (**PID**) link to view information about the currently running process.

Dynamic Storage Technology

Table 7-8 describes the management tasks available for the **View File System > Dynamic Storage Technology Options** task in Novell Remote Manager for Linux.

Table 7-8 *View File System > Dynamic Storage Technology Options*

Subtasks	Management Tasks
Volume information	View a list of NCP volumes and NSS volumes on the server. Click the **Add Shadow** link next to an NSS volume to view share information, where you can create a shadow volume. (NCP volumes are not supported as shadow volumes.) Click the **Inventory** link next to a shadow volume to view an inventory report for both the primary and secondary volumes. Click the **View Log** link next to an NSS volume to download a copy of the audit log for the selected volume.

Subtasks	Management Tasks
Add Shadow link	This option takes you to the Share Information page. Scroll down to the **Volume Tasks** area to find the **Add Shadow Volume** task. The Share Information page and Add Shadow Volume page do not distinguish or validate whether the volumes you choose are actually supported file systems and available combinations. **WARNING:** NSS volumes must already exist when you create the shadow volume. The **Create if not present** option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.
Inventory link	View statistics and graphical trend displays for the volume's files and directories. For a DST shadow volume, the report includes information for both the primary storage area (primary area) and the secondary storage area (shadow area).
Volume information (**Info** icon)	NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics. Open files listed for each NCP connection. Add a shadow volume for the NCP volume. For unmounted DST shadow volumes, click the Info icon to access the dialog to remove the shadow volume relationship. This removes the entry in the `ncpserv.conf` file, but does not delete the volume itself. To unmount a shadow volume, click **Manage NCP Services > Manage Shares**, then click **Unmount** option next to the shadow volume.
Dynamic Storage Technology policies	Create a new policy. View a list of existing policies. Click the **Policy Name** link to modify or delete the policy.
Duplicate file resolution options	Set a global policy for how to handle duplicate files.
ShadowFS configuration	Set a global policy for whether to automatically start FUSE and Shadow File System at boot time.

7.2 NCP Server Console (NCPCON) Utility

The NCP Server Console (`ncpcon(8)`) utility is a Linux server console program for executing NetWare-related server console commands. You can use it to configure and manage NCP-specific functions on your OES 2015 SP1 server.

NCPCON is a management utility for NCP Server on Open Enterprise Server (OES) 2015 SP1. You must issue NCPCON commands as the `root` user. NCPCON commands can be issued by using either of the following methods:

- Use the `ncpcon` command in interactive mode by starting NCPCON, then entering the command at the NCPCON prompt.
- Use the `ncpcon` command in a scripting or command line mode by prepending the server console command with `ncpcon`. For scripting, double-quote the desired NCP Server console command. For example:

```
ncpcon mount sys
```

For a list of commands and usage information, see Section A.1, “NCPCON,” on page 161.

When NCPCON fails, the errors are logged in `ncpcon.err` file located at `/var/opt/novell/log`. The file stores the error number of the failed NCPCON command. The `ncpcon.err` file is overwritten if it already exists.

7.3 NCPTOP Quick Reference

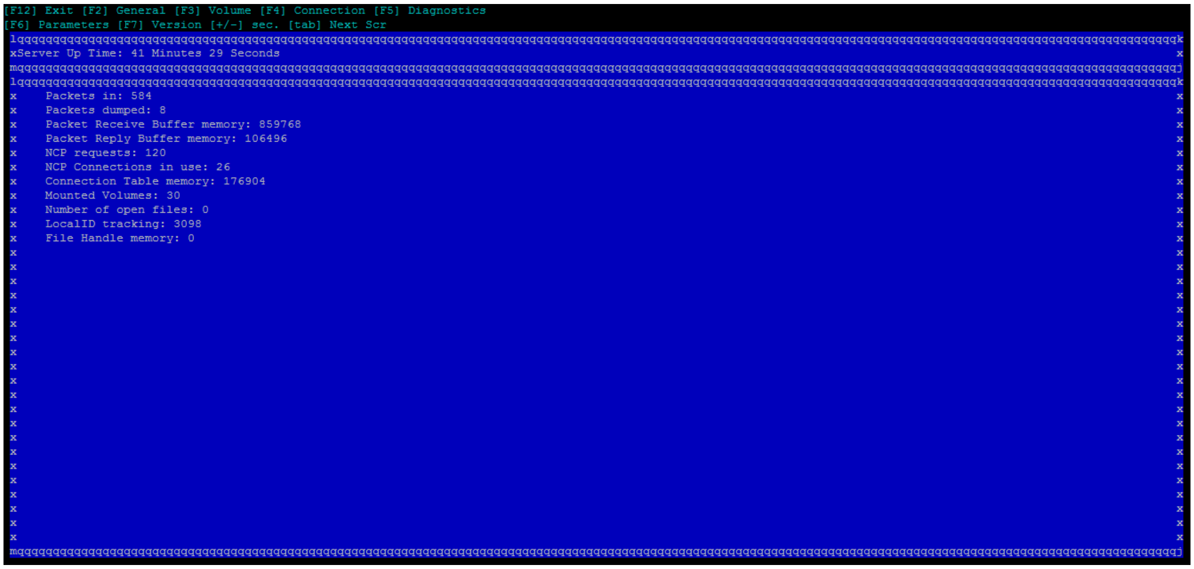
You can monitor NCP Server connections, communications, volumes, and diagnostics by using NCPTOP. NCPTOP is an interactive, real-time reporting utility that looks like the NetWare Monitor utility It is part of the `novell-ncpserv` RPM.

After NCP Server has been installed, you can start NCPTOP by entering `ncptop` at a terminal console on the Linux server. Different statistic monitoring functions of NCPTOP can be accessed by using the function keys, or you can tab through the reports. The purpose of each function key and its options are displayed within the NCPTOP utility. Table 7-9 provides an overview of tasks available.

***Table 7-9** NCPTOP Reports*

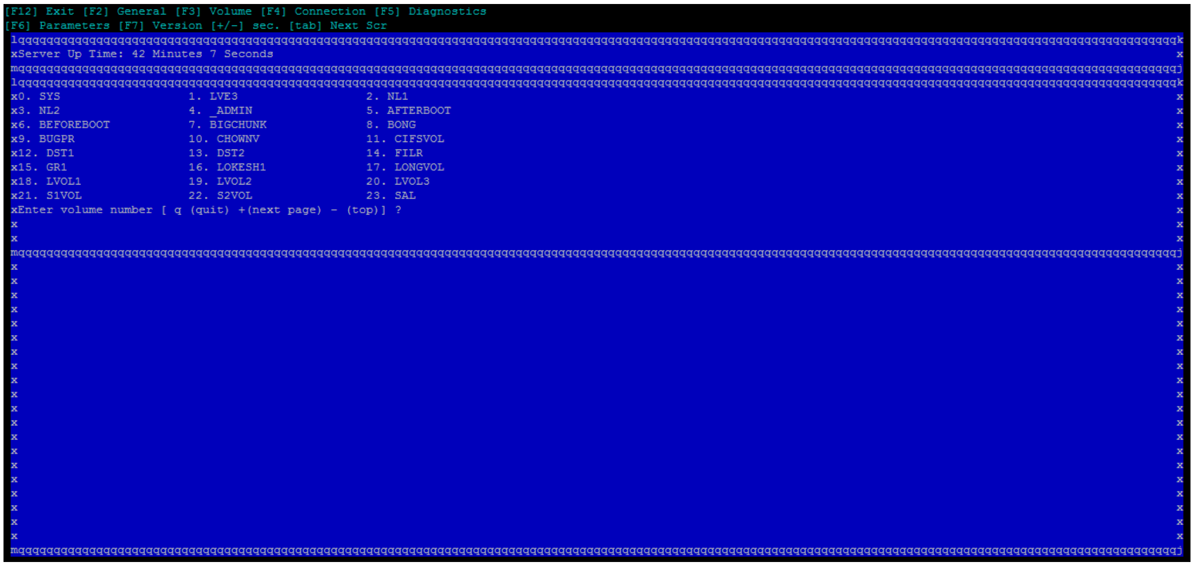
Function Key	Report	Description
F2	General	Displays a general communications report for NCP Server. See Figure 7-1 for an example report.
F3	Volume	Lists NCP volumes, and allows you to get the following details for a volume: ◆ Status ◆ Mount Point ◆ Shadow Mount Point ◆ Capacity ◆ Cached Files ◆ Cached Folders ◆ Trustee Count See Figure 7-2 for an example report.
F4	Connection	Lists the current connections, and allows you to get details for each connection. See Figure 7-3 for an example report.
F5	Diagnostics	Lists further diagnostic options. See Figure 7-4 for an example report.
F6	Parameters	Displays the current settings for the NCPCON set parameters. See Figure 7-5 for an example report. For information about the parameters, see the Section A.2, “NCPCON SET Parameters,” on page 185.
F7	Version	Reports the versions of the NCP Server software components. See Figure 7-6 for an example report.

Figure 7-1 *General Communications Report in NCPTOP*



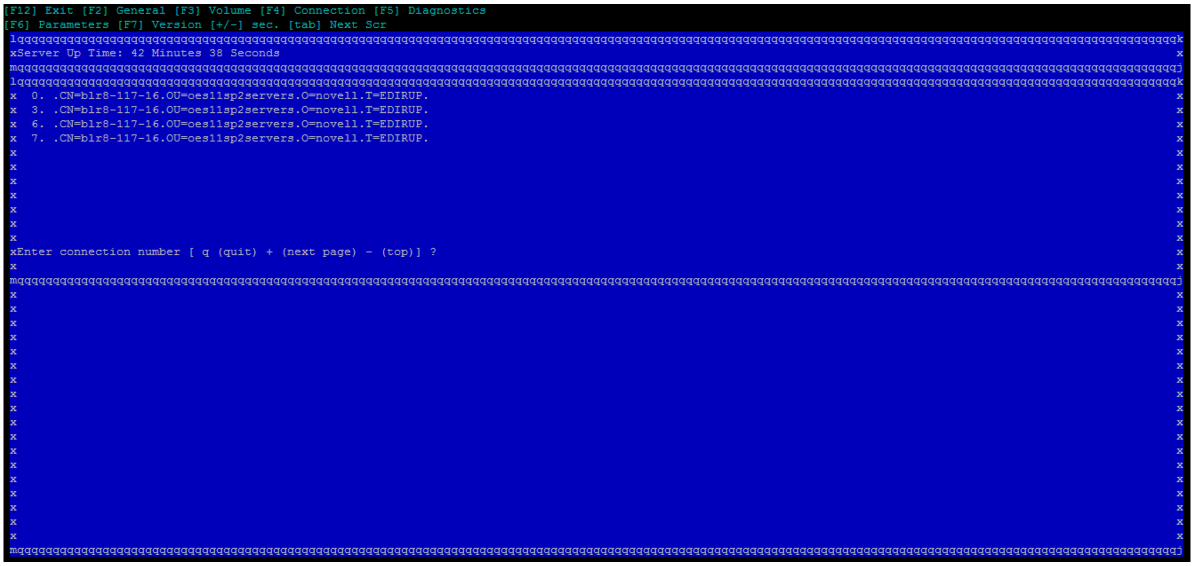
```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr
xServer Up Time: 41 Minutes 29 Seconds
x    Packets in: 584
x    Packets dumped: 8
x    Packet Receive Buffer memory: 859768
x    Packet Reply Buffer memory: 106496
x    NCP requests: 120
x    NCP Connections in use: 26
x    Connection Table memory: 176904
x    Mounted Volumes: 30
x    Number of open files: 0
x    LocalID tracking: 3098
x    File Handle memory: 0
```

Figure 7-2 *NCP Volumes Report in NCPTOP*



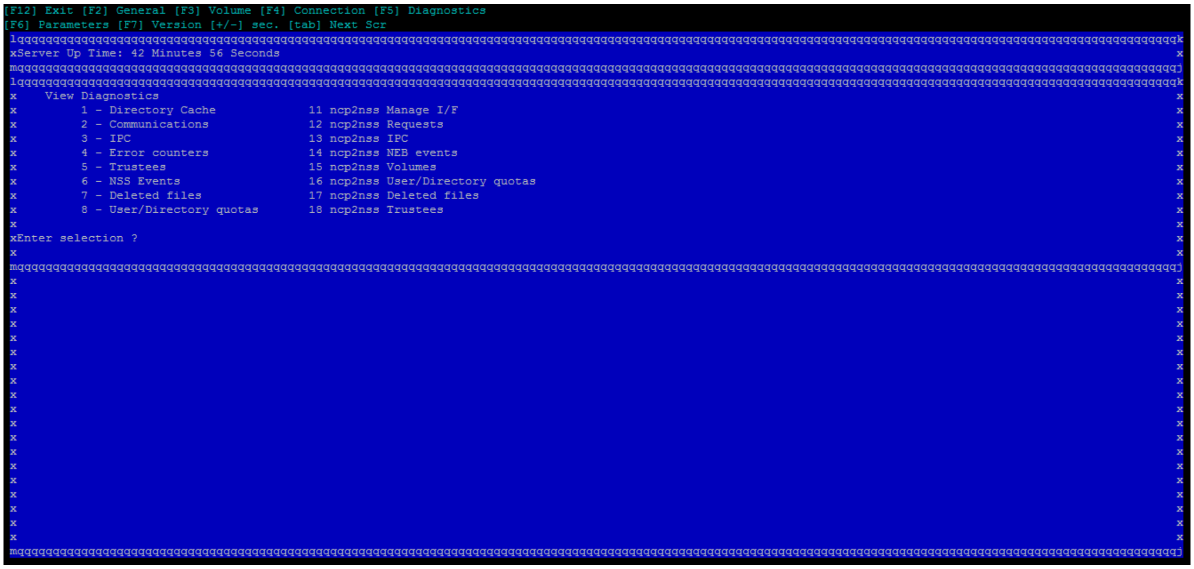
```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr
xServer Up Time: 42 Minutes 7 Seconds
x0. SYS                  1. LVE3                  2. NL1
x3. NL2                  4. _ADMIN                5. AFTERBOOT
x6. BEFOREBOOT           7. BIGCHUNK              8. BONG
x9. BUGPR                10. CHOWNV               11. CIFSVOL
x12. DST1                13. DST2                 14. FILR
x15. GR1                 16. LOKESH1              17. LONGVOL
x18. LVOL1               19. LVOL2                20. LVOL3
x21. S1VOL               22. S2VOL                23. SAL
xEnter volume number [ q (quit) +(next page) - (top)] ?
```

Figure 7-3 *Current Connections Report in NCPTOP*



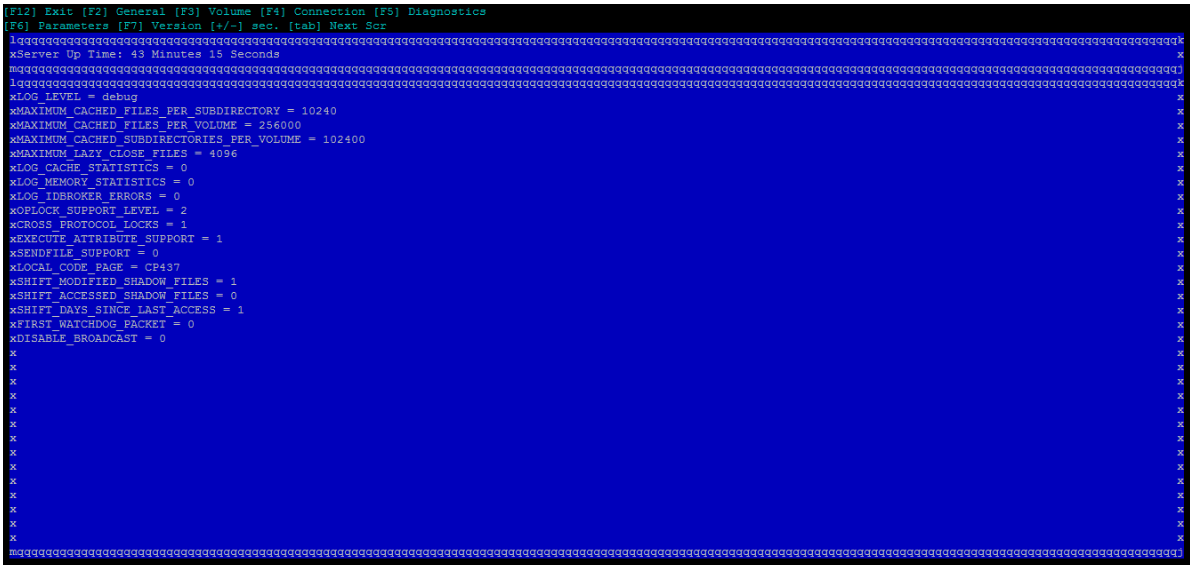
```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr
xServer Up Time: 42 Minutes 38 Seconds
x  0. .CN=blr8-117-16.OU=oes11sp2servers.O=novell.T=EDIRUP.
x  3. .CN=blr8-117-16.OU=oes11sp2servers.O=novell.T=EDIRUP.
x  6. .CN=blr8-117-16.OU=oes11sp2servers.O=novell.T=EDIRUP.
x  7. .CN=blr8-117-16.OU=oes11sp2servers.O=novell.T=EDIRUP.
xEnter connection number [ q (quit) + (next page) - (top)] ?
```

Figure 7-4 *Diagnostic Report in NCPTOP*



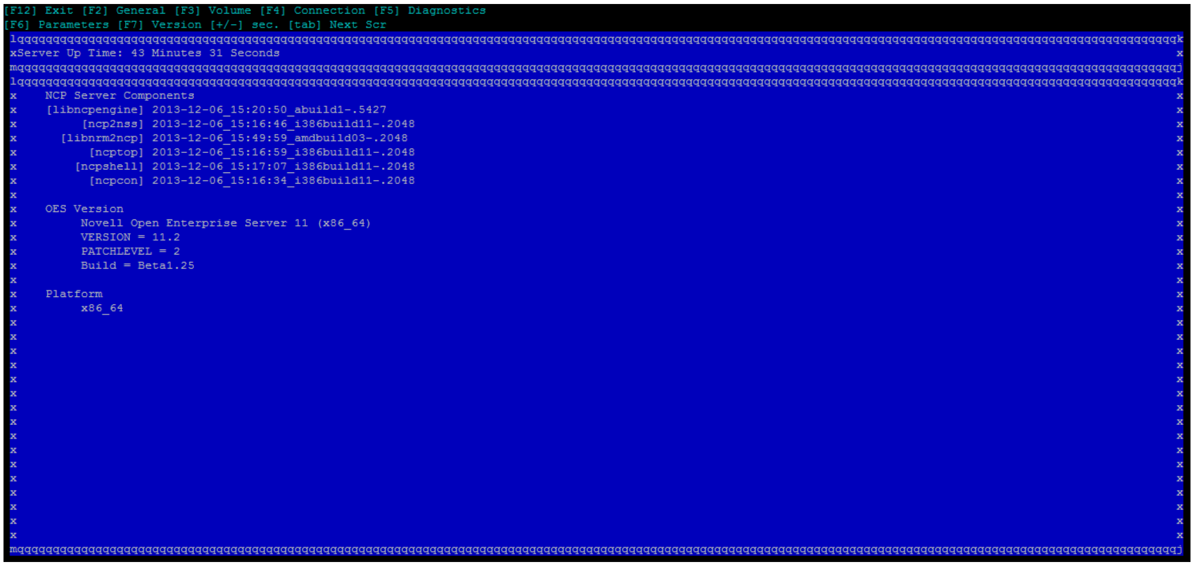
```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr
xServer Up Time: 42 Minutes 56 Seconds
x    View Diagnostics
x         1 - Directory Cache            11 ncp2nss Manage I/F
x         2 - Communications             12 ncp2nss Requests
x         3 - IPC                        13 ncp2nss IPC
x         4 - Error counters             14 ncp2nss NEB events
x         5 - Trustees                   15 ncp2nss Volumes
x         6 - NSS Events                 16 ncp2nss User/Directory quotas
x         7 - Deleted files              17 ncp2nss Deleted files
x         8 - User/Directory quotas      18 ncp2nss Trustees
x
xEnter selection ?
```

__Figure 7-5__ NCP Server Parameters Report in NCPTOP



```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr
xServer Up Time: 43 Minutes 15 Seconds
xLOG_LEVEL = debug
xMAXIMUM_CACHED_FILES_PER_SUBDIRECTORY = 10240
xMAXIMUM_CACHED_FILES_PER_VOLUME = 256000
xMAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME = 102400
xMAXIMUM_LAZY_CLOSE_FILES = 4096
xLOG_CACHE_STATISTICS = 0
xLOG_MEMORY_STATISTICS = 0
xLOG_IDBROKER_ERRORS = 0
xOPLOCK_SUPPORT_LEVEL = 2
xCROSS_PROTOCOL_LOCKS = 1
xEXECUTE_ATTRIBUTE_SUPPORT = 1
xSENDFILE_SUPPORT = 0
xLOCAL_CODE_PAGE = CP437
xSHIFT_MODIFIED_SHADOW_FILES = 1
xSHIFT_ACCESSED_SHADOW_FILES = 0
xSHIFT_DAYS_SINCE_LAST_ACCESS = 1
xFIRST_WATCHDOG_PACKET = 0
xDISABLE_BROADCAST = 0
```

__Figure 7-6__ NCP Server Components Versions Report in NCPTOP



```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr
xServer Up Time: 43 Minutes 31 Seconds
x    NCP Server Components
x    [libncpengine] 2013-12-06_15:20:50_abuild1-.5427
x         [ncp2nss] 2013-12-06_15:16:46_i386build11-.2048
x      [libnrm2ncp] 2013-12-06_15:49:59_amdbuild03-.2048
x          [ncptop] 2013-12-06_15:16:59_i386build11-.2048
x        [ncpshell] 2013-12-06_15:17:07_i386build11-.2048
x          [ncpcon] 2013-12-06_15:16:34_i386build11-.2048
x
x    OES Version
x         Novell Open Enterprise Server 11 (x86_64)
x         VERSION = 11.2
x         PATCHLEVEL = 2
x         Build = Beta1.25
x
x    Platform
x         x86_64
```

8 Managing NCP Server

This section describes how to manage NCP Server on an Open Enterprise Server (OES) 2015 SP1 server.

- Section 8.1, "Using Novell Remote Manager to Monitor NCP Server," on page 63
- Section 8.2, "Using NCPCON to Monitor NCP Server," on page 63
- Section 8.3, "Using NCPTOP to Monitor NCP Server," on page 65

8.1 Using Novell Remote Manager to Monitor NCP Server

Viewing server information can help you troubleshoot server problems. You can see process information and change file attributes for specific NCP program files.

1. In Novell Remote Manager, click **Manage NCP Services > View Diagnostic Information**.
2. Click the PID value to access additional pages for process information and to change file attributes for specific NCP program files.

8.2 Using NCPCON to Monitor NCP Server

1. Open a terminal console on the Linux server you want to manage, then log in as the `root` user.
2. At a terminal console prompt, enter

   ```
   ncpcon
   ```

3. In NCPCON, use any of the following NCPCON commands to view server information:

Command	Description
`config`	Displays the NCP Server configuration information, such as the server name, server version, product version, NCP version, mixed-mode paths status (yes/no), and commit files status (yes/no).

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><code>stats</code></td><td>Displays NCP statistics, such as the following:
◆ Server up time
◆ Packets in
◆ Packets dumped
◆ Packet receive buffer memory
◆ Packet reply buffer memory
◆ NCP requests
◆ NCP connections in use
◆ Connection table memory
◆ Mounted volumes
◆ Number of open files
◆ Local ID tracking
◆ File handle memory
◆ Volume sys: file and subdirectory caching memory
◆ Volume sys: trustee and inherited rights mask tracking memory</td></tr>
<tr><td>version</td><td>Displays version information for all currently running Novell NCP Server components, the OES build, and the hardware platform.</td></tr>
<tr><td><code>volume</code></td><td>Displays a list of currently mounted NCP volumes.</td></tr>
<tr><td><code>volume <i>ncp_volume_name</i></code></td><td>Displays information about the specified volume. The volume must be mounted before you issue the command.</td></tr>
<tr><td><code>log [filename] [level]</code></td><td>Adjusts the logging level of either the NCP Server log (<code>/var/opt/novell/log/ncpserv.log</code>) or the <code>ncp2nss</code> daemon log (<code>/var/opt/novell/log/ncp2nss.log</code>).
This command can be added to a cluster load script.
Options:
◆ filename
<code>[ncpserv.log | ncp2nss.log]</code>
◆ level
<code>[debug | dump | error | everything | info | nothing | warning]</code>
Examples:
<code>log ncpserv.log debug</code>
<code>log ncp2nss.log warning</code>
By default, the logging level is set to warning for both the NCP Server and ncp2nss daemon logs.</td></tr>
</table>

8.3 Using NCPTOP to Monitor NCP Server

You can monitor NCP Server connections, communications, volumes, and diagnostics by using NCPTOP (`ncptop(8)`), which is an interactive, real-time reporting utility.

1. Open a terminal console, then log in as the `root` user.
2. At the terminal console prompt, enter

```
ncptop
```

3. Press the function keys to view reports:

Function Key	**Reports**	**Description**
F2	General	Displays a general communications report for NCP Server.
F3	Volume	Lists NCP volumes, and allows you to get the following details for a volume: ◆ Status ◆ Mount Point ◆ Shadow Mount Point ◆ Capacity ◆ Cached Files ◆ Cached Folders ◆ Trustee Count
F4	Connection	Lists the current connections, and allows you to get details for each connection.
F5	Diagnostics	Lists further diagnostic options.
F6	Parameters	Displays the current settings for the NCPCON SET parameters. For more information about the parameters, see the Section A.2, "NCPCON SET Parameters," on page 185.
F7	Version	Reports the versions of the NCP Server software components.

9 Managing Connections for NCP Volumes and NSS Volumes

The Connection Manager allows you to view information about NCP and manage NCP client connections on an Open Enterprise Server (OES) 2015 SP1 server. Connections include those for NCP volumes (NCP shares on Linux POSIX file systems) and Novell Storage Services (NSS) volumes.

9.1 Understanding Connections

The Connection Manager reports the status of current connections for NCP Server and lists the connections. You can access the reports by using the **Manage NCP Services** > **Manage Connections** page in Novell Remote Manager or the `connection` command in the NCP Server Console (`ncpcon(8)`) utility. In Novell Remote Manager, you can also view open files for a connection, clear specific NCP connections, and send a broadcast message out to current NCP connections.

9.1.1 Connection Information

The Connection Information report displays the current status of the following parameters:

Parameter	Description
Connection Slots Allocated	Displays the number of slots currently allocated for use. As connection slots required on this server exceed the current number of slots displayed here, new slots are allocated. Depending on the server's memory, connection slots are usually allocated in blocks of 16. Connection slots are allocated as needed by users and other services.
Connection Slots Being Used	Displays the number of connection slots currently in use. As this number matches or exceeds the Connection Slots Allocated entry, more connection slots are allocated to the connection table.
Signing Level	Displays the level at which NCP packet signature signing is set on the server. NCP packet signatures prevent packet forgery by requiring the server and the workstation to sign each NCP packet. A higher packet signature number impacts the performance of your server. At some point, the need for security might outweigh certain performance issues. ◆ **0:** The server does not sign packets (regardless of the client level). ◆ **1:** The server signs packets only if the client requests it (the client level is 2 or higher). This is the default value. ◆ **2:** The server signs packets if the client is capable of signing (the client level is 1 or higher). ◆ **3:** The server signs packets and requires all clients to sign packets or logging in will fail.
Login State	Displays whether users are allowed to log in to the server. To disable users from being able to log in to the server (for server maintenance or other reasons), enter `disable login` at the NCPCON prompt, or enter `ncpcon disable login` at a terminal console prompt. To allow users to log in to the server, enter `enable login` at the NCPCON prompt, or enter `ncpcon enable login` at a terminal console prompt.
Licensed Connections	Displays the number of connections that are currently licensed. Licensed connections are authenticated, logged in, and consume a license. An unlicensed connection does not consume a license and can be authenticated or not. An unlicensed, authenticated connection can access the eDirectory database but cannot access any other resources.
Not Logged In Connections	Clears all user connections that are open but not currently authenticated to the server. Use this parameter to clear all user connections that are not logged in.

9.1.2 Connection Listing

The Connection Listing page displays the following information about each current connection:

Table 9-1 Connection Listing Report

Parameter	Description
Station	Shows the connection number for each connection. Connection 0 is the connection used by the server. The server's operating system uses connection numbers to control each station's communication with other stations. Remote Manager does not distinguish connections that don't count against the server's connection limit.
Name	Shows the name of the user, server, service, login status, and links to specific information about that user connection such as the login time, connection number, network address, login status, number of NCP requests, files in use, and security equivalence. Connections with an asterisk (*) displayed next to the name indicate an unlicensed connection (it does not consume a license). These licenses can be either authenticated or not authenticated. An unlicensed, authenticated connection can access the NetIQ eDirectory database but not other server resources. From this detailed Connection Information page, you can also clear the connection or send a message to the user.
Reads & Writes	Shows the number of reads and writes (in bytes) made by each connection.
NCP Request	Shows the number of NCP requests made by each connection.
Login Time	Shows the login day, date, and time for the connection.

9.1.3 Detailed Connection Information

For each connection, the Connection Manager reports additional details, which are available by clicking the **Name** link for the connection. Some parameters are not present if they do not apply.

Table 9-2 Detailed Connection Information Report for a Specific Connection

Parameter	Description
Connection	The station number for the connection.
Login Status	Shows whether the connection is Authenticated or Not Logged In.
Authentication Method	Shows the authentication method used if the connection is logged in.
Login Time	Shows the login day, date, and time for the connection.
Privileges	Shows whether the connection has privileges, such as Supervisor or Console Operator.
Connection Type	Shows whether the connection is internal or external.
NCP Requests	Shows the total number of NCP requests made by the connection.
Bytes Read	Shows the total number of reads made by the connection.
Bytes Written	Shows the total number of writes made by the connection.
Network Address	Shows the IP address where the connection originates.
Open Files	Shows the files open for the connection.

Parameter	Description
Security Equivalence	Shows the name of the user, server, or service if it is logged in.

9.2 Managing User Login for NCP Server

- Section 9.2.1, “Enabling Login,” on page 70
- Section 9.2.2, “Disabling Login,” on page 70

9.2.1 Enabling Login

1 Open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, enter

```
ncpcon enable login
```

9.2.2 Disabling Login

1 Open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, enter

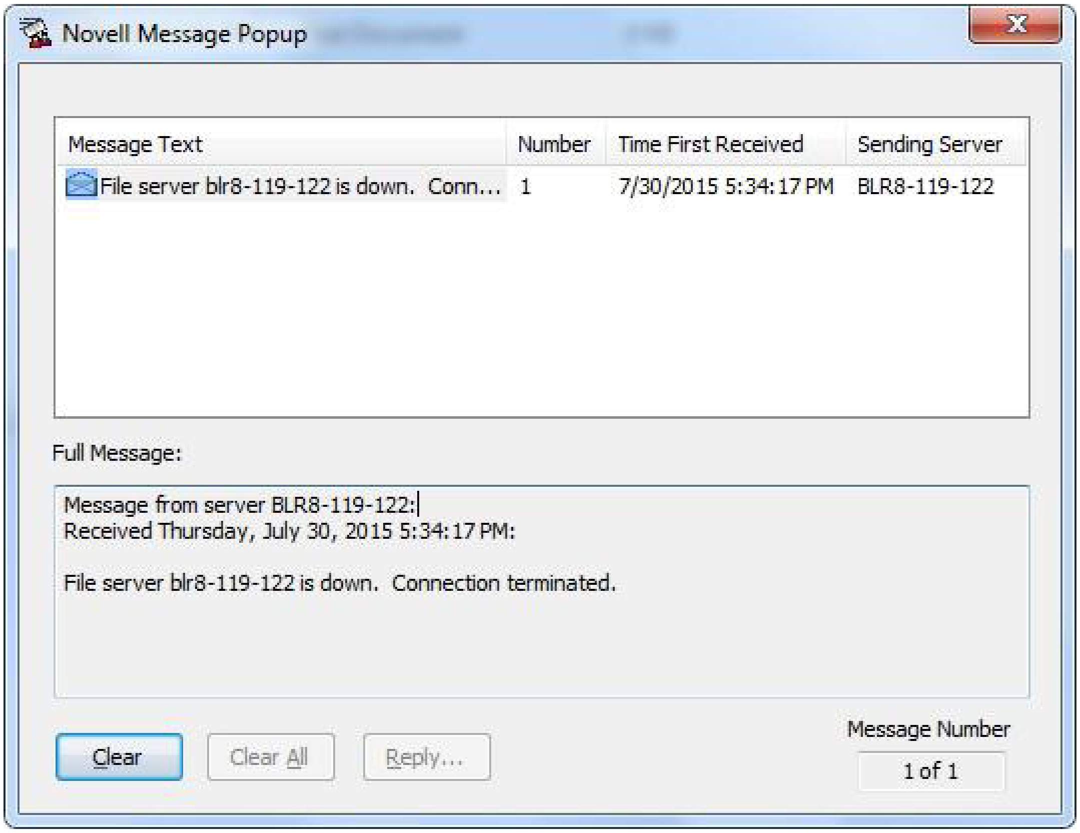
```
ncpcon disable login
```

9.3 Sending Messages to Logged-In Users

You can use the Connection Manager to send a message to NCP clients that are connected to the NCP Server via the Novell Client. Broken connections and users that are not logged in through Novell Client software do not receive the message. You typically send messages before you shut down, reset, or restart your server for any reason. You might also want to send a message to a specific user before you close an open file or clear a connection.

For example, the message appears in a Novell Message Popup dialog box at the users’ workstations.

Figure 9-1 Example Message Delivery



Message Text	Number	Time First Received	Sending Server
File server blr8-119-122 is down. Conn...	1	7/30/2015 5:34:17 PM	BLR8-119-122

Full Message:

Message from server BLR8-119-122:
Received Thursday, July 30, 2015 5:34:17 PM:

File server blr8-119-122 is down. Connection terminated.

Message Number: 1 of 1

- Section 9.3.1, "Enabling or Disabling Broadcast Message Support," on page 71
- Section 9.3.2, "Broadcasting a Message to All Users," on page 71
- Section 9.3.3, "Sending a Message to a Specific User," on page 72
- Section 9.3.4, "Configuring the Novell Client for Sending and Receiving Messages," on page 72

9.3.1 Enabling or Disabling Broadcast Message Support

The ability to send broadcast messages is enabled by default. You can disable this feature by enabling the DISABLE_BROADCAST parameter. The parameter's default setting is 0, which allows messages.

1. In Novell Remote Manager for Linux, select **Manage NCP Services > Manage Server**.
2. In the **Server Parameter Information** list, click the **Parameter Value** link for the DISABLE_BROADCAST parameter.
3. Specify the new value as 0 (default, enables broadcasting) or 1 (disables broadcasting), then click **Change**.

9.3.2 Broadcasting a Message to All Users

1. In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the **Connections Manager** page.
2. Type the message in the **Broadcast Message to Everyone** field.

You can enter up to 252 characters and spaces in the message.

3 Click **Send**.

9.3.3 Sending a Message to a Specific User

1 In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the **Connections Manager** page.

2 Scroll down to view the connections in the Connection Listing report.

3 (Optional) Sort the list by clicking the **Sort** icon ▼ in the column heading of interest.

4 Click the **Name** link for a specific connection to view details about it.

5 Type the message for the user in the **Send Message** field.

You can enter up to 252 characters and spaces in the message.

6 Click **Send**.

9.3.4 Configuring the Novell Client for Sending and Receiving Messages

For OES 2 SP1 and later, the Send Message capability is available in the Novell Client 4.9x for Windows XP/2003, the Novell Client 1.0 SP1 for Vista, and the Novell Client 2.0 for Linux.

The ability for a user to send and receive broadcast messages on the user's workstation is controlled by four NCP client property settings in the Novell Client Properties (right-click Red N, then select **Novell Client Properties**).

***Table 9-3** Novell Client Properties for Broadcast Messages*

Property	Description	Settings
Receive Broadcast Messages (under the Advanced Menu Settings tab)	Specifies which broadcast messages, if any, to be received by this client.	All - Receive all broadcast messages. Server Only - Receive broadcast messages sent by NCP Server only. None - Do not receive any broadcast messages.
Enable Send Message (under the Advanced Menu Settings tab)	Enables or disables the Send Message function for this client.	On (default) or Off
Enable Send Message to Server Dialog (under the Advanced Menu Settings tab)	Enables or disables the ability of this client to send broadcast messages to the NCP server where the user is logged in.	On or Off (default)
Enable Send Message to User Dialog (under the Advanced Menu Settings tab)	Enables or disables the ability of this client to send broadcast messages to specific NCP users.	On (default) or Off

To send a broadcast message:

1. Right-click the red N to open the menu, then select **Novell Utilities > Send Message > To Users** to open the Send Message dialog box.
2. From the list of available servers, double-click the server to see a list of users and groups connected to that server.
3. Type the message.

   You can enter up to 252 characters and spaces in the message.
4. Select the users and groups to send the message to. Press and hold down the Control key to select multiple users or groups.

   Only users who are logged in are eligible to receive the messages. Broken connections, users who are not logged in through Novell Client software, and users who are logged in with a Novell Client that does not support the Send Message feature cannot receive the message.
5. Click **Send**.

   The Send Message Results dialog box appears, showing the users and groups to whom the message was sent.

9.4 Viewing Connections for NCP Server

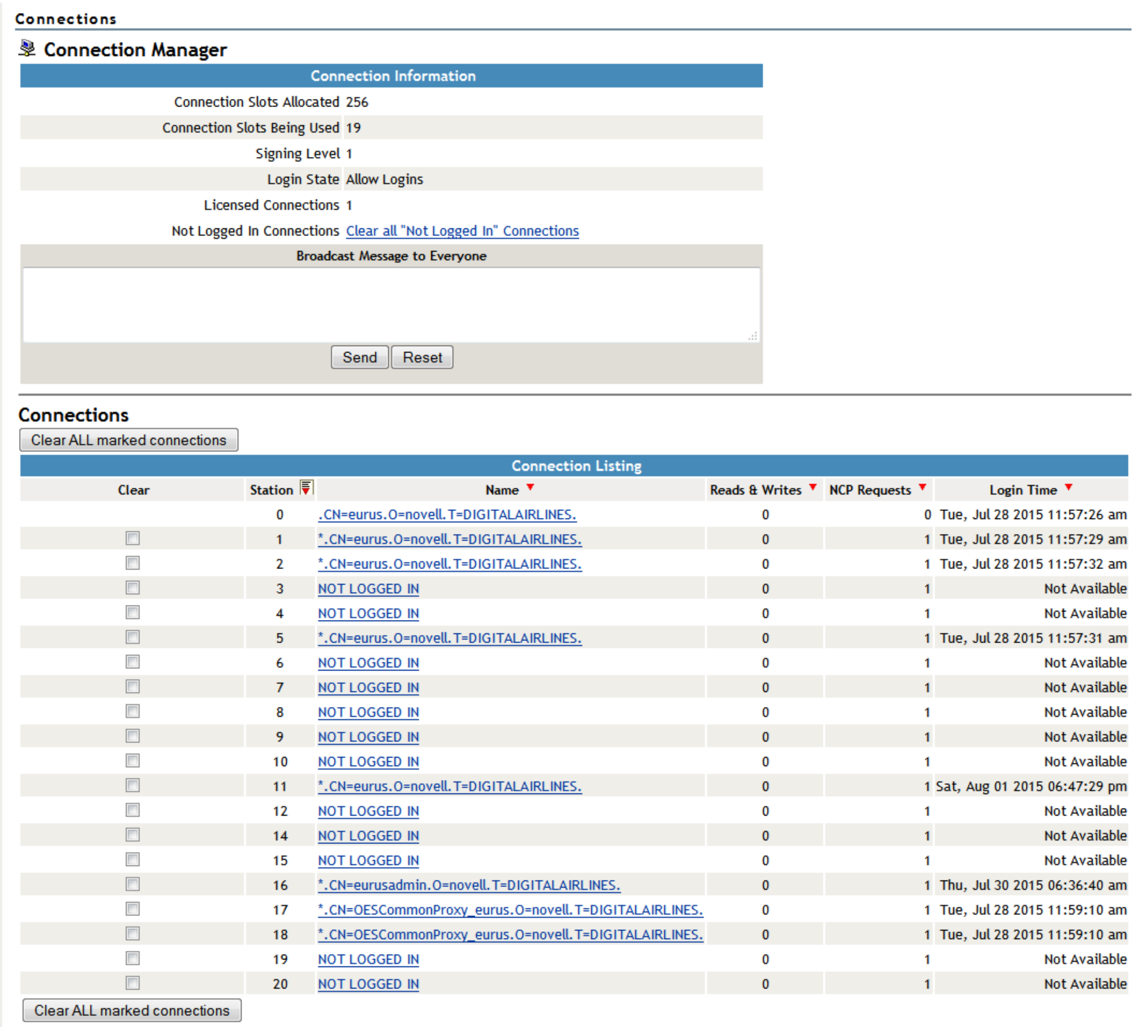
For an explanation of the connection parameters, see Section 9.1, “Understanding Connections,” on page 67.

- Section 9.4.1, “Using Novell Remote Manager to View Connections,” on page 73
- Section 9.4.2, “Using NCPCON to View Connections,” on page 75

9.4.1 Using Novell Remote Manager to View Connections

1. In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the Connection Manager page.

   The Connection Manager page reports the **Connection Information** and **Connection Listing**.



Connection Manager

Connection Information	
Connection Slots Allocated	256
Connection Slots Being Used	19
Signing Level	1
Login State	Allow Logins
Licensed Connections	1
Not Logged In Connections	Clear all "Not Logged In" Connections

Connections

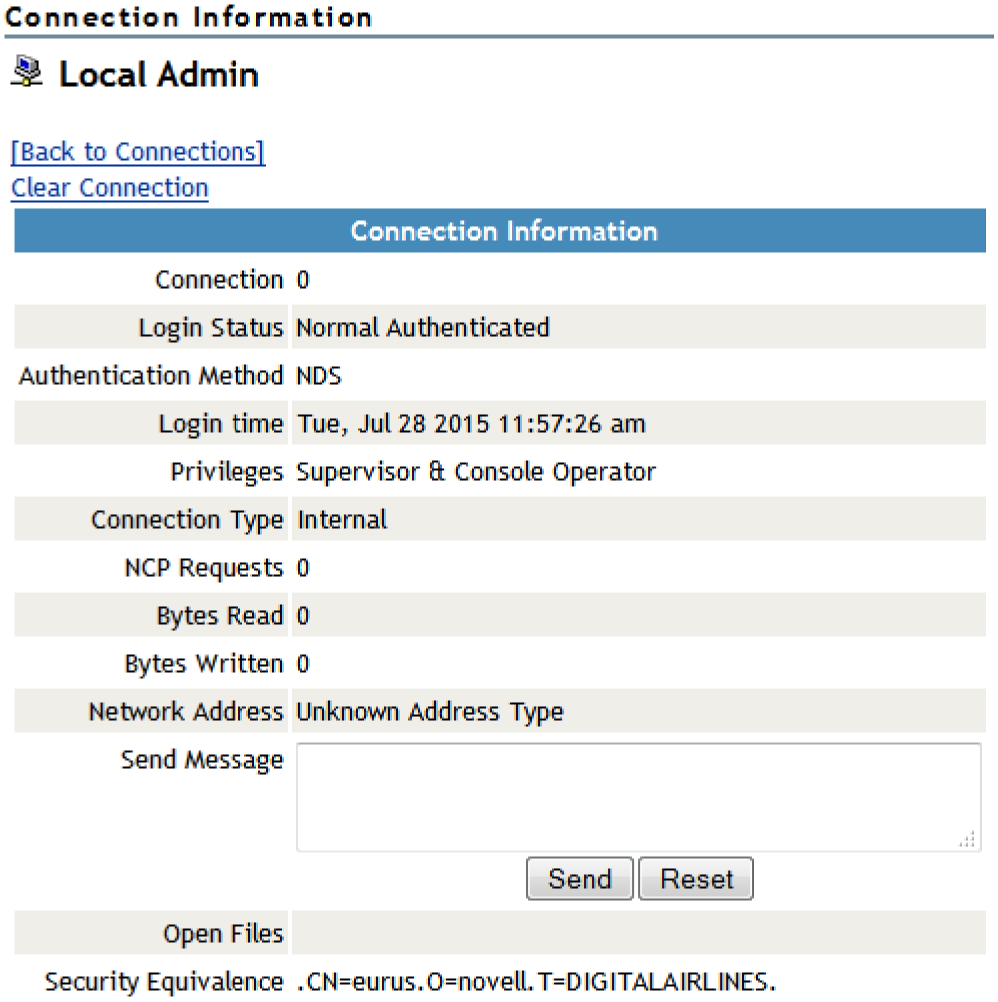
Connection Listing

Clear	Station	Name ▼	Reads & Writes ▼	NCP Requests ▼	Login Time ▼
	0	.CN=eurus.O=novell.T=DIGITALAIRLINES.	0	0	Tue, Jul 28 2015 11:57:26 am
□	1	*.CN=eurus.O=novell.T=DIGITALAIRLINES.	0	1	Tue, Jul 28 2015 11:57:29 am
□	2	*.CN=eurus.O=novell.T=DIGITALAIRLINES.	0	1	Tue, Jul 28 2015 11:57:32 am
□	3	NOT LOGGED IN	0	1	Not Available
□	4	NOT LOGGED IN	0	1	Not Available
□	5	*.CN=eurus.O=novell.T=DIGITALAIRLINES.	0	1	Tue, Jul 28 2015 11:57:31 am
□	6	NOT LOGGED IN	0	1	Not Available
□	7	NOT LOGGED IN	0	1	Not Available
□	8	NOT LOGGED IN	0	1	Not Available
□	9	NOT LOGGED IN	0	1	Not Available
□	10	NOT LOGGED IN	0	1	Not Available
□	11	*.CN=eurus.O=novell.T=DIGITALAIRLINES.	0	1	Sat, Aug 01 2015 06:47:29 pm
□	12	NOT LOGGED IN	0	1	Not Available
□	14	NOT LOGGED IN	0	1	Not Available
□	15	NOT LOGGED IN	0	1	Not Available
□	16	*.CN=eurusadmin.O=novell.T=DIGITALAIRLINES.	0	1	Thu, Jul 30 2015 06:36:40 am
□	17	*.CN=OESCommonProxy_eurus.O=novell.T=DIGITALAIRLINES.	0	1	Tue, Jul 28 2015 11:59:10 am
□	18	*.CN=OESCommonProxy_eurus.O=novell.T=DIGITALAIRLINES.	0	1	Tue, Jul 28 2015 11:59:10 am
□	19	NOT LOGGED IN	0	1	Not Available
□	20	NOT LOGGED IN	0	1	Not Available

2 (Optional) Sort the **Connection Listing** by clicking the **Sort** icon ▼ in the column heading of the information of interest.

The default sort order is by stations. The current sort order is indicated by the **Sorted By** icon ▼ in the column heading. The **Login Time** heading sorts from the least recent to the most recent.

3 (Optional) Click the **Name** link for a specific connection to view more details about it.



Connection Information

Local Admin

[Back to Connections]

Clear Connection

Connection Information	
Connection	0
Login Status	Normal Authenticated
Authentication Method	NDS
Login time	Tue, Jul 28 2015 11:57:26 am
Privileges	Supervisor & Console Operator
Connection Type	Internal
NCP Requests	0
Bytes Read	0
Bytes Written	0
Network Address	Unknown Address Type
Send Message	
Open Files	
Security Equivalence	.CN=eurus.O=novell.T=DIGITALAIRLINES.

9.4.2 Using NCPCON to View Connections

1 Open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, enter the following to open the NCP Server Console (`ncpcon(8)`) utility:

```
ncpcon
```

3 At the NCPCON prompt, do any of the following:

- Get the Connection Information report by entering

  ```
  connection
  ```

- Get the Connection Listing report by entering

  ```
  connection list
  ```

- Get the Detailed Connection Information report for a specific connection by entering

```
connection connection_number
```

Replace *connection_number* with the station number of the connection of interest. You can find the connection number by viewing the connection listing.

9.5 Sorting Entries in the Connection Listing

In the Connection Listing report on the Connection Manager page, you can sort the connection information by any of the column headings:

1. In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the **Connection Manager** page.
2. Scroll down to view the Connection Listing report.
3. Sort the entries in the Connection Listing report by clicking the **Sort** icon ▾ in the column heading of interest.
   - **Station** (default; ascending order, with Connection 0 first)
   - **Name** (alphabetical order)
   - **Reads and Writes** (descending order, largest volume of traffic first)
   - **NCP Requests** (descending order, highest number of requests first)
   - **Login Time** (reverse chronological order, longest duration first)

   When the page refreshes, the list is sorted in order by the connection information, and the **Sorted By** icon ▤ appears in its column heading.

9.6 Clearing Not-Logged-In Connections to NCP Server

If users cannot connect to the server, all the licensed user connections might be in use. You can view and clear the connections of users with active connections that are not logged in to the server.

To clear connections to the NCP Server for users that are not logged in:

1. In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the Connection Manager page.
2. In the **Connection Listing**, click the **Sort** icon ▾ for the **Name** column so that all **Not Logged In** connections are grouped together.
3. Review the **Not Logged In** connections to determine which ones you want to clear.
4. (Optional) Click the **Name** link for a specific connection to view more details about it.
5. Do one of the following:
   - **Clear All Not Logged in Connections:** Under **Connection Information**, click the **Clear All "Not Logged In" Connections** link.
   - **Clear One or Multiple Not Logged In Connections:** Under **Connection Listing**, select the check box next to the specific **Not Logged In** connections you want to clear, then click **Clear ALL Marked Connections**.

9.7 Auditing Closed User Connections and Deleted eDirectory User Entries

NCP engine logs the connection details when a user logs out gracefully or when it could not find the user entry in eDirectory for the connection. It may happen that a user entry was deleted by the administrator when a user has already logged in to the NCP server.

Security watchdog helps to keep the user connection alive by periodically checking it. If the user connection is unresponsive or unreachable, security watchdog performs either of the following operations:

- Schedules the connection for termination
- Aborts the connection
- Terminates the connection forcefully

watchdog and NCP engine log user details in XML format at `/var/opt/novell/log/ncpserv.audit.log` and in plain text format at `/var/opt/novell/log/ncpserv.log`.

The log details include:

- Timestamp
- Name of the user with eDirectory tree name
- Station number
- Termination method
- Description

NOTE: Novell Client for windows maintains two separate connection for a user who logs in. One of those connections is used to monitor user connection. Hence, while closing or aborting a user connection, the log may print details for each connection.

Sample Logs

Graceful logout - XML

```
<libncpengine name="NCPConnection" timestamp="Tue 19 May 2015 02:47:41 PM IST PM
IST" errno="0">
<Station_User type="string">.CN=testuser.O=novell.T=TESTTREE.</Station_User>
<Station_Number type="int">16</Station_Number>
<Termination_method type="string">Logout</Termination_method>
<description type="string">User Logged Out Gracefully</description>
</libncpengine>
```

Graceful logout - Text

```
[i 2015-05-19 14:47:41] User ".CN=testuser.O=novell.T=TESTTREE." from Station 16
Time Stamp "Tue May 19 14:47:41 2015 pm" Disconnected
```

User Entry Deleted - XML

```
<libncpengine name="NCPConnection" timestamp="Tue 19 May 2015 02:51:33 PM IST PM
IST" errno="0">
<Station_User type="string">.testuser.novell.TESTTREE.</Station_User>
<Station_Number type="int">4</Station_Number>
<Termination_method type="string">Deleted</Termination_method>
<description type="string">User Details Deleted</description>
</libncpengine>
```

```
<libncpengine name="NCPConnection" timestamp="Tue 19 May 2015 02:51:33 PM IST PM
IST" errno="0">
<Station_User type="string">.testuser.novell.TESTTREE.</Station_User>
<Station_Number type="int">17</Station_Number>
<Termination_method type="string">Deleted</Termination_method>
<description type="string">User Details Deleted</description>
</libncpengine>
```

User Entry Deleted - Text

```
[i 2015-05-19 14:51:33] User ".testuser.novell.TESTTREE." from Station 4 Time Stamp
"Tue May 19 14:51:33 2015 pm" Deleted
```

```
[i 2015-05-19 14:51:33] User ".testuser.novell.TESTTREE." from Station 17 Time
Stamp "Tue May 19 14:51:33 2015 pm" Deleted
```

Connection Aborted - XML

```
<libncpengine name="NCPConnection" timestamp="Tue 19 May 2015 02:57:33 PM IST PM
IST" errno="0">
<Station_User type="string">.CN=testuser.O=novell.T=TESTTREE.</Station_User>
<Station_Number type="int">16</Station_Number>
<Termination_method type="string">Connection aborted</Termination_method>
<description type="string">Connection is aborted by security watchdog.</
description>
</libncpengine>
```

Connection Aborted - Text

```
[i 2015-05-19 14:57:33] User ".CN=admin.O=novell.T=M77-EDIR888-MANISH-TREE." at
station 16 Time Stamp "Tue May 19 14:57:33 2015 pm" Connection aborted
```

Connection Terminated - XML

```
<libncpengine name="NCPConnection" timestamp="Tue 19 May 2015 02:57:33 PM IST PM
IST" errno="0">
<Station_User type="string">.CN=testuser.O=novell.T=TESTTREE.</Station_User>
<Station_Number type="int">16</Station_Number>
<Termination_method type="string">Force Termination</Termination_method>
<description type="string">User did not logout within 5 minutes after security
watch dog notice</description>
</libncpengine>
```

Connection Terminated - Text

```
[i 2015-05-19 14:57:33] User did not logout within 5 minutes after security watch
dog notice
[i 2015-05-19 14:57:33] User ".CN=testuser.O=novell.T=TESTTREE." at station 16 Time
Stamp "Tue May 19 14:57:33 2015 pm" Terminated
```

Connection Scheduled for Termination - XML

```
<libncpengine name="NCPConnection" timestamp="Tue 19 May 2015 02:57:33 PM IST PM
IST" errno="0">
<Station_User type="string">.CN=testuser.O=novell.T=TESTTREE.</Station_User>
<Station_Number type="int">16</Station_Number>
<Termination_method type="string">Scheduled for Termination</Termination_method>
<description type="string">User connection is Scheduled for Termination</
description>
</libncpengine>
```

Connection Scheduled for Termination - Text

```
[i 2015-05-19 14:57:33] User ".CN=testuser.O=novell.T=TESTTREE." at station 16 Time
Stamp "Tue May 19 14:57:33 2015 pm" Scheduled for Termination
```

9.8 Clearing Connections to NCP Server

You might need to clear connections for one or multiple users. For example, if a user’s workstation quits working, it usually leaves its connection to the server open and might also leave files open. You can clear the user’s connection to allow the open files to close.

- Section 9.8.1, “Using Novell Remote Manager to Clear NCP Connections,” on page 79
- Section 9.8.2, “Using NCPCON to Clear NCP Connections,” on page 79

9.8.1 Using Novell Remote Manager to Clear NCP Connections

1. In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the **Connections Manager** page.
2. Scroll down to view the connections in the Connection Listing report.
3. (Optional) Sort the list by clicking the **Sort** icon ▾ in the column heading of interest.
4. Review the connections to determine which ones you want to clear.
5. (Optional) Click the **Name** link for a specific connection to view more details about it. From this page, you can click the **Clear Connection** link, or click **Back to Connections** to return to the Connection Manager page.
6. Select the check box next to each specific connection that you want to clear.
7. Click **Clear ALL Marked Connections**.

9.8.2 Using NCPCON to Clear NCP Connections

1. Open a terminal console, then log in as the `root` user.
2. At the terminal console prompt, enter the following to open the NCP Server Console (`ncpcon(8)`) utility:

   ```
   ncpcon
   ```
3. Get the Connection Listing report by entering

   ```
   connection list
   ```
4. Review the list to locate the connection number of the connection you want to clear.
5. (Optional) Get the details connection information for a specific connection by entering

   ```
   connection connection_number
   ```

6 Clear the connection by entering

```
connection clear connection_number
```

7 Clear all connections by entering

```
connections clearALL
```

9.9 Finding the Connection for an Open File

Sometimes you know the filename of the file you want to close, and you need to find the connection associated with the file.

1 Open a terminal console, then log in as the `root` user.

2 At the console prompt, enter the following command to get a list of NCP connections for a given file:

```
ncpcon files list f=filename
```

Replace *filename* with the Linux path for the file, including the filename, such as `/usr/novell/sys/text.txt`. For example:

```
ncpcon files list f=/usr/novell/sys/test.txt
```

9.10 Viewing Open Files for an NCP Server Connection, and Closing All Open Files

Before clearing a connection and closing all of its open files, you might want to get an idea of the types of files that the user or operation is accessing. For example, you might want more information about the connection if the connection has been open a long time, or it has a large volume of traffic associated with it.

1 In Novell Remote Manager, click **Manage NCP Services > Manage Connections** to open the **Connections Manager** page.

2 Scroll down to view the connections in the **Connection Listing** report.

3 (Optional) Sort the list by clicking the Sort icon ▾ in the column heading of interest.

4 Click the **Name** link for a specific connection to view its details.

5 Scroll down to view the **Open Files** section for a list of files currently opened by the selected connection.

The application that is used to open a file determines whether the file is held open and locked for access to other users. Some applications open the file and copy the information to a working file, and overwrite the original when you save changes. These open files do not appear in the Open Files list. Other applications create a temporary file for changes and lock the original file for write access to other users. These open files appear in the Open Files list. The temporary file is listed in a file system view, but does not appear as an open file. When you clear the connection, the open files in the list are closed, and the application should automatically close and delete the temporary files.

For example, Microsoft Word creates a system file that begins with `~$`, such as `~$myfile8.doc`. OpenOffice and LibreOffice create a hidden file that begins with .~lock, such as `.~lock.myfile10.odt`. You can view the temporary files by selecting **Manage Shares**, then navigating the NCP volume or NSS volume to the folder where the open file is stored.

6. (Optional) If the connection has been opened by a user, you can send a brief message before clearing the connection. Type the message in the **Send Message** field, then click **Send**.

   Broadcast messages work only for users that are using a Novell Client that supports broadcast messages, and the broadcast message option is enabled.

7. (Optional) Clear the connection and close all open files by clicking **Clear Connection** link at the top of the report.

9.11 Viewing Open Files for an NCP Server Connection, and Closing a Specific Open File

You might want to close a specific open file for the following reasons:

- A file in a shared storage has been held open for a very long time. The application that is being used (such as Microsoft Word or OpenOffice) has locked the file for write access to other users.
- You know which user has the file open, and the user is not available to close the file, or cannot close the file.
- The user has multiple files open.
- You want to close only one of the files.

To use NCPCON to view the list of open files for a connection, then close a specific open file:

1. Open a terminal console, then log in as the `root` user.
2. At the console prompt, enter the following command to get a list of NCP connections for a given file:

   ```
   ncpcon files list f=filename
   ```

   Replace *filename* with the Linux path for the file, including the filename, such as `/media/nss/VOL1/Document.rtf`.

   For example, the following response shows that the admin user in connection 15 has a lock held open on the file:

   ```
   # ncpcon files list f=/media/nss/VOL1/Document.rtf

   ... Executing " files list f=/media/nss/VOL1/Document.rtf"

   Connection  User Name            Rights
   15      .CN=admin.O=novell.T=SUMMER. 0x9

   Count of locks found on the file /media/nss/VOL1/Document.rtf: 1.

   ... completed OK [elapsed time = 1 Second 4294051 msecs 640 usecs]
   ```

3. Visually confirm that you have the correct file and connection.
4. Enter the following command to close the open file by filename:

   ```
   ncpcon files close f=filename
   ```

   For example:

   ```
   ncpcon files close f=/media/nss/VOL1/Document.rtf
   ```

   You can alternatively specify the connection number to close all open files for that connection, including the filename of interest.

```
ncpcon files close c=connection_number
```

For example:

```
ncpcon files close c=15
```

5 Verify that any temporary file that the application opened for the file has been removed from the folder by the application. Otherwise, the user might not be able to save changes to the file of interest.

5a In Novell Remote Manager, select **Managing NCP Services > Manage Shares**.

5b Click the volume's name link, then navigate the directory structure to the folder where the open file was located.

5c Use the `Search` feature to find a temporary file for the open file, such as `~$myfile.doc` or `.~lock.myfile.odt`.

5d Click the **File Information** icon next to the file name.

5e On the File Information page, click **Delete File**.

For more information about temporary files created by an application, see Step 5 in Section 9.10, "Viewing Open Files for an NCP Server Connection, and Closing All Open Files," on page 80.

10 Managing NCP Volumes

This section describes how to create and manage NCP volumes on an Open Enterprise Server (OES) 2015 SP1 server.

10.1 Understanding NCP Volumes

NCP volumes are NCP shares on Linux POSIX file systems such as Ext3, XFS, and Reiser. Novell Storage Services (NSS) volumes are a special type of NCP volume.

The directory and file access is controlled with the NetWare trustee model for file system trustees and trustee rights. Users access data on NCP volumes by using the Novell Client software on their Windows, Vista, or Linux workstations. This document refers collectively to those workstations as "Novell clients".

To give eDirectory users access to the files via Samba, you can Linux-enable users with Linux User Management. NCP authenticates users and enforces the trustee settings. For information about Linux-enabling users with Linux User Management, see the *OES 2015 SP1: Linux User Management Administration Guide*.

10.1.1 NCP Shares as NCP Volumes

You create NCP shares by specifying mount points on any Linux POSIX file system by using the NCP Server Console (NCPCON, `ncpcon(8)`) utility or Novell Remote Manager for Linux.

When NCP Server is installed, an NCP volume named SYS is automatically created and mounted. Its NCP share mount point is `/usr/novell/sys`. This NCP volume contains the same `login` and `public` directories that exist on NetWare. These directories let Novell clients run commands for logging in, mapping drives, and so on, as well as the means for client commands to be run from login scripts.

Creating an NCP volume for Linux POSIX file systems adds the NCP volume mount information to `/etc/opt/novell/ncpserv.conf` and creates a Volume object in NetIQ eDirectory. Volume names can be up to 14 alphanumeric characters. Underscores are allowed.

If the server is in a Novell Distributed File Services management context, you must run VLDB repair to create a DFS GUID (globally unique ID) to add as an attribute of the Volume object, and to add the volume information to the VLDB database. For information about using DFS junctions for NSS volumes, see the *OES 2015 SP1: Novell Distributed File Services Administration Guide for Linux*.

10.1.2 NSS Volumes as NCP Volumes

By default, NSS volumes created with NSS management tools are NCP volumes. You create and manage NSS volumes by using the NSS Management Utility (NSSMU) or the Storage plug-in for Novell iManager, just as you do on NetWare.

In order to create an NSS volume on your OES 2015 SP1 server, you must install the Novell Storage Services component of OES 2015 SP1 Services.

IMPORTANT: For information about creating and managing NSS volumes on Linux, see “Managing NSS Volumes” in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

Novell clients can access NSS files on a Linux server if the following requirements are met:

- NCP Server is installed and running on the server.
- The administrator user has created NSS pools and volumes with NSSMU or the Storage plug-in to iManager.
- The administrator, or a user with sufficient file system rights, has made the appropriate volume, directory, and file trustee assignments for users of the data (that is, for non-administrator users).

NOTE: The DOS namespace is not supported on the NCP volumes. If the namespace is changed to DOS, NCP volumes might not be mounted and might not be accessible from the clients.

If the server is in a Novell Distributed File Services management context, a DFS GUID is automatically created when you create an NSS volume with NSSMU or iManager. Its DFS GUID is added as an attribute of the volume’s Volume object in eDirectory, and an entry is added to the VLDB. For information about using DFS junctions for NSS volumes, see the *OES 2015 SP1: Novell Distributed File Services Administration Guide for Linux*.

10.1.3 Understanding Time Stamps on Linux

In NCPCON and in the Novell Remote Manager for Linux, you can make your selection based on three time stamps:

- **Last Time Modified:** Time of the last data modification for the selected file.
- **Last Time Accessed:** Time of the last access.
- **Last Time Changed:** Time of the last file status change.

These time stamps are defined by POSIX and supported by Linux. Many operations change more than one time stamp. The change time is controlled automatically. NCP can modify the access time and the modify time, but cannot control whether the change time is reset. For example, if you copy a file from one location to another, NCP can preserve the access and modify times, but the change time is reset because the file’s path changed. That is, it had a status change but the file was not opened for access and its data was not modified.

10.2 Creating NCP Volumes on Linux File Systems

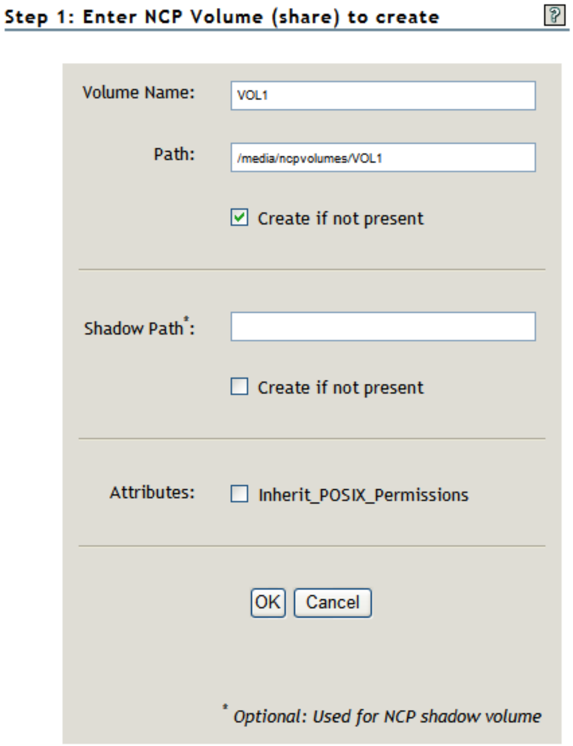
Creating an NCP share on a Linux POSIX file system creates an NCP volume name and associates it to a path for its mount point. You must create one or multiple NCP volumes in order to make Linux POSIX file system files and directories on an OES 2015 SP1 server accessible to workstations running Novell Client software. Novell clients can then access files and folders on that NCP volume just like they do on NetWare.

IMPORTANT: The procedures in this section apply only to NCP shares on Linux POSIX file systems, not NSS volumes. For information about creating and managing NSS volumes on Linux, see "Managing NSS Volumes" in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

- Section 10.2.1, "Using Novell Remote Manager to Create an NCP Volume on a Linux File System," on page 85
- Section 10.2.2, "Using NCPCON to Create an NCP Volume," on page 86
- Section 10.2.3, "Using NSSMU to Create an NCP Volume on a Linux File System," on page 87

10.2.1 Using Novell Remote Manager to Create an NCP Volume on a Linux File System

1 In Novell Remote Manager, click **Manage NCP Services > Manage Shares**, then click **Create New Share**.



Step 1: Enter NCP Volume (share) to create

Volume Name: VOL1

Path: /media/ncpvolumes/VOL1

☑ Create if not present

Shadow Path*:

□ Create if not present

Attributes: □ Inherit_POSIX_Permissions

* Optional: Used for NCP shadow volume

2 In **Volume Name**, type the name of the NCP volume you want to create, such as `VOL1`.

The share name you specify is the volume name NCP clients will see. It is associated to a path on your Linux server. Names can be up to 14 alphanumeric characters. Underscores are allowed.

3 In **Path**, specify the path on a Linux POSIX file system (Ext3, XFS, or Reiser) to the NCP share name, then select **Create If Not Present** check box beneath it if the directory in the path does not already exist.

For example, type `/media/ncpvolumes/VOL1` as the share path.

IMPORTANT: You should not create an NCP share on NSS file systems. NSS volumes are by default NCP shares.

---

4 The **Shadow Path** indicates the secondary storage location meant for DST operations.

Selecting the Create if not **Present** option creates the path, if it is not already available.

5 (Optional) Enable or disable the **Inherit POSIX Permissions** option by selecting or deselecting the check box.

The **Inherit POSIX Permissions** option is disabled (deselected) by default. This setting applies only for the specified NCP volume on Linux POSIX file systems (that is, for Ext3, XFS, or Reiser file systems, and not for NSS).

IMPORTANT: We recommend that the **Inherit POSIX Permissions** option be disabled (deselected). For information about the security implications of enabling this option, see Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,” on page 91.

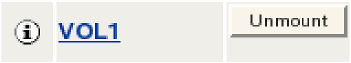
---

6 Click **OK** to confirm the creation of the NCP volume (share).

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

7 Verify that the share was created successfully by clicking **Manage NCP Services > Manage Shares** to see a list of NCP shares.

The NCP volume should appear in the list, and be mounted. Mounted volumes appear with the name hyperlinked, and an **Unmount** button next to it.



10.2.2 Using NCPCON to Create an NCP Volume

1 Open a terminal console on the Linux server that you want to manage, then log in as the `root` user.

2 Use one of the following methods to create an NCP share on a Linux POSIX volume:

- At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

  ```
  create volume ncp_volume_name path
  ```

- At the terminal console prompt, enter

  ```
  ncpcon create volume ncp_volume_name path
  ```

  For example, if the volume name is `vol1` and the path is `/home/novell`, enter

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

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.

10.2.3 Using NSSMU to Create an NCP Volume on a Linux File System

You can use NSSMU to create a Linux LVM volume group and logical volume on a device, make a file system on the volume, and mount the volume. You must have free unpartitioned space available on a device. The device should not be shareable for clustering.

For more information, see "Creating a Non-LVM Linux Volume" , "Creating an LVM Logical Volume", and "Clustering LVM Volume Groups with Novell Cluster Services" in the *OES 2015 SP1: Linux POSIX Volume Administration Guide*.

10.3 Mounting NCP Volumes

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

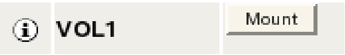
- Section 10.3.1, "Using Novell Remote Manager to Mount an NCP Volume," on page 87
- Section 10.3.2, "Using NCPCON to Mount an NCP Volume," on page 87

10.3.1 Using Novell Remote Manager to Mount an NCP Volume

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

To mount an NCP volume:

1 In Novell Remote Manager, click **Manage NCP Services > Manage Shares**, then click the **Mount** button next to the NCP volume you want to mount.



10.3.2 Using NCPCON to Mount an NCP Volume

1 Open a terminal console on the Linux server that you want to manage, then log in as the `root` user.

2 Use one of the following methods to mount an NCP volume:

   - At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

     ```
     mount ncp_volume_name
     ```

   - At the terminal console prompt, enter

     ```
     ncpcon mount ncp_volume_name
     ```

     For example, if volume `sys` is dismounted, mount it by entering

     ```
     ncpcon mount sys
     ```

   Replace *ncp_volume_name* with the name of the NCP volume you want to mount. Volume names are not case sensitive. You can also replace *ncp_volume_name* with *all* to mount all NCP volumes on the server.

10.4 Dismounting NCP Volumes

Dismounting an NCP volume removes accessibility for Novell clients to the mount point represented by the volume name.

- Section 10.4.1, “Using NCPCON to Dismount an NCP Volume,” on page 88
- Section 10.4.2, “Using Novell Remote Manager to Dismount an NCP Volume,” on page 88

10.4.1 Using NCPCON to Dismount an NCP Volume

1. Open a terminal console on the Linux server that you want to manage, then log in as the `root` user.
2. Use one of the following methods to dismount an NCP volume:
   - At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

     ```
     dismount ncp_volume_name
     ```

   - At a terminal console prompt, enter

     ```
     ncpcon dismount ncp_volume_name
     ```

     For example, if volume `vol1` is mounted, dismount it by entering

     ```
     ncpcon dismount vol1
     ```

   Replace *ncp_volume_name* with the name of the NCP volume you want to dismount. Volume names are not case sensitive.

10.4.2 Using Novell Remote Manager to Dismount an NCP Volume

1. In Novell Remote Manager, click **Manage NCP Services > Manage Shares**, then click the **Unmount** button next to the NCP volume you want to dismount.

10.5 Viewing the Size of an NCP Volume

The amount of space available to an NCP volume depends on the size of the partition where the underlying Linux POSIX file system was created and any additional devices that might be mapped to paths that are under the NCP volume’s share path. Space on the Linux file system is overbooked from the point of view of the NCP shares on it. If you create multiple NCP volumes on the same Linux volume, each NCP volume reports the space available to it as the unused space on the Linux volume.

You can use the Volume Inventory report in Novell Remote Manager for Linux to view the size of the NCP volume and the space available to it. Do not use Linux utilities (such as `df -h`) to determine the size of an NCP volume.

1. Open Novell Remote Manager for Linux for the server you want to manage.
2. Select **View File System**, then select **NCP Volume Inventory**.
3. Click the link of the NCP volume to create a Volume Inventory report for the volume.
4. Under **Key Statistics**, view the **Space in Use** and **Space Available**.

You can also use `ncpcon volumes /s` to view the used and free space details.

10.6 Purging Deleted Files from an NSS Volume

Deleted files might be available for salvage on NSS volumes where the Salvage attribute is enabled. Purging deleted files permanently removes them from the volume. Purged files cannot be salvaged.

- Section 10.6.1, "Using NCPCON to Purge Deleted Files," on page 89
- Section 10.6.2, "Using Management Tools to Purge Deleted Files," on page 89

10.6.1 Using NCPCON to Purge Deleted Files

The `purge volume` command in NCPCON purges deleted files from an NSS volume on Linux. This command works only with NSS volumes.

1. Open a terminal console on the Linux server you want to manage, then log in as the `root` user.
2. Use one of the following methods to purge an NCP volume:
   - At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

     ```
     purge volume ncp_volume_name
     ```

   - At a terminal console prompt, enter

     ```
     ncpcon purge volume ncp_volume_name
     ```

     For example, to purge all deleted files on an NSS volume `vol1`, enter

     ```
     ncpcon purge volume vol1
     ```

   Replace *ncp_volume_name* with the name of the NSS volume where you want to purge all deleted files. Volume names are not case sensitive.

10.6.2 Using Management Tools to Purge Deleted Files

You can purge and salvage (or undelete) NSS files on your Linux server by using the following tools:

- **The Files and Folders role in iManager 2.7.7:** For instructions, see "Salvaging and Purging Deleted Volumes, Directories, and Files" in the *OES 2015 SP1: NSS File System Administration Guide for Linux*.
- **NetStorage:** For instructions, see "Purging and Salvaging Deleted NSS Files" in the *OES 2015 SP1: NetStorage Administration Guide for Linux*.
- **Novell Client:** For information, see "Using the Novell Client" in the *OES 2015 SP1: File Systems Management Guide*.
- **Novell Remote Manager:** For information, see "Salvaging and Purging Deleted Files on an NSS Volume" in the *OES 2015 SP1: Novell Remote Manager Administration Guide*.

10.7 Removing an NCP Volume

Removing an NCP volume deletes the NCP share mount point information (path and volume name association) from the `/etc/opt/novell/ncpserv.conf` file. It also removes the NCP volume's Volume object from NetIQ eDirectory. It does not remove or delete data from the directory represented by the share path. NCP clients cannot see or access the data after it is no longer defined as an NCP volume.

IMPORTANT: If the NCP volume is in a Novell Distributed File Services management context, removing the NCP volume's Volume object breaks junctions that point to that NCP volume. If you create an NCP volume by the same name for the same share, the junctions are still broken because the DFS GUID is different. You must delete and re-create the junctions that point to the new NCP volume.

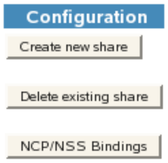
After an NCP volume has been removed, if you need to restore the mount point, you must create a new NCP volume for the share as you did when you first created it.

- Section 10.7.1, "Using Novell Remote Manager to Remove an NCP Volume," on page 90
- Section 10.7.2, "Using NCPCON to Remove an NCP Volume," on page 90

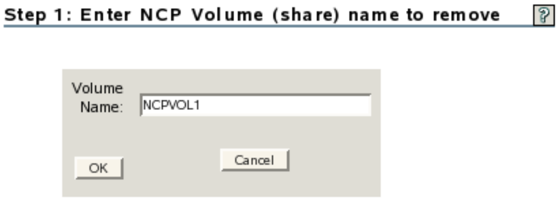
10.7.1 Using Novell Remote Manager to Remove an NCP Volume

1 In Novell Remote Manager, click **Manage NCP Services > Manage Shares**.

2 In the **Configuration** area, click **Delete Existing Share**.



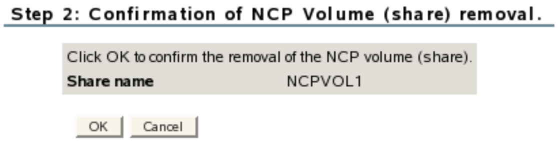
3 Specify the name of the NCP volume you want to remove, then click **OK**.



Step 1: Enter NCP Volume (share) name to remove

Volume Name: NCPVOL1

4 Verify the information, then click **OK** to confirm the volume removal.



Step 2: Confirmation of NCP Volume (share) removal.

Click OK to confirm the removal of the NCP volume (share).

Share name NCPVOL1

5 When the NCP share has been removed successfully, click **Done** to return to the Manage Shares page.

10.7.2 Using NCPCON to Remove an NCP Volume

Before removing a volume, best practice is to dimount the volume to gracefully terminate connections to the data.

1 Open a terminal console on the Linux server you want to manage, then log in as the `root` user.

2 Use one of the following methods to remove an NCP volume:

- At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

```
remove volume ncp_volume_name
```

- At a terminal console prompt, enter

  ```
  ncpcon remove volume ncp_volume_name
  ```

  For example, to remove volume `vol1`, enter

  ```
  ncpcon remove volume vol1
  ```

Replace *ncp_volume_name* with the name of the NCP volume that you want to remove. Volume names are not case sensitive.

10.8 Configuring Inherit POSIX Permissions for an NCP Volume

For NCP volumes on Linux, the ability to inherit POSIX permissions (Group ID and mode bits) from a parent directory is disabled by default. This ensures that local access to data (that is, local access in the Linux environment, not via NetIQ eDirectory) is available only to the `root` user. Only authorized eDirectory users can access the data. As with NetWare volumes, NCP Server controls access to data by using the Novell trustee model of file system trustees and trustee rights.

If the **Inherit POSIX Permissions option** is enabled, it allows the POSIX permissions (GID and mode bits) to be inherited from the parent directory. This lets shared areas be more easily created and managed for local Linux users. However, it makes the volume less secure.

IMPORTANT: The disabled setting for the **Inherit POSIX Permissions** option is a more secure management method for NCP volumes.

Inherit POSIX Permissions is disabled by default and is not allowed to be set on an NSS volume. There is an explicit check for this, and if the volume is an NSS volume, an error 22 is returned. NSS has its own handling of POSIX permissions. For information, see Section 6.2.1, “POSIX Permissions on the NSS File System,” on page 49.

Inherit POSIX Permissions is disabled by default on clustered NCP volumes in OES 2 SP1 Linux and earlier releases. You cannot use the methods described in this section to set the Inherit POSIX Permissions option for a clustered NCP volume because it does not have an entry in the `ncpserv.conf` file. The clustered NCP volume is defined in the mount command line in its cluster resource load script and removed in its unload script.

Use any of the following methods to configure the Inherit POSIX Permissions setting for unclustered NCP volumes:

- Section 10.8.1, “Configuring the Inherit POSIX Permissions for a New NCP Volume,” on page 92
- Section 10.8.2, “Configuring the Inherit POSIX Permissions Setting for an Existing NCP Volume,” on page 92
- Section 10.8.3, “Configuring Inherit POSIX Permissions for a Clustered NCP Volume,” on page 94

10.8.1 Configuring the Inherit POSIX Permissions for a New NCP Volume

You can enable or disable the **Inherit POSIX Permissions** option when you create an NCP volume on a Linux POSIX file system in Novell Remote Manager. The option is disabled by default. For information about creating an NCP volume, see Section 10.2.1, "Using Novell Remote Manager to Create an NCP Volume on a Linux File System," on page 85.

10.8.2 Configuring the Inherit POSIX Permissions Setting for an Existing NCP Volume

- "Using Novell Remote Manager to Configure Permissions" on page 92
- "Using NCPCON to Configure Permissions" on page 92
- "Using ncpserv.conf to Configure Permissions" on page 93

Using Novell Remote Manager to Configure Permissions

1. In a Web browser, open Novell Remote Manager for Linux for the server you want to manage, then log in as the `root` user.
2. Select **Manage NCP Services > Manage Shares**.
3. On the NCP Shares page, locate the volume's share name in the **Active Shares** area.
4. If the volume is mounted, click **Unmount** next to its share name.
5. Click the **Information** icon next to the volume's share name.
6. On the Share Information page, click **Attributes**.
7. On the Modify Volume Properties page, enable or disable the **Inherit_POSIX_Permissions** parameter by selecting or deselecting its check box, then click **Update**.
8. On the NCP Shares page, mount the volume by clicking **Mount** next to its share name.

   Novell Remote Manage for Linux automatically restarts the NetIQ eDirectory daemon to make the changed setting take effect.

Using NCPCON to Configure Permissions

1. Open a terminal console, then log in as the `root` user.
2. Start NCPCON by entering the following at the terminal console prompt:

   ```
   ncpcon
   ```

3. Display the current volume settings by entering the following at the NCPCON prompt:

   ```
   change volume ncp_volumename
   ```

   Replace *ncp_volumename* with the name of the NCP volume you want to manage.
4. Dismount the volume by entering the following at the NCPCON prompt:

   ```
   dismount ncp_volumename
   ```

   Replace *ncp_volumename* with the name of the volume you want to manage.
5. Enable or disable the Inherit_POSIX_Permissions (set the parameter to On or Off), by entering one the following commands:

```
change volume ncp_volumename Inherit_POSIX_Permissions on

change volume ncp_volumename Inherit_POSIX_Permissions off
```

6 Mount the volume by entering the following at the NCPCON prompt:

```
mount ncp_volumename
```

7 Display the volume settings again to verify the change you made to the Inherit_POSIX_Permissions setting. At the NCPCON prompt, enter

```
change volume ncp_volumename
```

8 Exit NCPCON by entering

```
exit
```

Using ncpserv.conf to Configure Permissions

You can enable or disable the **Inherit POSIX Permissions** parameter for an existing NCP volume by adding the `Inherit_POSIX_Permissions` flag to the VOLUME definition for that volume in the NCP Server configuration file (`/etc/opt/novell/ncpserv.conf`). Remove the flag from a volume definition to disable it.

1 Dismount the NCP volume where you want to change the setting.

1a Open a terminal console, then log in as the `root` user.

1b At the terminal console prompt, enter

```
ncpcon dismount ncp_volumename
```

Replace *ncp_volumename* with the name of the volume you want to manage.

2 Modify the setting for the volume in the `/etc/opt/novell/ncpserv.conf` file.

2a Open the `/etc/opt/novell/ncpserv.conf` file in text editor.

2b Do one of the following:

- **Enable:** Add the `Inherit_POSIX_Permissions` flag to the end of the VOLUME definition line for the NCP volume where you want to enable it:

  For example:

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

- **Disable:** Remove the `Inherit_POSIX_Permissions` flag from the VOLUME definition line for the NCP volume where you want to disable it. This is the default setting.

  For example:

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

2c Save the file.

The changes do not go into effect until you restart `ndsd`.

3 Restart the NetIQ eDirectory (`ndsd`) daemon to make the changes to `ncpserv.conf` go into effect.

Use the following steps to stop and start `ndsd` when a single instance is running. For information about stopping and starting `ndsd` when you are running multiple instances of it on the same server, see Using Multiple Instances in the NetIQ eDirectory 8.8 SP7 What's New Guide.

3a Use the following commands to stop `ndsd`:

```
rcndsd stop
```

3b Use the following commands to start `ndsd`:

```
rcndsd start
```

4 Mount the NCP volume:

4a Open a terminal console, then log in as the `root` user.

4b At the terminal console prompt, enter

```
ncpcon mount ncp_volumename
```

Replace *ncp_volumename* with the name of the volume that you modified.

10.8.3 Configuring Inherit POSIX Permissions for a Clustered NCP Volume

To set the Inherit POSIX Permissions option for a clustered volume, add `"/OPT=Inherit_POSIX_Permissions`" to the mount command. Place the option before the volume name; otherwise, the mount fails.

The syntax for the mount command line in the cluster load script is:

```
exit_on_error ncpcon mount /OPT=Inherit_POSIX_Permissions
<NCPvolumename>=VOL_ID,PATH=<volumeMountPoint>
```

10.9 Configuring the NCP/NSS Bindings for an NSS Volume

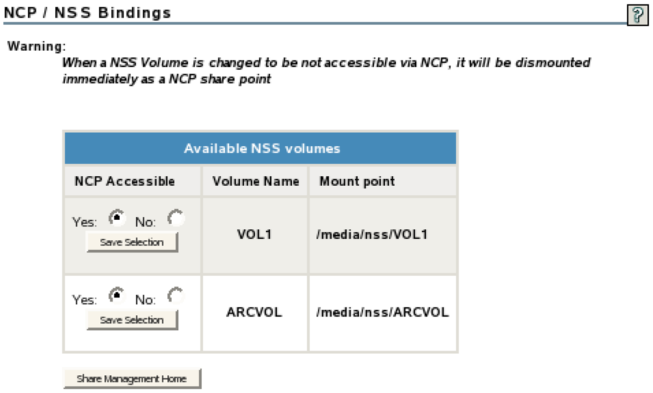
- Section 10.9.1, “Understanding the NCP/NSS Bindings Parameter,” on page 94
- Section 10.9.2, “Enabling the NCP/NSS Bindings for an NSS Volume,” on page 95
- Section 10.9.3, “Disabling the NCP/NSS Bindings for an NSS Volume,” on page 96

10.9.1 Understanding the NCP/NSS Bindings Parameter

NSS volumes are automatically mounted by default on system restart in NSS, then in NCP Server. This is the desired behavior for all independent NSS volumes that are not in shadow volumes, and for NSS volumes that you use as primary storage locations in a DST shadow volumes. When an NSS volume is used as the secondary storage area in a DST shadow volume, you want the NSS volume to be mounted in NSS, but not in NCP Server. This allows DST to control access to the secondary storage area via the primary storage area. Files in the secondary storage area cannot be directly accessed by users.

The NCP/NSS Bindings parameter for an NSS volume governs whether the volume is automatically mounted on system restart in NCP Server. When the parameter is enabled, the NSS volume is automatically mounted for NCP Server. When it is disabled, the NSS volume is not mounted for NCP Server. The NCP/NSS Bindings parameter is enabled by default, making the volume NCP accessible.

In the NCP/NSS Bindings dialog, NSS volumes are enabled by default to be **NCP Accessible**, and have a setting of **Yes**.

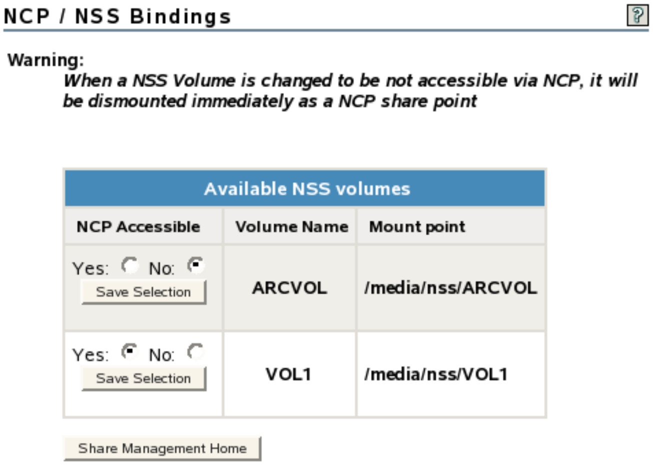


NCP / NSS Bindings

Warning:
When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: ● No: ○	VOL1	/media/nss/VOL1
Yes: ● No: ○	ARCVOL	/media/nss/ARCVOL

For example, if you plan to create a DST shadow volume that uses `VOL1` as the primary storage location and `ARCVOL` as the secondary storage location, set **NCP Accessible** to **Yes** for `VOL1`, and set it to **No** for `ARCVOL`.



NCP / NSS Bindings

Warning:
When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

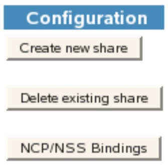
Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: ○ No: ●	ARCVOL	/media/nss/ARCVOL
Yes: ● No: ○	VOL1	/media/nss/VOL1

After you remove a shadow volume, the NCP/NSS Bindings parameter for the NSS volume that was used as the secondary storage area remains disabled until you enable it. You must enable the bindings and mount the volume in order to enable users to access the now independent volume.

10.9.2 Enabling the NCP/NSS Bindings for an NSS Volume

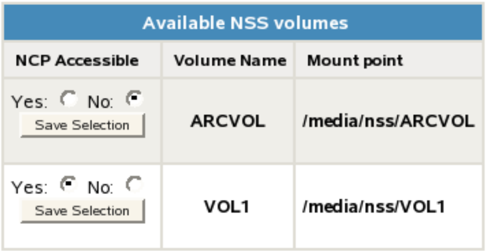
The volume's NCP/NSS Bindings parameter must be enabled for NSS volumes that you use as primary storage locations in a DST shadow volumes, and for all independent NSS volumes that are not in shadow volumes. This is the default.

1 In Novell Remote Manager for Linux, select **Manage NCP Services > Manage Shares**.



2 In the **Configuration** area of the NCP Shares page, click **NCP/NSS Bindings** to open the NCP/NSS Bindings page.

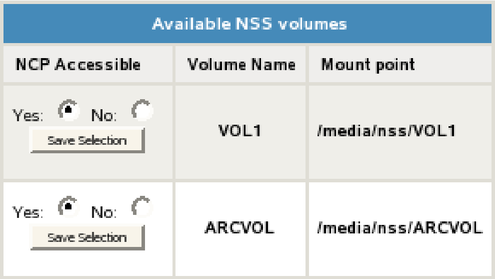
3 In the **Available NSS Volumes** list, locate the NSS volume that you want to enable.



Available NSS volumes

NCP Accessible	Volume Name	Mount point
Yes: ○ No: ● Save Selection	ARCVOL	/media/nss/ARCVOL
Yes: ● No: ○ Save Selection	VOL1	/media/nss/VOL1

4 If the volume’s **NCP Accessible** setting is **No**, click **Yes** to make the NSS volume accessible to NCP so that the volume is automatically mounted in NCP after it is mounted in NSS.



Available NSS volumes

NCP Accessible	Volume Name	Mount point
Yes: ● No: ○ Save Selection	VOL1	/media/nss/VOL1
Yes: ● No: ○ Save Selection	ARCVOL	/media/nss/ARCVOL

5 Beneath the volume’s setting for **NCP Accessible**, click **Save Selection** to save and apply the new setting.

6 Verify that the NSS volume is available for NCP by selecting **Manage NCP Services > Manage Shares** to view a list of active volumes.

If the NSS/NCP bindings are enabled, the NSS volume appears in the **Volume Information** list, and a **Mount** button is displayed next to it.

7 If you want users to be able to access the volume at this time, click **Mount**.

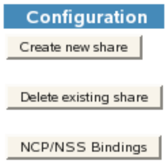
When the volume is successfully mounted, the volume’s name is hyperlinked, and an **Unmount** button is displayed next to it.

10.9.3 Disabling the NCP/NSS Bindings for an NSS Volume

The volume’s NCP/NSS Bindings parameter must be disabled for NSS volumes that you use as secondary storage locations in a DST shadow volumes.

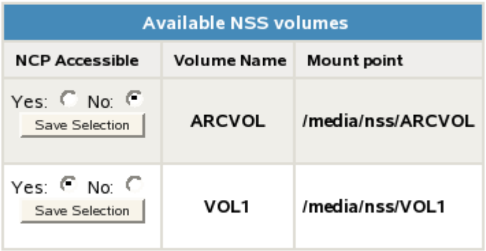
1 In Novell Remote Manager for Linux, select **Manage NCP Services > Manage Shares**.

2 In the **Configuration** area of the NCP Shares page, click **NCP/NSS Bindings**.



3 In the **Available NSS Volumes** list, locate the NSS volume that you want to disable.

4 In the **NCP Accessible** column, click **No** to make the NSS volume not accessible to NCP so that it is not mounted in NCP after it is mounted in NSS.



Available NSS volumes

NCP Accessible	Volume Name	Mount point
Yes: ○ No: ● Save Selection	ARCVOL	/media/nss/ARCVOL
Yes: ● No: ○ Save Selection	VOL1	/media/nss/VOL1

5. Beneath the volume’s setting for **NCP Accessible**, click **Save Selection** to save and apply the new setting.
6. Verify that the NSS volume is not available for NCP by selecting **Manage NCP Services > Manage Shares** to view a list of active volumes.

   If the NCP/NSS bindings were successfully disabled, the NSS volume should not appear in the **Volume Information** list.

10.10 Generating Inventories for Directories or NCP Volumes

You can inventory NCP mounted volumes, or general file system directories or subdirectories as well as view graphs, profiles, reports, and key statistics about each of these items, including space usage trends.

IMPORTANT: To view the graphical displays in the inventory report, Sun Java must be installed on the computer you use to access Novell Remote Manager, and the browser must have Java and JavaScript enabled.

Generating this report can take a while, depending on the number of files and folders in the specified directory path.

With a few clicks, you get available space trend graphs; profiles for file types, file owner, last accessed, last modified, creation time, and file size; and links to specific reports for each of these. You can also customize the scan to look for specific file information.

The **File Owner Profile** gathers the ownership statistics from the NSS management interface. If the eDirectory user name is available from the NSS management interface, the file owner is reported as the eDirectory user name, such as `jsmith`. Otherwise, the owner is reported as the `nobody` user. You do not need to enable the users with Linux User Management (LUM) to get the file owner’s name.

This section includes the following tasks:

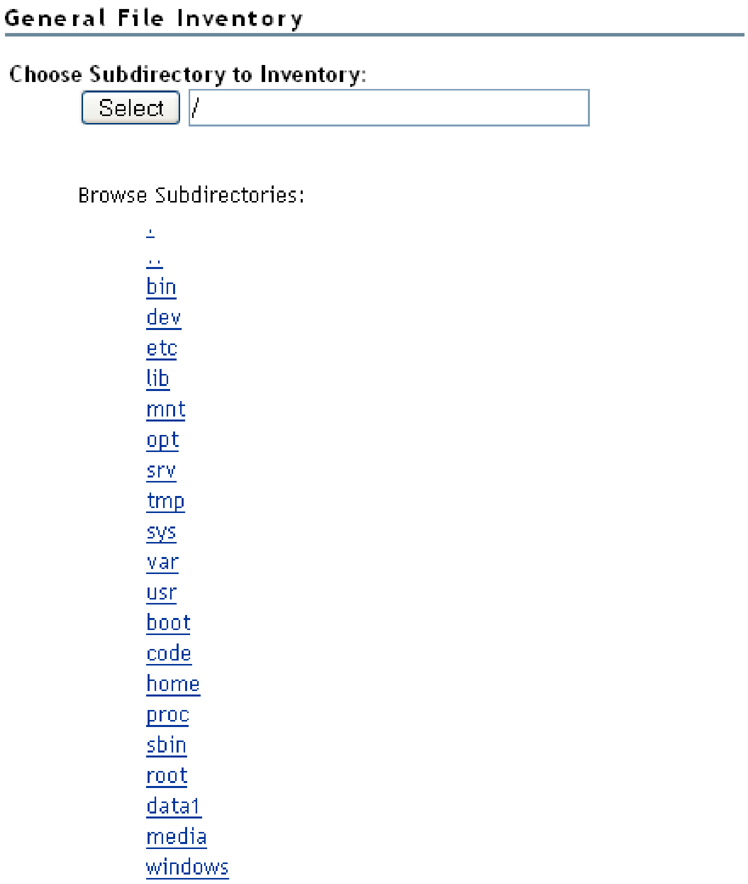
- Section 10.10.1, “Generating a File Inventory Report,” on page 98
- Section 10.10.2, “Generating an NCP Volume Inventory Report,” on page 99
- Section 10.10.3, “Viewing a Saved NCP Volume Report,” on page 101
- Section 10.10.4, “Generating a Customized Report,” on page 101

10.10.1 Generating a File Inventory Report

To generate an inventory report for a the entire server or any subdirectory including mounted NCP volumes:

1 Click **View File System Listing** > **Inventory**.

This opens the General File Inventory page. By default, the / (`root`) directory is selected.



General File Inventory

Choose Subdirectory to Inventory:

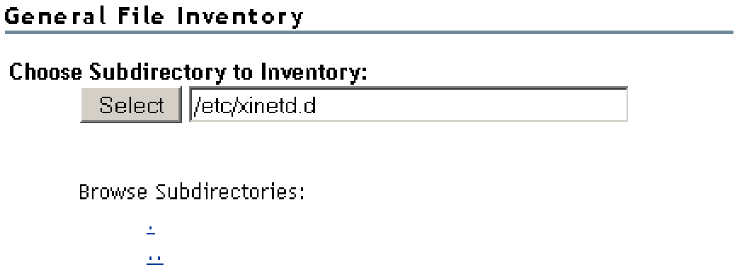
Select /

Browse Subdirectories:

.
..
bin
dev
etc
lib
mnt
opt
srv
tmp
sys
var
usr
boot
code
home
proc
sbin
root
data1
media
windows

2 Do one of the following:

- Click the **Start Scan** button to generate an inventory of the entire server (the default selection is the / [`root`] subdirectory).
- Select a subdirectory to generate a report from by clicking the *subdirectory_name* links until the desired subdirectory appears in the **Scan** field, then click the **Scan** button.



General File Inventory

Choose Subdirectory to Inventory:

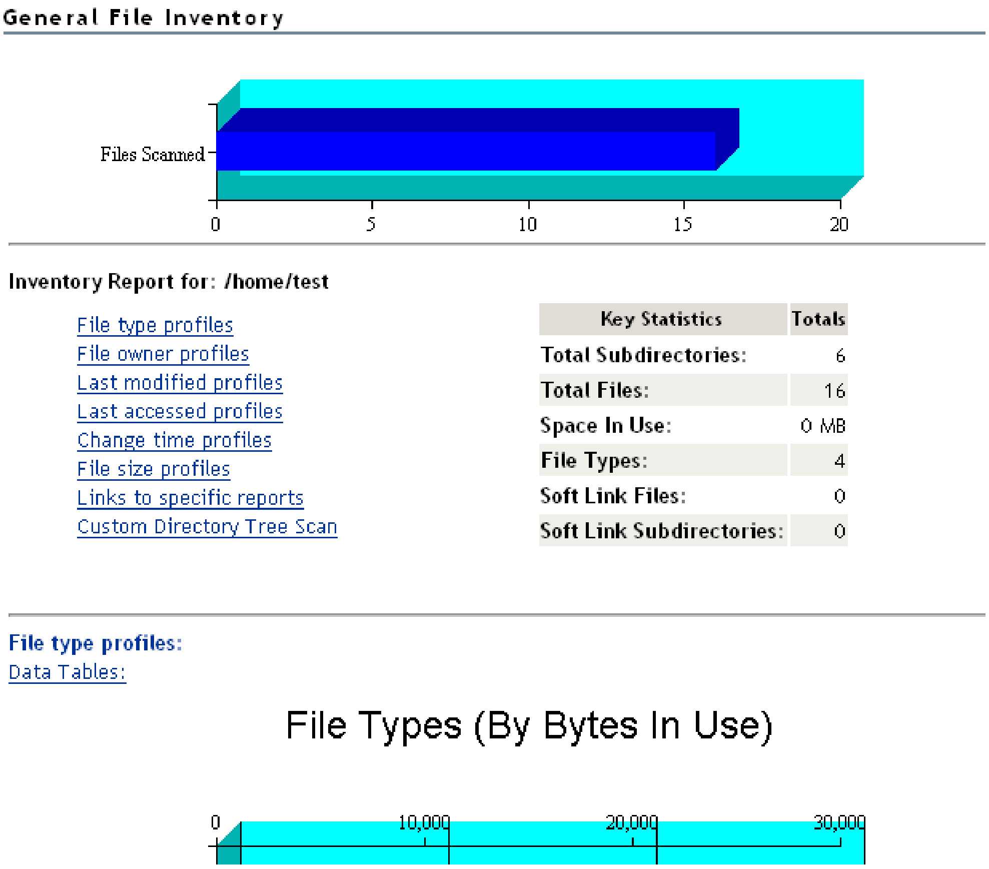
Select /etc/xinetd.d

Browse Subdirectories:

.
..

- If you are viewing the File System Listing page for the desired directory, you can generate the same reports by clicking the **Inventory** link on this page.

A report similar to the following is generated:



General File Inventory

Inventory Report for: /home/test

- File type profiles
- File owner profiles
- Last modified profiles
- Last accessed profiles
- Change time profiles
- File size profiles
- Links to specific reports
- Custom Directory Tree Scan

Key Statistics	Totals
Total Subdirectories:	6
Total Files:	16
Space In Use:	0 MB
File Types:	4
Soft Link Files:	0
Soft Link Subdirectories:	0

File type profiles:

Data Tables:

File Types (By Bytes In Use)

3 Click any of the links to the left of the **Key Statistics** table to move quickly to the generated information.

or

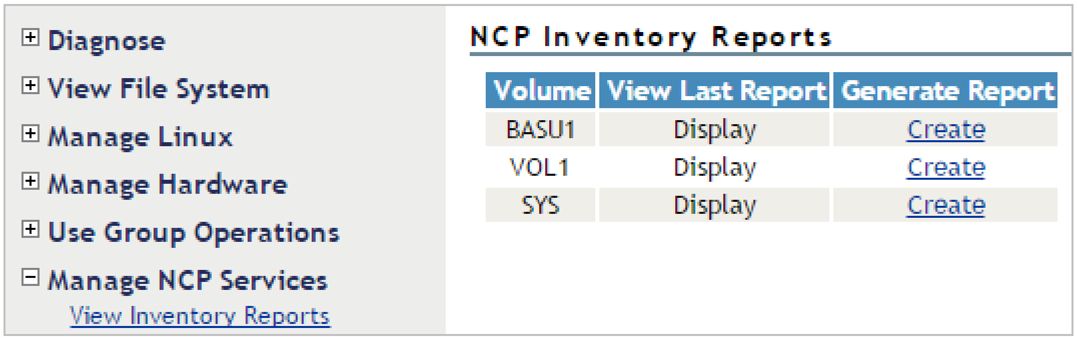
Create a custom report. See "Generating a Customized Report" on page 101.

10.10.2 Generating an NCP Volume Inventory Report

To quickly generate an inventory report for a mounted NCP volume:

1 Use either of the following methods to generate an NCP Volume Inventory Report.

- Select **Manage NCP Services > Volume Inventory Reports**, locate the NSS volume in the list, then click **Create** in the **Generate Report** column for the volume.

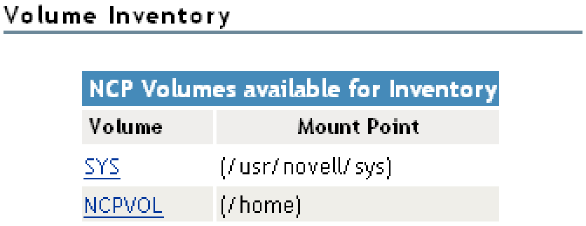


NCP Inventory Reports

Volume	View Last Report	Generate Report
BASU1	Display	Create
VOL1	Display	Create
SYS	Display	Create

- Select **View File System** > **Volume Inventory**, then select the name link of an available NCP volume in the list.

  This opens the Volume Inventory page that shows all mounted volumes available for inventory.

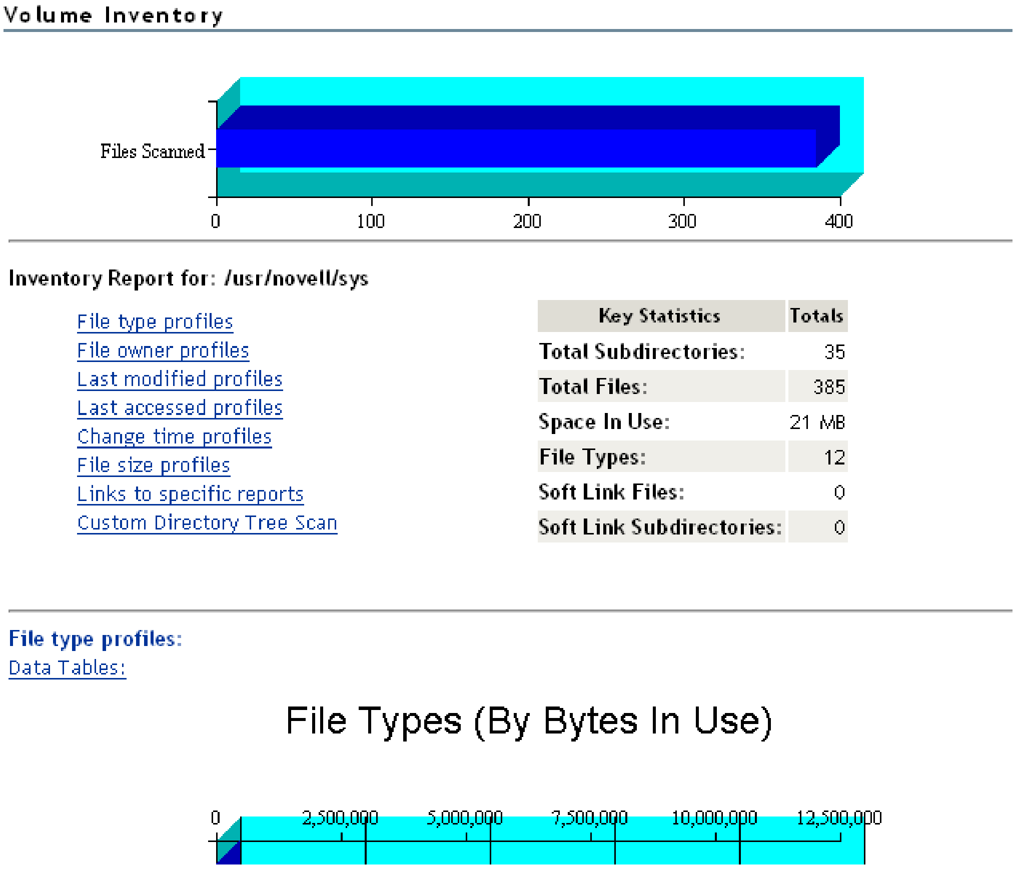


Volume Inventory

NCP Volumes available for Inventory	
Volume	Mount Point
SYS	(/usr/novell/sys)
NCPVOL	(/home)

2 View the generated report.

For example:



Volume Inventory

Inventory Report for: /usr/novell/sys

- File type profiles
- File owner profiles
- Last modified profiles
- Last accessed profiles
- Change time profiles
- File size profiles
- Links to specific reports
- Custom Directory Tree Scan

Key Statistics	Totals
Total Subdirectories:	35
Total Files:	385
Space In Use:	21 MB
File Types:	12
Soft Link Files:	0
Soft Link Subdirectories:	0

File type profiles:

Data Tables:

File Types (By Bytes In Use)

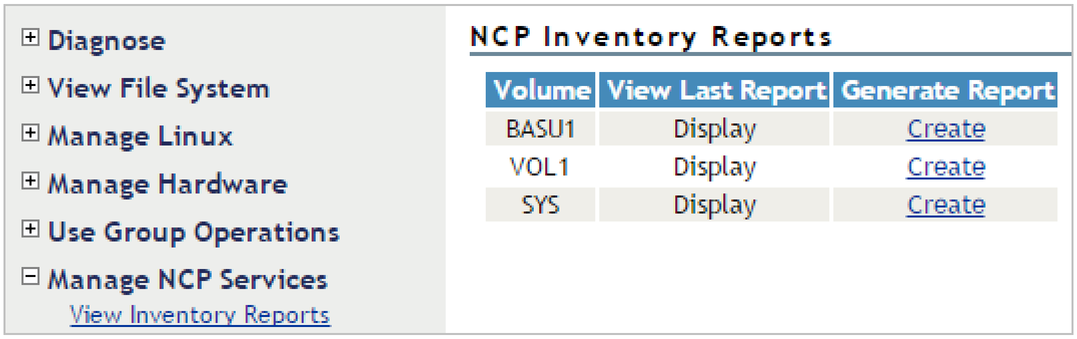
3 Click any of the links to the left of the **Key Statistics** table to move quickly to the generated information.

or

Create a custom report. See "Generating a Customized Report" on page 101.

10.10.3 Viewing a Saved NCP Volume Report

An inventory report is saved when you run an inventory on an NCP volume. You can view the last saved report by going to the **Manage NCP Services > Volume Inventory Reports** page and clicking the **View Last Report > Display** option for the volume. The saved report provides the same statistics as running **View File System > NCP Volumes Inventory**. Graphics are not available in a saved report.



NCP Inventory Reports

Volume	View Last Report	Generate Report
BASU1	Display	Create
VOL1	Display	Create
SYS	Display	Create

10.10.4 Generating a Customized Report

After generating an inventory report for a volume or directory, you can create a customized scan to report more specific information and perform additional actions on the files such as move, copy, or delete files selected in the report.

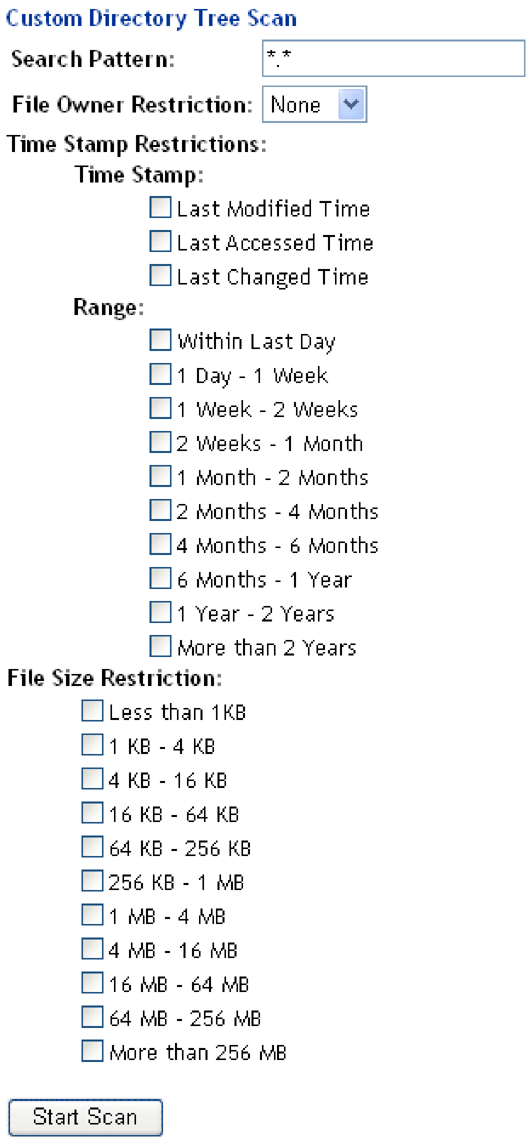
- "Generating the Report" on page 102
- "Performing Actions on Files from Custom Reports" on page 103

Generating the Report

1 Create the initial report as specified in "Generating a File Inventory Report" on page 98.

2 In the generated report, click the **Custom Directory Tree Scan** link.

A page similar to the following is returned.



Custom Directory Tree Scan

Search Pattern: *.*

File Owner Restriction: None

Time Stamp Restrictions:

Time Stamp:

□ Last Modified Time
□ Last Accessed Time
□ Last Changed Time

Range:

□ Within Last Day
□ 1 Day - 1 Week
□ 1 Week - 2 Weeks
□ 2 Weeks - 1 Month
□ 1 Month - 2 Months
□ 2 Months - 4 Months
□ 4 Months - 6 Months
□ 6 Months - 1 Year
□ 1 Year - 2 Years
□ More than 2 Years

File Size Restriction:

□ Less than 1KB
□ 1 KB - 4 KB
□ 4 KB - 16 KB
□ 16 KB - 64 KB
□ 64 KB - 256 KB
□ 256 KB - 1 MB
□ 1 MB - 4 MB
□ 4 MB - 16 MB
□ 16 MB - 64 MB
□ 64 MB - 256 MB
□ More than 256 MB

Start Scan

3 Type the specific search criteria in the **Search Pattern** field.

. is the default entry.

4 Select the desired settings in the **File Owner Restriction** drop-down box.

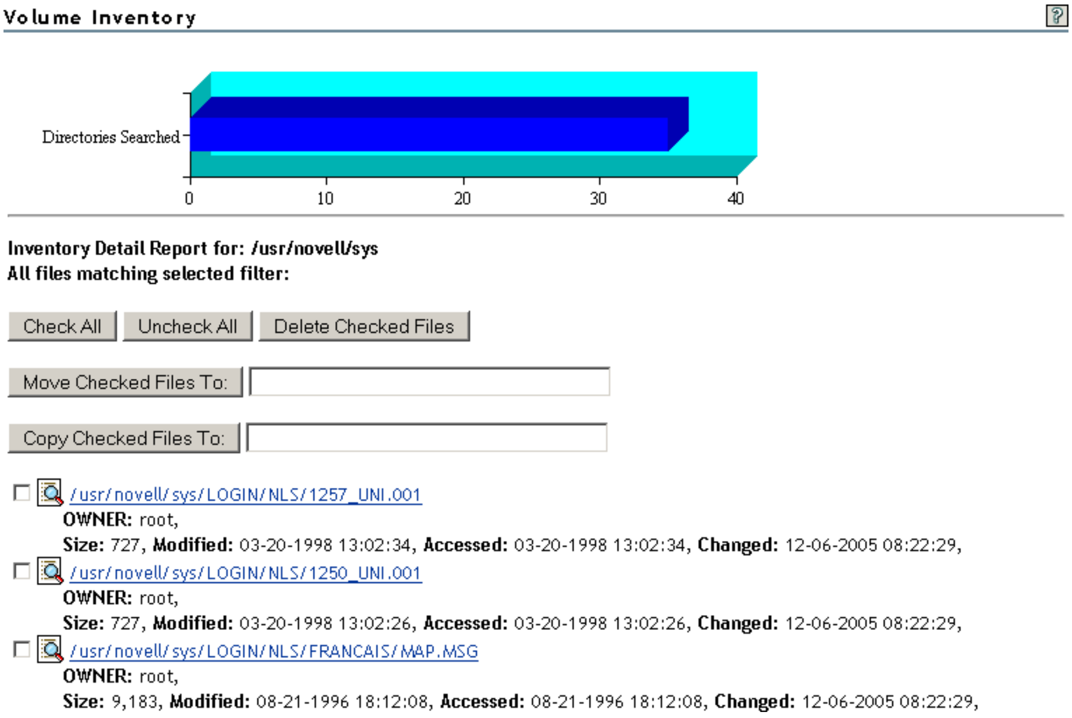
None is the default selection.

5 Select the check boxes to customize the report by **Time Stamp** or **File Size** restrictions.

No restrictions is the default setting.

6 Click **Start Scan**.

A page similar to the following is returned:



Inventory Detail Report for: /usr/novell/sys
All files matching selected filter:

□ /usr/novell/sys/LOGIN/NLS/1257_UNI.001
OWNER: root,
Size: 727, **Modified:** 03-20-1998 13:02:34, **Accessed:** 03-20-1998 13:02:34, **Changed:** 12-06-2005 08:22:29,

□ /usr/novell/sys/LOGIN/NLS/1250_UNI.001
OWNER: root,
Size: 727, **Modified:** 03-20-1998 13:02:26, **Accessed:** 03-20-1998 13:02:26, **Changed:** 12-06-2005 08:22:29,

□ /usr/novell/sys/LOGIN/NLS/FRANCAIS/MAP.MSG
OWNER: root,
Size: 9,183, **Modified:** 08-21-1996 18:12:08, **Accessed:** 08-21-1996 18:12:08, **Changed:** 12-06-2005 08:22:29,

Performing Actions on Files from Custom Reports

After a custom report is generated, you can perform the following actions on the files listed in the report.

- “Moving Selected Files” on page 103
- “Copying Selected Files” on page 103
- “Deleting Selected Files” on page 104
- “Opening or Downloading a File” on page 104
- “Managing Individual Files” on page 104

Moving Selected Files

1. From the generated report, select the check box to the left of each file that you want to move. If you want to move all the files in the list, click the **Check All** button.
2. Specify the path where you want to move the selected files to in the field to the right of the **Move Checked File To** button.
3. Click the **Move Checked File To** button.

Copying Selected Files

1. From the generated report, select the check box to the left of each file that you want to copy. If you want to copy all the files in the list, click the **Check All** button.
2. Specify the path where you want to copy the selected files to in the field to the right of the **Copy Checked File To** button.
3. Click the **Copy Checked File To** button.

Deleting Selected Files

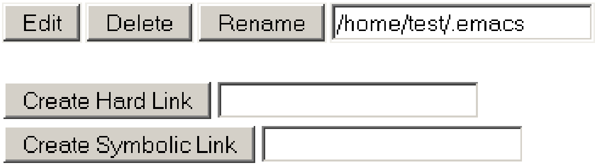
1. From the generated report, select the check box to the left of each file that you want to delete. If you want to delete all the files in the list, click the **Check All** button.
2. Click the **Delete Checked Files** button.

Opening or Downloading a File

1. From the generated report, select the *file_name* link for the file you want to open or download.
2. From the resulting dialog box, select **Open With** or **Save to Disk**, then click **OK**.

Managing Individual Files

1. From the generated report, click the **File Information** icon.
2. Perform the desired actions by entering the required information in the applicable field and clicking the applicable button.



/home/test/.emacs

11 Configuring NCP Volumes with Novell Cluster Services

This section describes how to share NCP volumes in Open Enterprise Server (OES) 2015 SP1 clusters running Novell Cluster Services for Linux.

11.1 Planning for NCP Volumes in a Cluster Environment

Creating NCP volumes on a Linux LVM volume group clustered resource allows your NCP users to access the data by using NCP clients. NCP volumes can be used in a cluster environment with some modifications to the load, unload, and monitor scripts for the Linux LVM volume group cluster resource.

Make sure your system satisfies the “Requirements for Creating LVM Cluster Resources” in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*. The additional prerequisites in this section apply for NCP volumes:

11.1.1 Open Enterprise Server (OES) 2015 SP1

NCP Server for Linux runs only on OES 2015 SP1 servers. For information about installing and configuring OES 2015 SP1, see the “OES 2015 SP1: Installation Guide”.

11.1.2 Novell Cluster Services for Linux

NCP Server for Linux supports Novell Cluster Services for OES 2015 SP1 servers. For information, see “Installing, Configuring, and Repairing Novell Cluster Services” in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

11.1.3 NCP Server and Dynamic Storage Technology

The NCP Server and Dynamic Storage Technology (DST) software is not cluster aware. This OES install option must be selected and installed on every OES 2015 SP1 node in the cluster where you want to fail over shared NCP volumes.

For install information, see Chapter 3, "Installing and Configuring NCP Server for Linux," on page 17.

11.1.4 Shareable Devices

The NCP volume must reside on a shareable device. For more information, see "Shared Disk Configuration Requirements" and "SAN Rules for LUN Masking" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

- You need an unpartitioned disk or LUN that is connected via Fibre Channel or iSCSI protocols to the OES 2015 SP1 server.
- The disk or LUN must be able to be managed by LVM.

11.1.5 LVM Volume Groups

Novell Cluster Services for Linux requires that shared devices be managed by LVM and uses an LVM volume group that is activated exclusively on one node at a time. For information, see "Requirements for Creating LVM Cluster Resources" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

11.1.6 File Systems

In a cluster environment, NCP Server supports NCP volumes on Linux POSIX file systems, including Ext3, XFS, and ReiserFS. For information about requirements and caveats, see "Requirements for Creating LVM Cluster Resources" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

11.1.7 Novell iManager 2.7.7

The Clustering plug-in to iManager 2.7.7 is used to configure cluster resources, load scripts, and unload scripts for the Linux LVM volume group clustered resource. The Directory Administration plug-in is used to create the virtual cluster server object for the NCP volume.

11.1.8 Novell Remote Manager for Linux

The NCP Server plug-in to Novell Remote Manager for Linux is used to configure the NCP volume (or share) on the LVM logical volume on a clustered LVM volume group.

11.2 Clustering an NCP Volume on a Linux POSIX File System

This section describes how to configure a Linux POSIX file system for clustering with Novell Cluster Services for Linux, then how to set up a clustered NCP volume on the cluster resource. You can set up NCP volumes at the root of the cluster resource, or for subdirectories on it. You can create multiple

NCP volumes on a Linux POSIX cluster resource. To provide NCP access to the share, you must create an NCS:NCP Server object and associate it with one or multiple NCP volumes, and bind the object to the IP address of the Linux POSIX cluster resource.

For prerequisites, see Section 11.1, “Planning for NCP Volumes in a Cluster Environment,” on page 105.

IMPORTANT: NCP Server does not support cross-protocol locks across a cluster migration or failover of the resource. If a file is opened with multiple protocols when the migration or failover begins, the file should be closed and reopened after the migration or failover to acquire cross-protocol locks on the new node.

- Section 11.2.1, “Gathering Information for Clustering the NCP Volume,” on page 107
- Section 11.2.2, “Creating and Cluster-Enabling a Linux LVM Volume Group Clustered Resource,” on page 108
- Section 11.2.3, “Creating a Shared NCP Volume on the Linux POSIX Cluster Resource,” on page 109
- Section 11.2.4, “Configuring an LVM Cluster Resource with NSSMU,” on page 111
- Section 11.2.5, “Modifying the Load Script for the LVM Volume Group Cluster Resource,” on page 112
- Section 11.2.6, “Modifying the Unload Script for the LVM Volume Group Cluster Resource,” on page 113
- Section 11.2.7, “Activating the Script Changes,” on page 113

11.2.1 Gathering Information for Clustering the NCP Volume

Gather the information that you will use as you follow the steps to cluster an NCP volume.

IMPORTANT: On Linux, all names are case sensitive in the tools and cluster scripts.

Cluster Information	Example	Description
RESOURCE_IP	10.10.10.44	IP address of the Linux POSIX cluster resource. The cluster resource must have a unique static IP address that is in the same subnet as the IP addresses that are used for the cluster and cluster nodes.
VOLGROUP_NAME	myclustervg01	Name of the LVM volume group. The name must be one word, must consist of standard alphanumeric characters, and must not be any of the following reserved words: Container Disk LVM Plugin Region Segment Volume

Cluster Information	Example	Description
MOUNT_DEV	`/dev/$VOLGROUP_NAME/`*`volume_name`*	The Linux path for the LVM volume. For example: `/dev/$VOLGROUP_NAME/myclustervol01`
MOUNT_FS	ext3	The file system type you specify when you mount the volume.

MOUNT_POINT	`/mnt/lxvol44`	The mount location for the LVM volume. You can mount the LVM volume anywhere. It can have the same or different name than the underlying LVM volume. For example:
		`/mnt/lxvol44`
		`/mnt/users`
		`/home`

NCP_VOLUME	`USERS`	The name you give to the NCP volume. This is the share name seen by the users.
NCP_mount_point	`/path_to_`*`mount_point`*	The NCP share mount point must be the same as that for the LVM volume (that is, at the root of the LVM volume), or it can be a subdirectory below that location.
NCP_SERVER	cluster1-lxvol44-server	The virtual server object (NCS:NCP Server) name for the NCP volume. This example uses a naming convention based on the one used by NSS pool resources (*clustername-poolname*-server), but the Linux POSIX cluster resource name is used instead. *clustername-resourcename*-server
LVM logical volume	mycluster_lxvo44	Name of the LVM logical volume that you create on the volume group.

11.2.2 Creating and Cluster-Enabling a Linux LVM Volume Group Clustered Resource

The following procedure assumes that you are using a disk (or LUN) that does not contain data that you want to keep. You will initialize the disk and remove all segment managers.

WARNING: Initializing a disk destroys all data on it.

1. On the first OES 2015 SP1 node in the cluster, log in as the `root` user, then open a terminal console.
2. In NSSMU, initialize the disk that you want to use. Ensure that the device is not marked as shareable.
3. Create a Linux LVM volume group cluster resource as described in "Requirements for Creating LVM Cluster Resources" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

   Use the sample values that are provided in the Section 11.2.1, "Gathering Information for Clustering the NCP Volume," on page 107 to do the following:

   - Create a clustered Linux LVM volume group.

- Create a an LVM logical volume on the volume group.
- Make a file system on the logical volume.
- Create a cluster resource for the volume group by using the Generic_FS template for Novell Cluster Services.
- Create a Virtual Server object for the cluster resource.

4 Bring the LVM volume group cluster resource online.

5 After you have configured the Linux POSIX cluster resource, continue with Section 11.2.3, "Creating a Shared NCP Volume on the Linux POSIX Cluster Resource," on page 109.

11.2.3 Creating a Shared NCP Volume on the Linux POSIX Cluster Resource

- "Before You Begin" on page 109
- "Creating a Shared NCP Volume" on page 110

Before You Begin

After you create the NCP volume by using the procedure in this section, you must restart the NetIQ eDirectory (ndsd) daemon on this node. Stopping ndsd sends a notification that the server is down to NCP users of the local volumes and existing cluster volumes that are mounted on the server.

Two best practices for clusters should be observed:

- Perform maintenance tasks during non-peak hours so that users are minimally affected.
- When performing maintenance on a node, cluster migrate existing cluster resources to another node if you want the related users to be undisturbed.

If NCP users are connected to local or exiting cluster volumes on the node when you stop `ndsd`, they receive a "`Server is down`" notification from the NCP client.

When you start `ndsd`, NCP users of local volumes on the node are automatically reconnected and their sessions continue.

If you do not cluster migrate the existing cluster resources to another node, when you start `ndsd`, NCP users of existing cluster volumes on the node are not automatically reconnected because their cluster resources are no longer bound to NCP. You can offline the resources and then online the resources, or issue the ncpcon `bind` command for each resource at a terminal console (same as the command used in each of their respective load scripts). After a cluster resource is bound to NCP, its NCP users are automatically reconnected and their sessions continue.

To prevent NCP users from receiving any broadcast messages while you are performing these tasks, you can disable the NCP broadcast message support for the server. For instructions, see Section 9.3.1, "Enabling or Disabling Broadcast Message Support," on page 71.

Creating a Shared NCP Volume

Use the following procedure to create one or more shared NCP volumes on the Linux POSIX cluster resource.

1 On one node in the cluster, create the NCP volume in order to create its Volume object in NetIQ eDirectory. You do not create the NCP volume on every server.

For detailed instructions, see Section 10.2, "Creating NCP Volumes on Linux File Systems," on page 85.

1a In Novell Remote Manager, click **Manage NCP Services > Manage Shares**, then click **Create New Share**.

1b In **Volume Name**, type the name of the NCP volume you want to create, such as `USERS`.

1c In **Path**, specify the Linux path of the cluster-enabled Linux POSIX file system or one of its subdirectories, then select the **Create If Not Present** check box if the subdirectory in the path does not already exist.

For example, if the mount point for the cluster-enabled Linux POSIX file system is `/mnt/lxvol44`, you can create the NCP volume at its root by specifying `/mnt/lxvol44` as the share path, or you can create the NCP volume for a subdirectory on it, such as `/mnt/lxvol44/USERS`.

For the ongoing example, the NCP volume is created at the root of the Linux POSIX cluster resource. The mount point of the LVM volume and the NCP volume is the same, such as `/mnt/lxvol44`.

1d In **Shadow Path**, leave the field blank and do not select the **Create If Not Present** check box beneath it.

IMPORTANT: Dynamic Storage Technology does not support using NCP volumes in shadow volume pairs for OES 2015 SP1. This field is a placeholder for future capabilities.

1e Make sure the **Inherit POSIX Permissions** option is disabled by deselecting the check box.

In OES 2 SP1 Linux and earlier versions, the Inherit POSIX Permissions setting is disabled by default. Enabling the setting here has no effect when you mount the clustered NCP volume in the cluster load script. The setting also cannot be enabled later for clustered NCP volumes as you can for unclustered volumes.

1f Click **OK** to confirm the creation of the NCP volume (share).

This creates the Volume object for the NCP volume on the server, such as `cn=`*`servername`*`_USERS,ou=`*`context`*`,o=`*`mycompany`*. This object is renamed later when you create the virtual NCP server (`NCS:NCP Server`) object.

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

2 Verify that the share was created successfully by clicking **Manage NCP Services > Manage Shares** to see a list of NCP shares.

The NCP volume should appear in the list, and be mounted. Mounted volumes appear with the name hyperlinked, and an **Unmount** button next to it.

3 Dismount the share from the node by clicking **Manage NCP Services > Manage Shares**, then clicking the **Unmount** button next to it.

4 Repeat Step 1 through Step 3 for each NCP volume that you want to create on the Linux POSIX cluster resource.

5 Remove the NCP volume names that you created in the previous steps from the `/etc/opt/novell/ncpserv.conf` file, or comment out the lines.

You want the load and unload scripts for the cluster to control the mounts and dismounts for the NCP volumes. You will modify the cluster scripts later.

If an NCP volume line is present and active in the `ncpserv.conf` file, the node tries to mount the volume on system startup, even if the cluster resources are not loaded on the node. Mounting and dismounting volumes that are on clustered resources should be done in the cluster load and unload scripts, or at the command line after the resource is loaded. The names of the NCP volumes on the cluster resource should not appear in the `ncpserv.conf` file on any of the nodes.

5a On the cluster node where you created the NCP volumes, open a terminal console, then log in as the `root` user.

5b Open the `/etc/opt/novell/ncpserv.conf` file in a text editor.

```
gedit /etc/opt/novell/ncpserv.conf
```

5c Remove or comment out the line. Volume entries look like this:

```
VOLUME volumename /path_to_mount_point
```

For example, change

```
VOLUME USERS /mnt/lxvol44
```

to this:

```
;VOLUME USERS /mnt/lxvol44
```

5d Save your changes and close the file.

6 Restart the NetIQ eDirectory (`ndsd`) daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

7 If NSS is installed on the server, restart the Novell NCP/NSS IPC daemon by entering

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

For information about why this is necessary, see Section 3.5, “Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon,” on page 32.

8 For each of the other nodes in the cluster where you want to mount the shared cluster resource, create the path for the mount points of each of the NCP volumes that you created in Step 1 through Step 4:

8a On a cluster node, open a terminal console as the `root` user.

8b At the terminal console prompt, enter

```
mkdir /path_to_mount_point
```

For example, if the mount point is `/mnt/lxvol44`, enter

```
mkdir /mnt/lxvol44
```

11.2.4 Configuring an LVM Cluster Resource with NSSMU

NSSMU automatically uses the Generic File System template (Generic_FS_Template) to create a volume group cluster resource. After you create the resource, you can add lines to its load script, unload script, and monitor script to customize the resource for other uses. Compare the Generic_FS_Template to the resource template for your product to determine which lines need to be added or modified. For more information, see "Configuring an LVM Volume Group Cluster Resource with NSS Management Tools" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

11.2.5 Modifying the Load Script for the LVM Volume Group Cluster Resource

After you have created the NCP volume and an NCS:NCP Server object, you must modify the load script so that it mounts the NCP volume path as the Linux POSIX cluster resource is brought online. You must also bind the NCS:NCP Server object to the resource. For an example load script, see Section 11.3.1, "Sample Load Script for an NCP Volume Cluster Resource," on page 114.

1. In iManager, select **Clusters > Cluster Options**, then select the cluster.
2. Click the name link of the Linux POSIX cluster resource to open its Cluster Resource Properties page.
3. Click the **Scripts** tab to open the load script.
4. In the definition area, add the following lines to define the NCP volume and the virtual NCP server name:

   ```
   # define NCP volume
   NCP_VOLUME=USERS
   # define NCP server name
   NCP_SERVER=cluster1-lxvol44-server
   ```

   Replace `USERS` with the name of the NCP volume you created. Replace the NCP server name with the name for your virtual NCP server.
5. Above the exit line, add a line to mount the NCP volume:

   ```
   # mount the NCP volume
   exit_on_error ncpcon mount $NCP_VOLUME=VOL_ID,PATH=$MOUNT_POINT
   ```

   The volume ID uniquely identifies the volume and is a value between 0 and 254 (up to 255 volumes per server) that you specify so that the same volume ID is used by the NCP volume on all nodes in the server. Cluster volumes are typically numbered from 254 and downward to avoid conflicts with the automatic volume ID assignments that begin with 0.
6. Under the mount line, add a line to bind the NCP server name to the resource IP address:

   ```
   # bind the NCP volume
   exit_on_error ncpcon bind --ncpservername=$NCP_SERVER --ipaddress=$RESOURCE_IP
   ```

7. Click **Apply** to save your changes.

   The script changes are not active until the next time the cluster resource is taken offline, then brought online. Do not activate the script changes at this time.
8. Continue with Section 11.2.6, "Modifying the Unload Script for the LVM Volume Group Cluster Resource," on page 113.

11.2.6 Modifying the Unload Script for the LVM Volume Group Cluster Resource

After you have created the NCP volume and an NCS:NCP Server object, you must modify the unload script so that it dismounts the NCP volume path as the Linux POSIX cluster resource is brought offline. You must also unbind the NCS:NCP Server object from the resource. For an example unload script, see Section 11.3.2, “Sample Unload Script for an NCP Volume Cluster Resource,” on page 115.

1 In iManager, select **Clusters > Cluster Options**, then select the cluster.

2 Click the name link of the Linux POSIX cluster resource to open its Cluster Resource Properties page.

3 Click the **Scripts** tab, then click **Unload** to open the unload script.

4 In the definition area, add the following lines to define the NCP volume and the virtual NCP server name:

```
# define NCP volume
NCP_VOLUME=USERS
# define NCP server name
NCP_SERVER=cluster1-lxvol44-server
```

Replace `USERS` with the name of the NCP volume you created. Replace the NCP server name with the name for your virtual NCP server. Use the same values for variables that you did in the load script.

5 Under the definition, add a line to unbind the NCP server name from the resource IP address:

```
# unbind the NCP volume
ignore_error ncpcon unbind --ncpservername=$NCP_SERVER --
ipaddress=$RESOURCE_IP
```

6 Under the unbind line, add a line to dismount the NCP volume:

```
# dismount the NCP volume
ignore_error ncpcon dismount $NCP_VOLUME
```

7 Click **Apply** to save your changes.

The script changes are not active until the next time the cluster resource is taken offline, and then brought online.

8 Continue with Section 11.2.7, “Activating the Script Changes,” on page 113.

11.2.7 Activating the Script Changes

The script changes are not active until the next time the cluster resource is taken offline, and then brought online.

1 In iManager, select **Clusters > Cluster Manager**, then select the cluster.

2 Select the check box next to the Linux POSIX cluster resource, then click **Offline**.

Wait until the resource reports an Offline status before continuing.

3 Select the check box next to the Linux POSIX cluster resource, then click **Online**.

Wait until the resource reports an Online status before continuing.

4 Verify that an NCP user can access the volume. On a workstation, use the Novell Client to map a drive to the NCP volume.

11.3 Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume

The settings in the sample scripts in this section are based on the values in the following table. Ensure that you replace the values with the settings from your own configuration.

Variable	Template Value	Your Value
RESOURCE_IP	a.b.c.d	10.10.10.44
MOUNT_FS	reiserfs	ext3
VOLGROUP_NAME	LVM volume group name	myclustervg01
MOUNT_DEV	/dev/VOLGROUP_NAME/volumename	/dev/$VOLGROUP_NAME/ myclustervol01
MOUNT_POINT	/mnt/mount_point	/mnt/myclustervol01
NCP_VOLUME	volume_name	USERS
NCP_SERVER	ncp-server-name	cluster1-lxvol44-server
volume ID	VOL_ID	252

- Section 11.3.1, "Sample Load Script for an NCP Volume Cluster Resource," on page 114
- Section 11.3.2, "Sample Unload Script for an NCP Volume Cluster Resource," on page 115
- Section 11.3.3, "Sample Monitor Script for an NCP Volume Cluster Resource," on page 116

11.3.1 Sample Load Script for an NCP Volume Cluster Resource

You modify the load script for the cluster resource of the Linux POSIX file system by adding the extra lines needed for the NCP volume on it. The settings in the sample script are based on the values in Section 11.3, "Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume," on page 114. Ensure that you replace the values with the settings from your own configuration.

```
#! /bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# define the IP address
RESOURCE_IP=10.10.10.44

# define the file system type
MOUNT_FS=ext3

#define the volume group name
VOLGROUP_NAME=myclustervg01

# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/volume_name

# define the mount point
MOUNT_POINT=/mnt/mount_point

# activate the volume group
exit_on_error vgchange -a ey $VOLGROUP_NAME
```

```
# mount the file system
exit_on_error mount_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

# add the IP address
exit_on_error add_secondary_ipaddress $RESOURCE_IP

# mount the NCP volume
exit_on_error ncpcon mount $NCP_VOLUME=252,PATH=$MOUNT_POINT

# bind the NCP volume
exit_on_error ncpcon bind --ncpservername=$NCP_SERVER --ipaddress=$RESOURCE_IP

exit 0
```

11.3.2 Sample Unload Script for an NCP Volume Cluster Resource

You modify the unload script for the cluster resource of the Linux POSIX file system by adding the extra lines needed for the NCP volume on it. The settings in the sample script are based on the values in Section 11.3, "Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume," on page 114. Ensure that you replace the values with the settings from your own configuration.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# define the IP address
RESOURCE_IP=10.10.10.44

# define the file system type
MOUNT_FS=ext3

# define the volume group name
VOLGROUP_NAME=name

# define the mount point
MOUNT_POINT=/mnt/lxvol44

# define NCP volume
NCP_VOLUME=USERS

# define NCP server name
NCP_SERVER=cluster1-lxvol44-server

# unbind the NCP volume
ignore_error ncpcon unbind --ncpservername=$NCP_SERVER --ipaddress=$RESOURCE_IP

# dismount the NCP volume
ignore_error ncpcon dismount $NCP_VOLUME

# if not using SMS for backup, comment out this sleep delay
sleep 10

# unmount the volume
sleep 10 # if not using SMS for backup, please comment out this line
exit_on_error umount_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

#deactivate the volume group
exit_on_error vgchange -a n $VOLGROUP_NAME

exit 0
```

11.3.3 Sample Monitor Script for an NCP Volume Cluster Resource

You modify the monitor script for the cluster resource of the Linux POSIX file system by first enabling monitoring for the cluster resource, then modifying the variable values. The settings in the sample script are based on the values in Section 11.3, “Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume,” on page 114. Ensure that you replace the values with the settings from your own configuration.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# define the IP address
RESOURCE_IP=10.10.10.44

# define the file system type
MOUNT_FS=ext3

# define the volume group name
VOLGROUP_NAME=name

# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/volume_name

# define the mount point
MOUNT_POINT=/mnt/mount_point

# define NCP volume
NCP_VOLUME=lxvol44

# define NCP server name
NCP_SERVER=cluster1-lxvol44-server

# test the file system
exit_on_error status_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

# status the IP address
exit_on_error status_secondary_ipaddress $RESOURCE_IP

# check the logical volume
exit_on_error status_lv $MOUNT_DEV

exit 0
```

Monitoring the Cluster Resource

Add the following line to the monitor script:

```
exit_on_error ncpcon volume <volume_name>
```

Monitoring the Availability of NCP File Services

Add the following lines to the monitor script:

```
rcndsd status
if test $? != 0; then
    exit_on_error rcndsd restart
fi
sleep 5


exit_on_error rcndsd status
/etc/init.d/ncp2nss status
if test $? != 0; then
    exit_on_error /etc/init.d/ncp2nss restart
fi
sleep 5
exit_on_error /etc/init.d/ncp2nss status
```

12 Managing File System Trustees, Trustee Rights, and Attributes on NCP Volumes

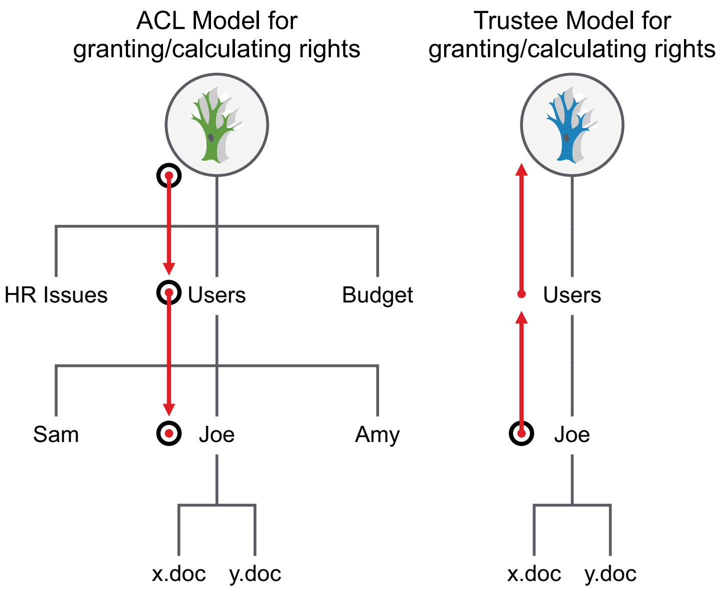
This section describes the NetWare trustee model and how to manage trustees and trustee rights for NCP volumes on an Open Enterprise Server (OES) 2015 SP1 server.

12.1 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 users in all child subdirectories. This means that a single trustee assignment can give a user rights to a large number of subdirectories and files. A user’s home directory is set up so that only the user and the system administrator have rights there. A user’s files are secure.

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.

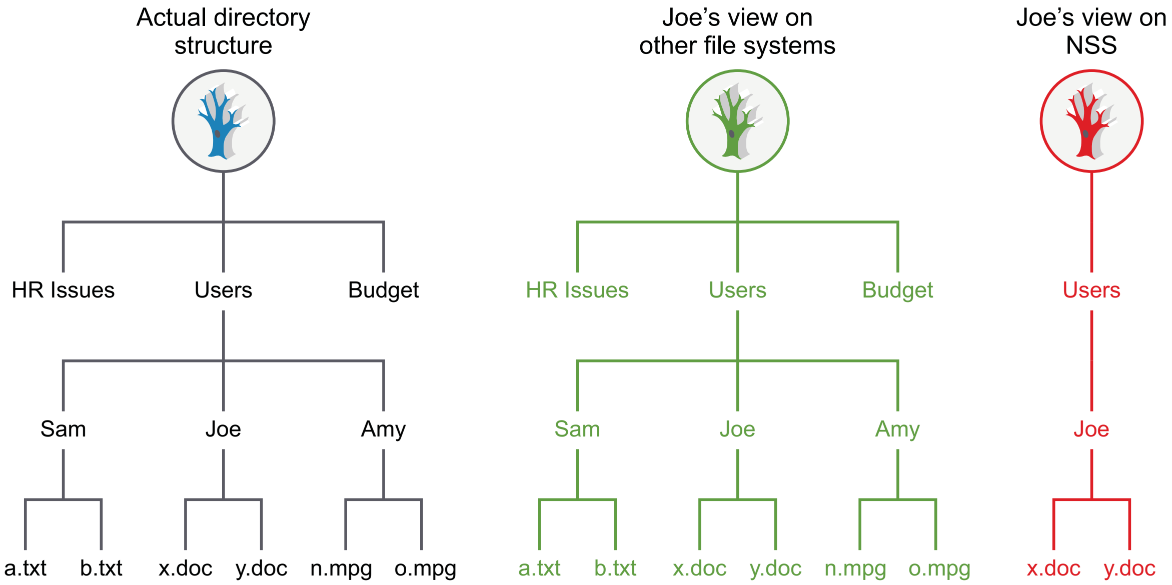
Figure 12-1 Compare the Linux ACL Model and the Novell Trustee Model


ACL Model for granting/calculating rights
Trustee Model for granting/calculating rights
HR Issues
Users
Budget
Sam
Joe
Amy
x.doc
y.doc
Users
Joe
x.doc
y.doc

The Novell Storage Services (NSS) volume on Linux and the NCP volumes on Linux use the Novell trustee model to control user access to files. Users can see only those directory paths that they need to see in order to access their files. On a Linux POSIX file system using Access Control Lists, visibility of the entire directory structure is not restricted.

For example, Figure 12-2 shows how the user Joe has restricted visibility into the file system to view only those paths needed to access the files in his home directory on an NSS volume on Linux. On Linux POSIX file systems without NCP Server, Joe is able to view the entire directory structure.

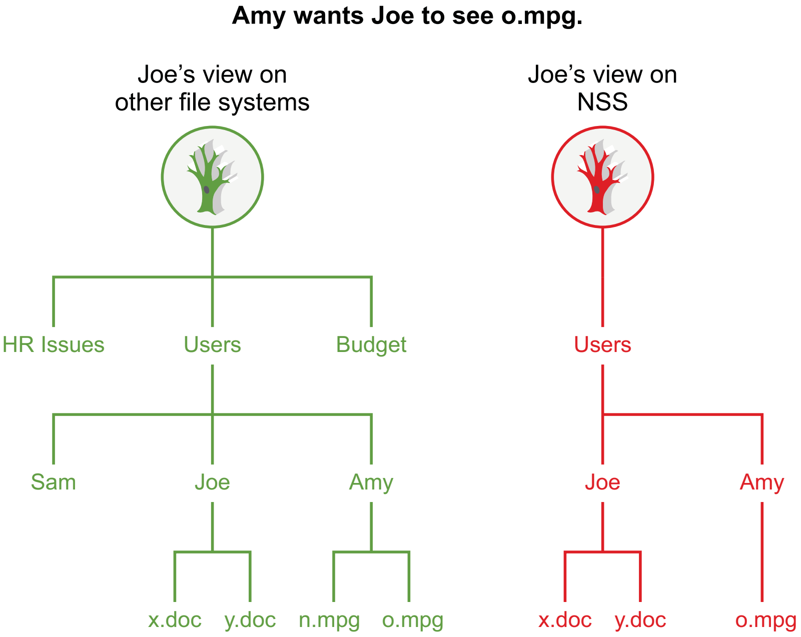
Figure 12-2 Comparison of File Visibility for Users of Linux POSIX Volumes and NSS Volumes on Linux



If users want to share files with others, they can grant rights through trustee assignments on the individual files, or by creating a shared subdirectory and assigning trustees to it. When a user is given a trustee assignment to a file or directory, he or she can automatically see each parent directory along the path up to the root. However, the user cannot see the contents of those directories, just the path to where he or she has rights.

For example, if the user Amy wants user Joe to see a particular file in her home directory, she can add Joe as a trustee of the file, then grant Joe limited rights to see the file. Joe can see the path to the file, but cannot see other files in Amy's home directory, as shown in Figure 12-3. On Linux file systems without NCP Server, Joe can see all files in Amy's home directory.

Figure 12-3 *File Visibility Granted to Trustees*



These differences in access control approaches 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 read and execute (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 is that of the user (or `root` if the user is not Linux-enabled with Linux User Management).
- The GID is `root`.
- The mode bits are:

```
rwx --- ---
```

This way, by default, the only people who can access a file or subdirectory from a LINUX environment are `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 10.8, "Configuring Inherit POSIX Permissions for an NCP Volume," on page 91 for information on how to enable or disable this option.

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 because 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.

12.2 Understanding File System Trustees, Trustee Rights, and Attributes

- Section 12.2.1, "Directory and File Trustee Rights," on page 122
- Section 12.2.2, "Directory and File Attributes," on page 122

12.2.1 Directory and File Trustee Rights

A trustee is any NetIQ eDirectory object, such as a User object, Group object, Organizational Role object, 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.

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

- Read (Default=On)
- Write (Default=Off)
- Create (Default=Off)
- Erase (Default=Off)
- Modify (Default=Off)
- File Scan (Default=On)
- Access Control (Default=Off)
- Supervisor (Default=Off)

12.2.2 Directory and File Attributes

NCP Server for Linux supports the directory and file attributes for NSS volumes. For a complete list of file attributes, see "Understanding File System Access Control Using Trustees" in the *OES 2015 SP1: File Systems Management Guide*.

The following file and directory attributes are supported for NCP volumes on Linux POSIX file systems.

- Read Only

- Hidden
- Shareable

Other file and directory attributes that are listed for NCP Server's support of the NSS file system are not supported for Linux POSIX file systems.

The other NSS file and directory attributes might appear to be supported on Linux POSIX file systems, and might also appear to be configurable, but the other file and directory attributes are not supported, and are 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 is on a non-NSS file system.

IMPORTANT: File and directory attributes are supported and enforced by the file system that underlies an NCP volume, not by NCP Server.

12.3 Managing File System Rights with NCPCON

Use the NCPCON utility to view, add, or remove file and directory rights for NSS volumes and NCP volumes on Linux.

- Section 12.3.1, "Viewing File and Directory Rights," on page 123
- Section 12.3.2, "Adding File and Directory Rights," on page 123
- Section 12.3.3, "Removing File and Directory Rights," on page 124

12.3.1 Viewing File and Directory Rights

To view file or directory rights, enter `ncpcon` at the Linux server console and then enter `rights view` *`path`*.

```
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 by using this command.

12.3.2 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
```

12.3.3 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
```

12.4 Managing File or Directory Trustees and Rights with iManager

You can optionally manage trustees and trustee rights for files and directories by using the **Files and Folders** role in Novell iManager.

1. In iManager, click **Files and Folders** > **Properties**.
2. Click the **Search** icon to select the directory or file that you want to manage.
3. Click **Rights**, then view, add, or remove trustees and set trustee rights for the selected file or directory.

   Changes are not saved until you click **Apply** or **OK**.
4. Click **Inherited Rights**, then view or modify inherited trustees and rights for the parent directories for the selected file or directory.

   Changes are not saved until you click **Apply** or **OK**.
5. Click **Apply** or **OK** to save your changes.

12.5 Managing File or Directory Attributes with iManager

You can optionally manage the file or directory attributes by using the **Files and Folders** role in Novell iManager.

1. In iManager, click **Files and Folders** > **Properties**.
2. Click the **Search** icon to locate and select the directory or file that you want to manage.
3. On the Properties page, select **Information**.
4. Enable or disable the file attribute by selecting or deselecting the check box next to the attribute.

   For NCP volumes, you can modify the following attributes:

   - Read Only
   - Hidden
   - Shareable

Changes are not saved until you click **Apply** or **OK**.

5 Click **Apply** or **OK** to save your changes.

12.6 Generating and Viewing NCP Trustee Reports for NSS Volumes

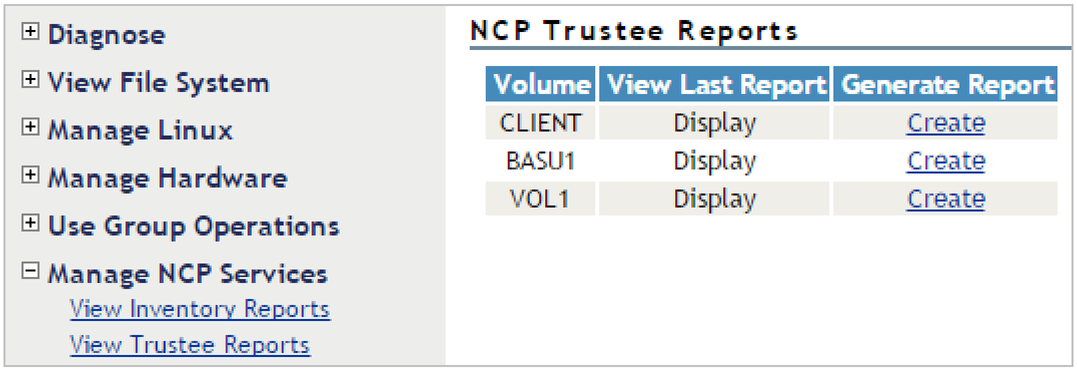
In Novell Remote Manager, the new **View Trustee Reports** option allows you to generate a trustee report for a specified NSS volume. This includes Dynamic Storage Technology shadow volumes that are comprised of two NSS volumes. You can display the last trustee report in the Web browser, or send the report to the e-mail addresses that you have preconfigured for Novell Remote Manager. A trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.

- Section 12.6.1, "Generating an NCP Trustee Report," on page 125
- Section 12.6.2, "Viewing a Saved NCP Trustee Report," on page 126

12.6.1 Generating an NCP Trustee Report

1 Log in to Novell Remote Manager as the `root` user.

2 In the left navigation panel, select **Manage NCP Services > View Trustee Report**s.



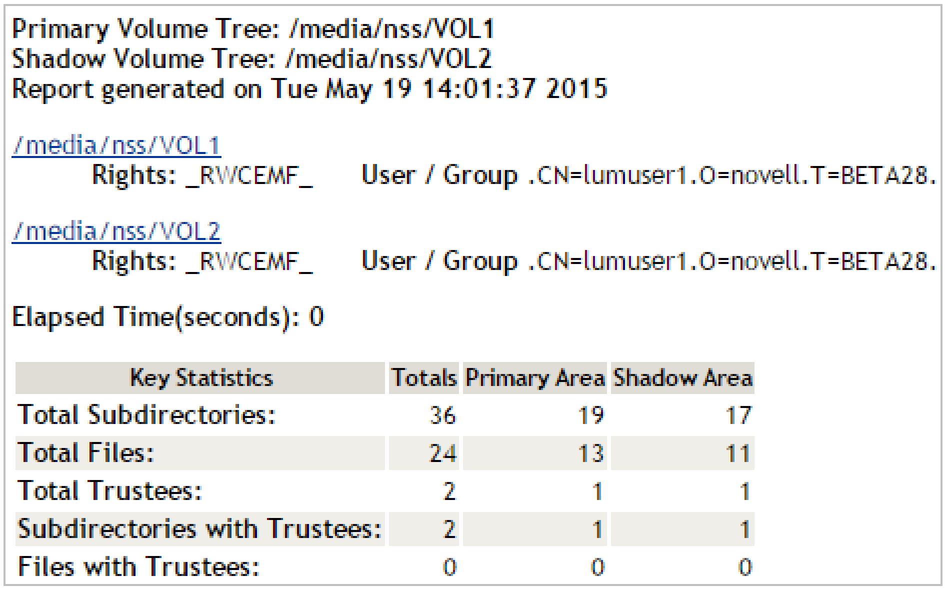
NCP Trustee Reports

Volume	View Last Report	Generate Report
CLIENT	Display	Create
BASU1	Display	Create
VOL1	Display	Create

3 On the NCP Trustee Reports page, locate the NSS volume in the list, then click its **Create** link in the **Generate Report** column.

4 View the NCP Trustee report.

A volume's trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume. For example, the following trustee report shows the rights for a folder in a Dynamic Storage Technology shadow volume.



Primary Volume Tree: /media/nss/VOL1
Shadow Volume Tree: /media/nss/VOL2
Report generated on Tue May 19 14:01:37 2015

/media/nss/VOL1
Rights: _RWCEMF_ User / Group .CN=lumuser1.O=novell.T=BETA28.

/media/nss/VOL2
Rights: _RWCEMF_ User / Group .CN=lumuser1.O=novell.T=BETA28.

Elapsed Time(seconds): 0

Key Statistics	Totals	Primary Area	Shadow Area
Total Subdirectories:	36	19	17
Total Files:	24	13	11
Total Trustees:	2	1	1
Subdirectories with Trustees:	2	1	1
Files with Trustees:	0	0	0

12.6.2 Viewing a Saved NCP Trustee Report

You can view the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.

1. Log in to Novell Remote Manager as the `root` user.
2. In the left navigation panel, select **Manage NCP Services > NCP Trustee Report**.
3. Locate the NSS volume of interest in the list, then click its **Display** link in the **View Last Report** column.

13 Using Opportunistic Locking for NCP File Handling

This section contains information to help you understand opportunistic locking (oplocks) for NCP Server for Open Enterprise Server (OES) 2015 SP1.

13.1 Understanding Opportunistic Locking for NCP Connections

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 tickle packets 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). 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.

WARNING: Level 2 oplocks are inappropriate for server-side database applications: Do not use oplock Level 2 with databases. Level 1 oplocks can remain switched on.

13.1.1 Level 2 OpLocks

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 does not notify the client when another connection wants exclusive access to that file (delete, rename, exclusive open, and so forth).

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 does the following:

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.

13.1.2 Level 1 OpLocks

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 cannot 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 does the following:

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.

      The Novell Client never does 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.

13.1.3 Guidelines for Using OpLocks

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 does not 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 needs 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 an L1 oplock, the open fails because the server cannot delay the request and wait for notification from the client that it has cleared the oplock.

13.2 Configuring OpLocks for NCP Server

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.

IMPORTANT: Ensure that users are running Client for Open Enterprise Server 2 SP4 and later.

By default, oplocks is set to level 1, which includes both level 1 and level 2 functionality.

You can modify the OPLOCK_SUPPORT_LEVEL parameter setting by using Novell Remote Manager for Linux as follows:

1. In Novell Remote Manager for Linux, select **Manage NCP Services > Manage Server**.
2. Click the **Parameter Value** link for OPLOCK_SUPPORT_LEVEL.
3. Set the value to 0, 1, or 2.
   - **0:** Disables oplocks support.
   - **1:** Enables oplocks support at L1.
   - **2:** Enables oplocks support at L2 (the default).
4. Click **OK** to apply the change.

You can also change or disable the setting by adding an OPLOCK_SUPPORT_LEVEL command to the `/etc/opt/novell/ncpserv.conf` configuration file. If you have never modified the OPLOCK_SUPPORT_LEVEL from the default setting of 2, you must add the parameter line. If you have previously modified the setting, the parameter appears as a line in the file, and you can simply change its value. After you manually modify the file, you must restart the NetIQ eDirectory daemon (`ndsd`).

1. Log in as the `root` user, then open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
2. Do one of the following:
   - If the OPLOCK_SUPPORT_LEVEL parameter is not listed, add a line for the OPLOCK_SUPPORT_LEVEL option with the value of 0, 1, or 2.

     For example, to disable oplocks support, set the value to 0 by adding this line:

     ```
     OPLOCK_SUPPORT_LEVEL 0
     ```

     Or, to set oplocks support to L1, set the value to 1 by adding this line:

```
OPLOCK_SUPPORT_LEVEL 1
```

- If the OPLOCK_SUPPORT_LEVEL parameter is already listed in the file, change its value to the desired setting of 0, 1, or 2.

3 Save the file.

4 After changing the oplock level in `/etc/opt/novell/ncpserv.conf`, you must restart `ndsd` to apply the changes. Open a terminal console as the `root` user, then enter

```
rcndsd restart
```

13.3 Configuring File Caching in the Client for Open Enterprise Server

Opportunistic locking is supported for Client for Open Enterprise Server 2 SP4 and later. In order to take advantage of opportunistic locking, the client must be enabled for file caching.

To enable file caching for Client for Open Enterprise Server:

1 On the desktop, right-click the **Client tray application** icon in the status area, then select **Client Properties**.

2 In the Configuration dialog box, select **Advanced Settings**.

3 In the **Parameter Groups** drop-down list, select **Performance, Cache**.

4 (Conditional) On Client for Open Enterprise Server 2 SP4 (IR6) or earlier:

In the list of options, select **File Caching** and set its value to **On**.

5 (Conditional) On Client For Open Enterprise Server 2 SP4 (IR7) or later:

To enable only read caching, in the list of options, select **File Caching** and set its value to **Read only**.

or

To enable both read and write caching, in the list of options, select **File Caching** and set its value to **Read and Write**.

6 Select **OK** to save and apply the settings.

13.4 Configuring OpLocks for NSS Volumes

On Linux, opportunistic locking for NSS volumes is controlled by the NCP Server `OPLOCK_SUPPORT_LEVEL` parameter setting. This NCP setting applies to all volumes mounted via `NCPCON MOUNT` on the server.

```
ncpcon set OPLOCK_SUPPORT_LEVEL=<level>
```

13.5 Configuring Mask Behavior for Range Locks

This parameter allows applications to acquire a lock above the 0x7fffffffffffffff region limitation set by the Linux file system. By default this parameter is turned on. Setting the parameter value to 0, turns off this parameter and does not permit locking beyond the 0x7fffffffffffffff region.

```
ncpcon set LOCK_RANGE_MASK=1
```

```
ncpcon set LOCK_RANGE_MASK=0
```

13.6 Additional Information

For issues and troubleshooting tips, see *Information on Opportunistic Locking (Technical Information Document 7001112 (formerly known as TID 10095627))*.

14 Using the Inventory to Monitor NCP Volumes

In Novell Remote Manager for Linux, you can view inventory reports for the NCP volume, with statistics and information about its files.

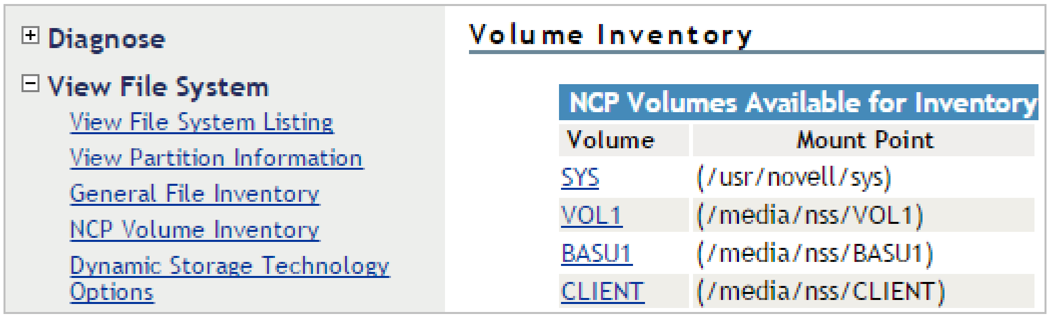
- Section 14.1, “Accessing the Volume Inventory,” on page 133
- Section 14.2, “Understanding the Volume Inventory,” on page 134
- Section 14.3, “Viewing Statistics for the Volume,” on page 149
- Section 14.4, “Using Inventory Detail Reports to Move, Copy, or Delete Files on the Volume,” on page 150
- Section 14.5, “Generating a Custom Inventory Report for DST Shadow Volumes,” on page 150

14.1 Accessing the Volume Inventory

1 Open Novell Remote Manager for Linux in a Web browser, then log in as the `root` user.

2 Use one of the following methods to view the volume inventory:

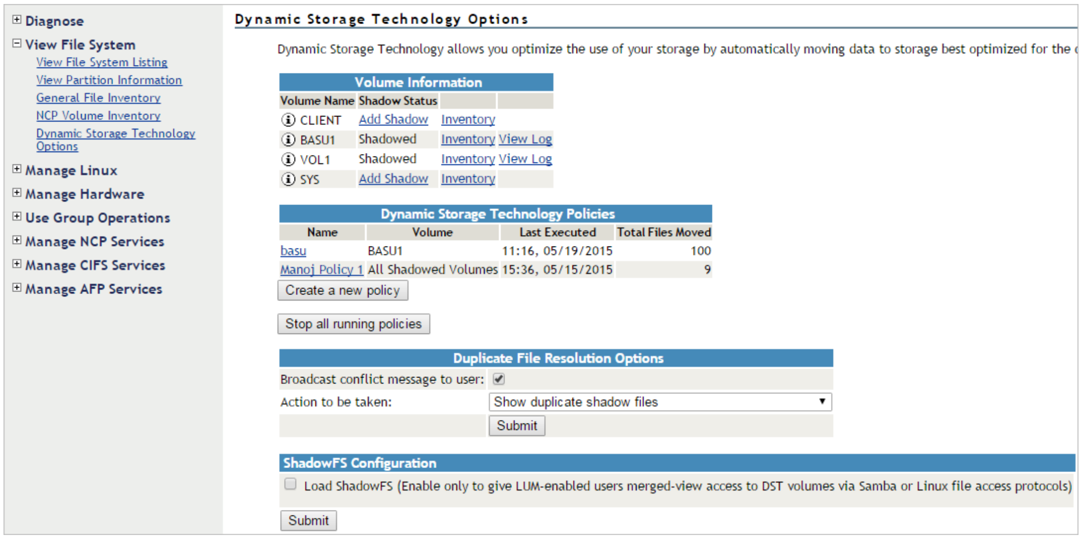
   - Select **View File System > NCP Volume Inventory**, locate the volume in the **NCP Volumes Available for Inventory** list, then click the **Volume** link for the volume.



NCP Volumes Available for Inventory

Volume	Mount Point
SYS	(/usr/novell/sys)
VOL1	(/media/nss/VOL1)
BASU1	(/media/nss/BASU1)
CLIENT	(/media/nss/CLIENT)

- Select **View File System > Dynamic Storage Technology Options**, locate the volume in the list, then click the **Inventory** link next to it.



Dynamic Storage Technology Options

Dynamic Storage Technology allows you optimize the use of your storage by automatically moving data to storage best optimized for the

Volume Information

Volume Name	Shadow Status		
CLIENT	Add Shadow	Inventory	
BASU1	Shadowed	Inventory	View Log
VOL1	Shadowed	Inventory	View Log
SYS	Add Shadow	Inventory	

Dynamic Storage Technology Policies

Name	Volume	Last Executed	Total Files Moved
basu	BASU1	11:16, 05/19/2015	100
Manoj Policy 1	All Shadowed Volumes	15:36, 05/15/2015	9

Duplicate File Resolution Options

Broadcast conflict message to user: ☑

Action to be taken: Show duplicate shadow files ▾

ShadowFS Configuration

☐ Load ShadowFS (Enable only to give LUM-enabled users merged-view access to DST volumes via Samba or Linux file access protocols)

14.2 Understanding the Volume Inventory

The inventory reports key statistics about the files in the selected volume, such as files scanned and the available space trends. It reports information for NCP volumes on Linux POSIX file systems, Novell Storage Services (NSS) volumes, and Dynamic Storage Technology (DST) shadow volumes.

- Section 14.2.1, “Inventory Summary,” on page 134
- Section 14.2.2, “Available Space Trend Graph,” on page 135
- Section 14.2.3, “Graphical Profiles,” on page 135
- Section 14.2.4, “Tabular Profiles,” on page 147
- Section 14.2.5, “Inventory Detail Reports,” on page 147
- Section 14.2.6, “Custom Scans,” on page 148

14.2.1 Inventory Summary

The inventory summary reports the number of files scanned on the volume and key statistics.

For a DST shadow volume, it shows information for the primary storage area and the secondary storage area. It also reports key statistics for the primary storage area, the secondary storage area, and both areas combined as the shadow volume.

Key Statistics	Description
Total Subdirectories	The total number of subdirectories in the volume.
Total Files	The total number of files in the volume.
Space in Use	The amount of space currently in use in the volume for data and metadata. On NSS volumes where salvage is enabled, the space in use includes space used by deleted files and directories.
Space Available	The amount of free space in the volume.

Key Statistics	Description
File Types	The number of different file types in use throughout the entire volume.
Soft Link Files	The NSS file system and NCP Server do not support soft links to files. This is a placeholder for future non-NCP support.
Soft Link Subdirectories	The NSS file system and NCP Server do not support soft links to subdirectories. This is a placeholder for future non-NCP support.
FIFO (named pipe) and Socket File Types	Although the NSS file system supports, NCP Server does not support and display FIFO (named pipe) and Socket File Types when a volume is scanned for files. This is a placeholder for future non-NCP support.

14.2.2 Available Space Trend Graph

The Available Space Trend Graph shows the trends for space usage on the volume. For a DST shadow volume, it shows information for the primary storage area and the secondary storage area.

14.2.3 Graphical Profiles

The **Profiles** portion of the inventory report graphically displays information about the volume. Graphical profiles are displayed by size in bytes and file count for the following categories:

- “File Type Profiles” on page 135
- “File Owner Profiles” on page 137
- “Time Stamp Profiles” on page 139
- “File Size Profiles” on page 145

File Type Profiles

File Type Profiles indicates storage space usage by file types that are actually in use on your system, such as LOG, TDF, DAT, XML, EXE, and so on.

Figure 14-1 *File type profiles - Bytes In Use*

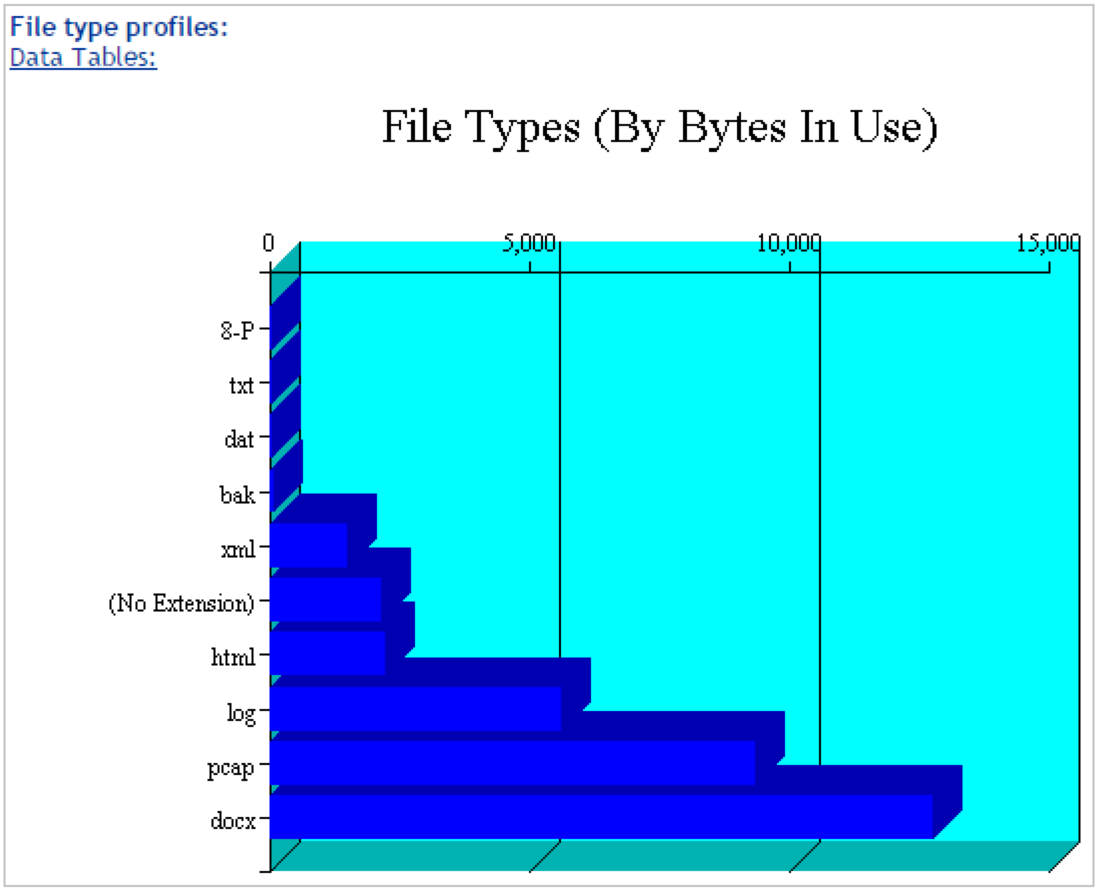
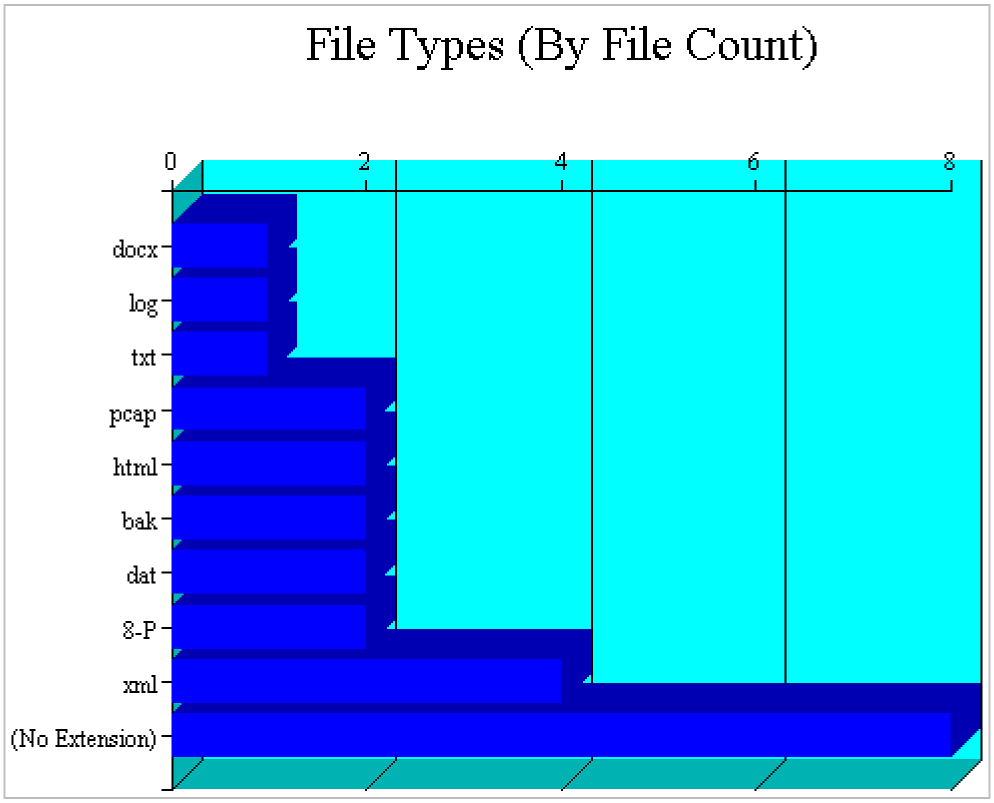


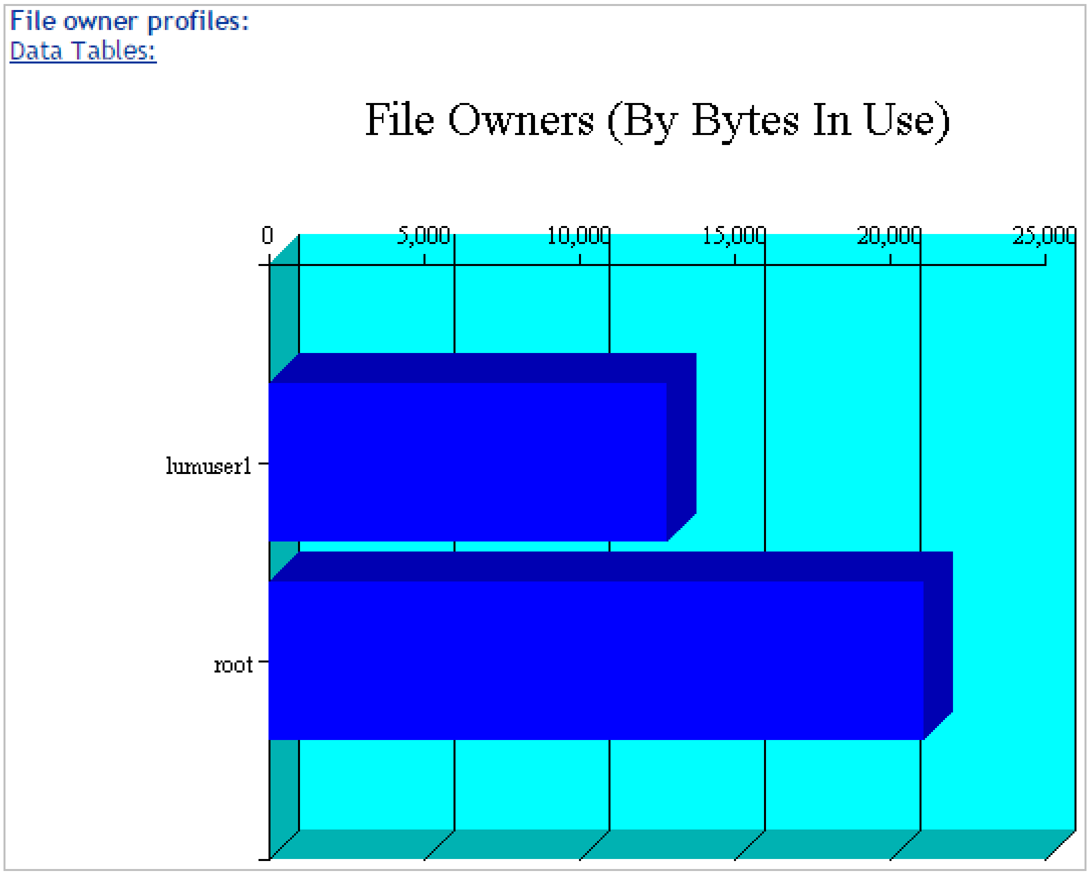
Figure 14-2 File type profiles - File Count



File Owner Profiles

File Owner Profiles indicates storage space usage by the designated owner of the file. It is not unusual in NCP to see the `root` user as the owner of files. For NCP volumes and NSS, file access is governed by the file system trustees assigned to the file, not the file owner. Trustees are users who have User objects defined in NetIQ eDirectory, and who have been granted file system rights for the file. NCP tracks ownership via the user's eDirectory GUID.

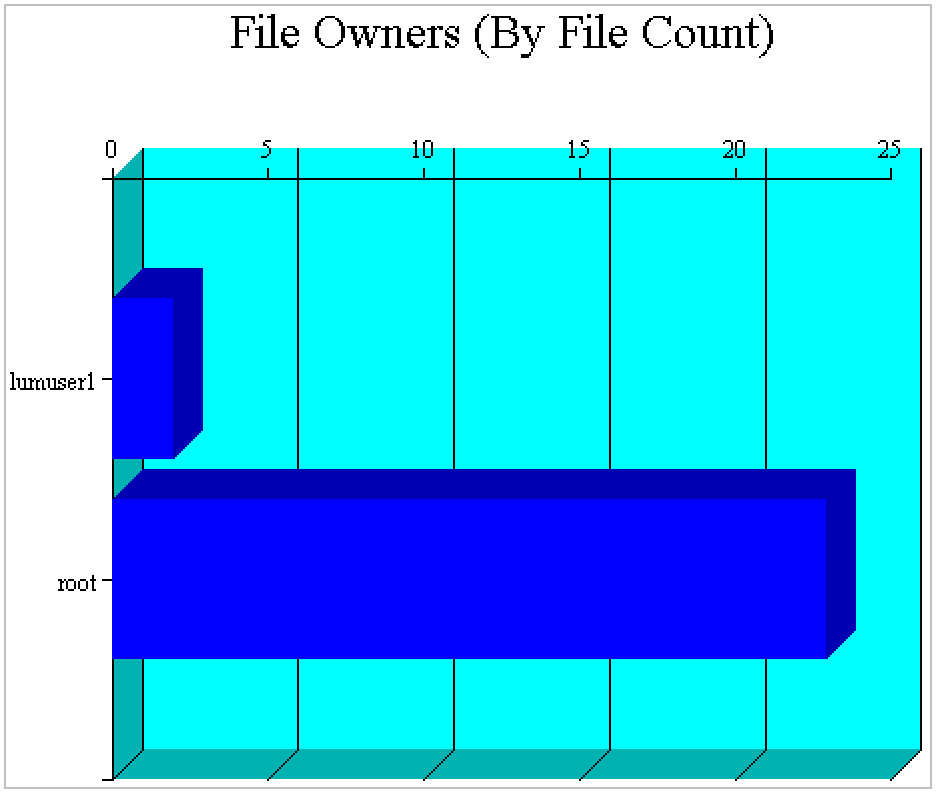
Figure 14-3 *File owner profiles - Bytes In Use*



File owner profiles:

Data Tables:

Figure 14-4 File owner profiles - File Count

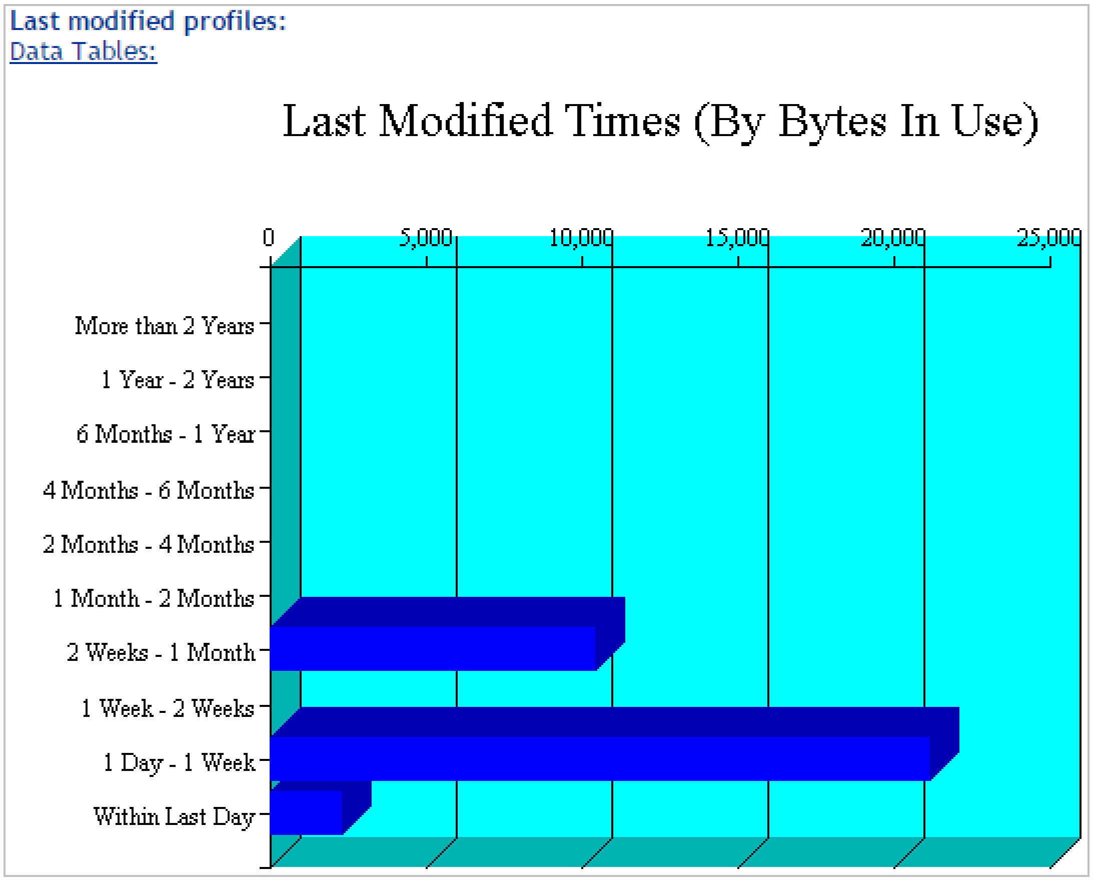


Time Stamp Profiles

Three time stamp profiles are generated:

- **Files Modified Profiles:** Modified dates indicate the last time someone changed the contents of a file.

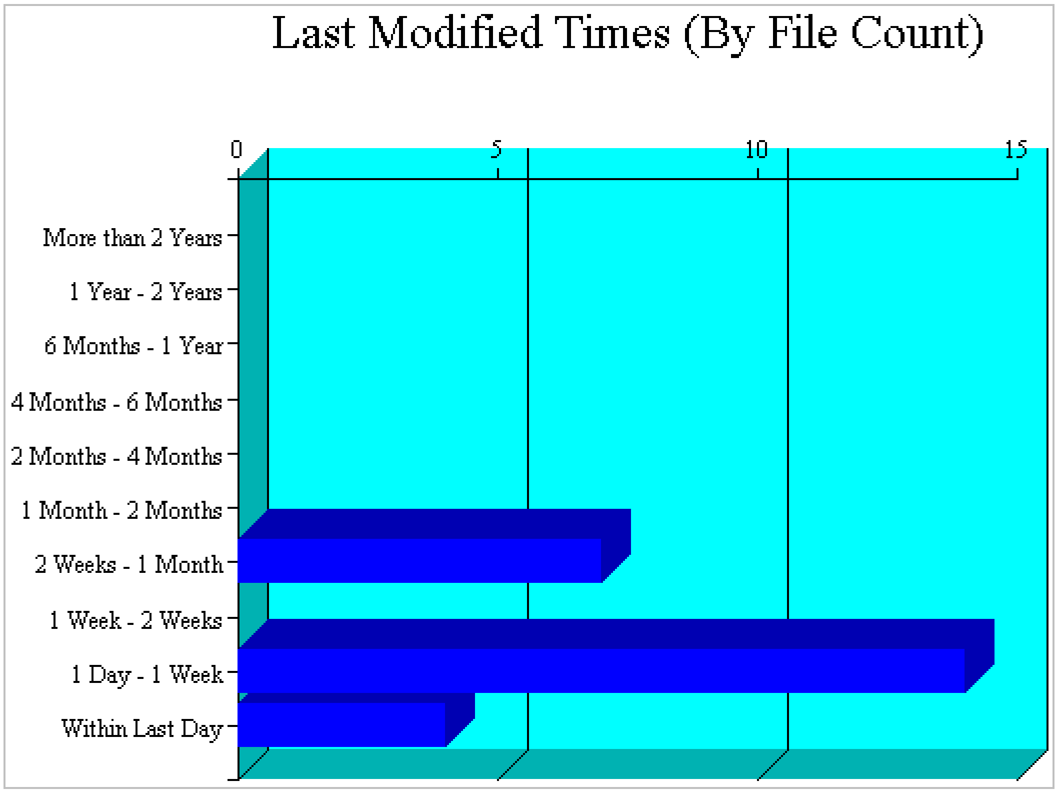
Figure 14-5 Last modifies profiles - Bytes In Use



Last modified profiles:

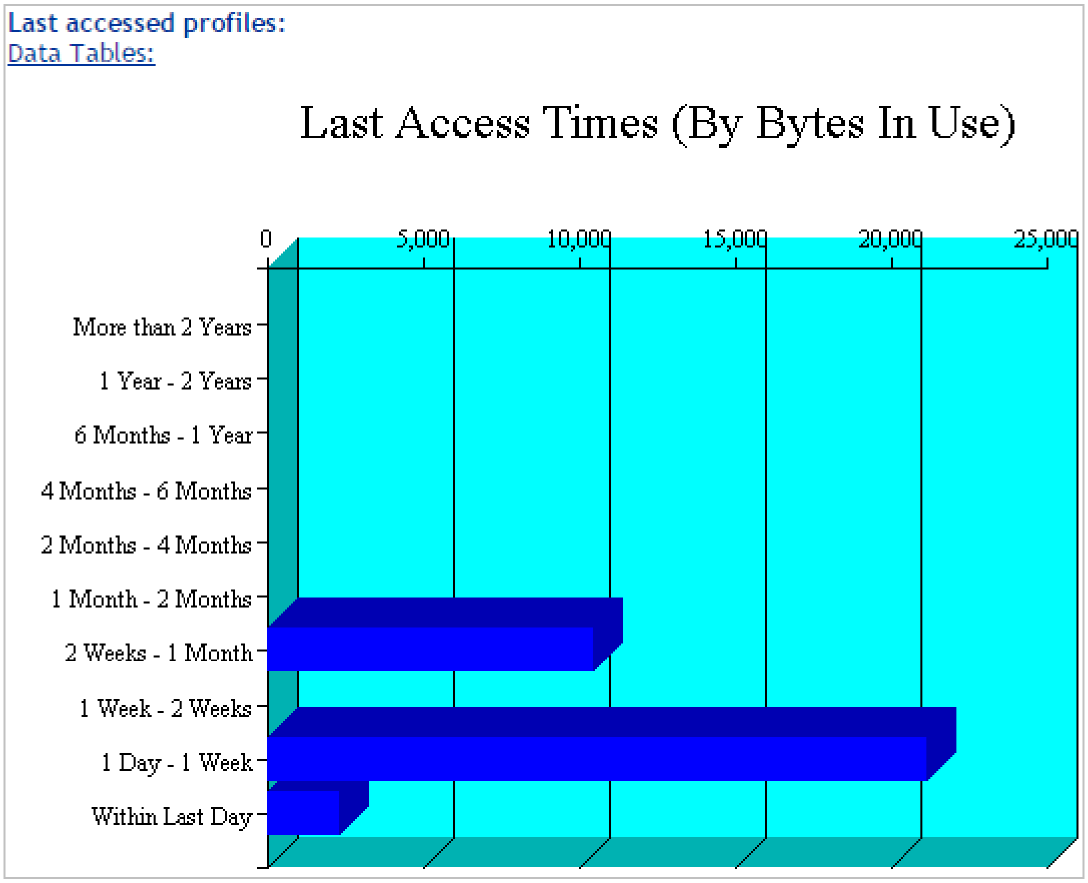
Data Tables:

Figure 14-6 Last modified profiles - File Count



- **Files Accessed Profiles:** Access dates indicate the last time someone accessed a file, but did not change the contents if this differs from the modified date.

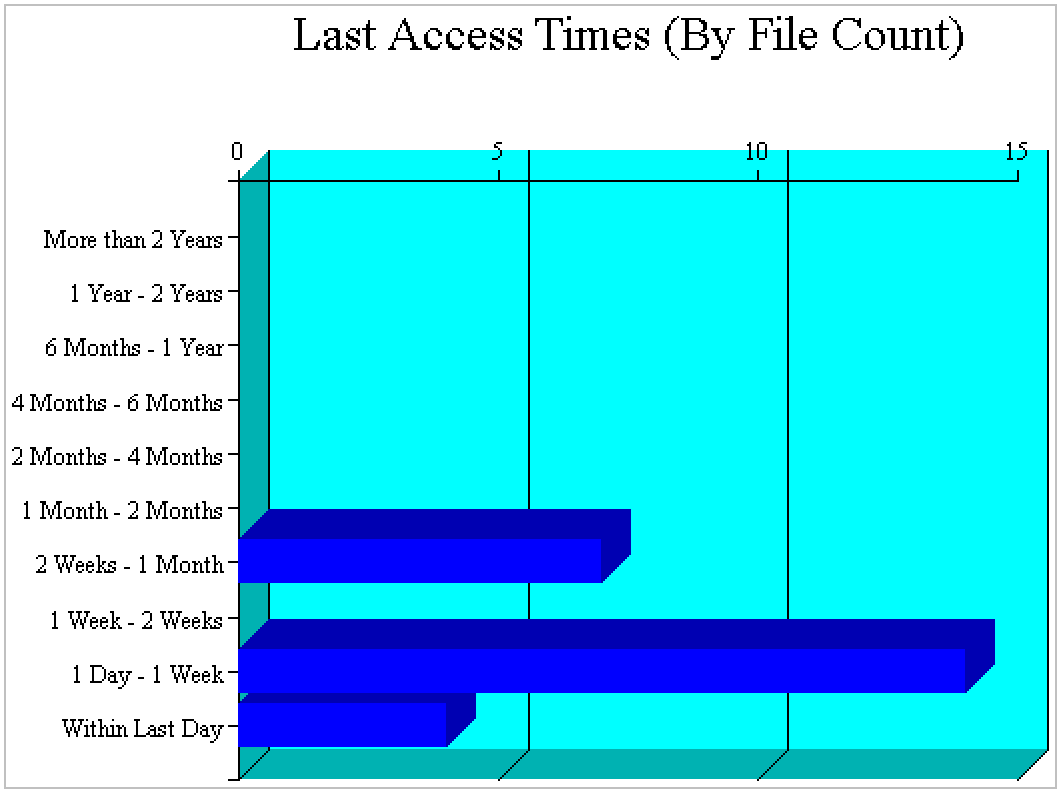
Figure 14-7 Last accessed profiles - Bytes In Use



Last accessed profiles:

Data Tables:

Figure 14-8 Last accessed profiles - File Count



- **Files Changed Profiles:** Change dates indicate the last time someone changed the metadata of a file, but did not change the contents if this differs from the modified date.

Figure 14-9 Change time profiles - Bytes In Use

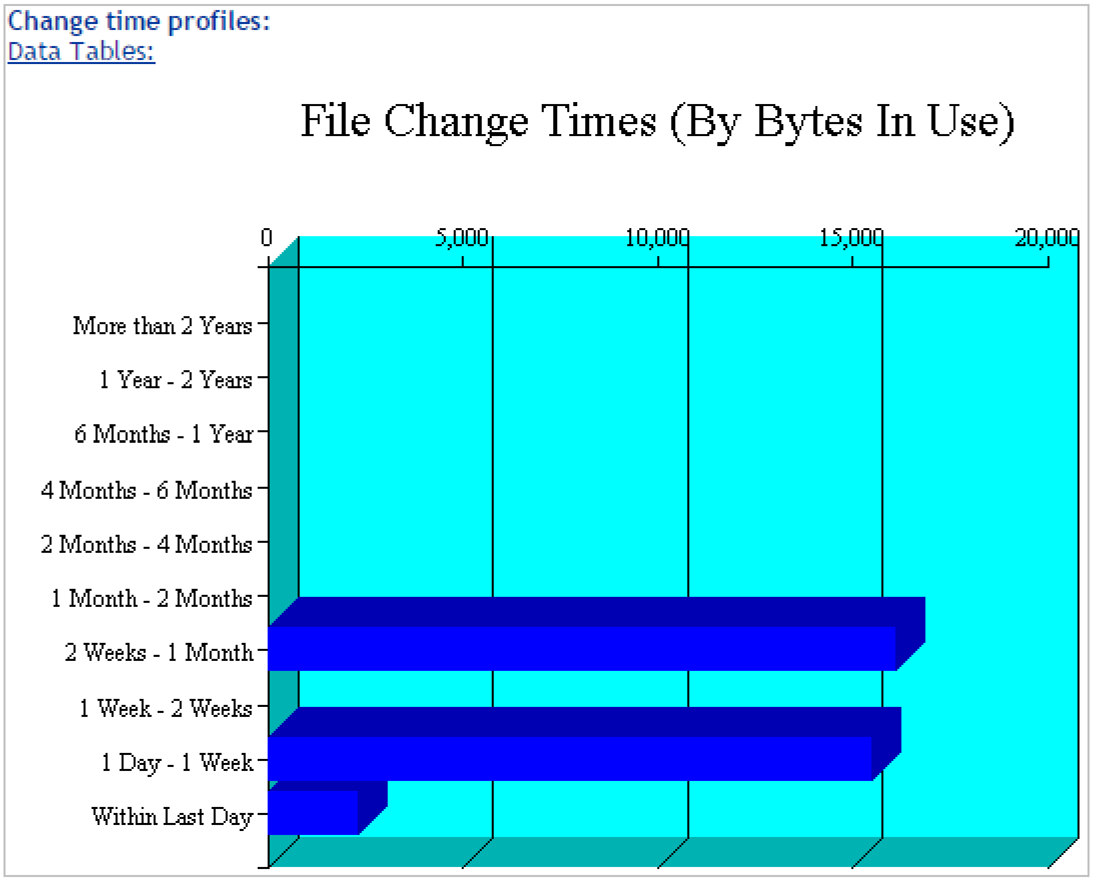
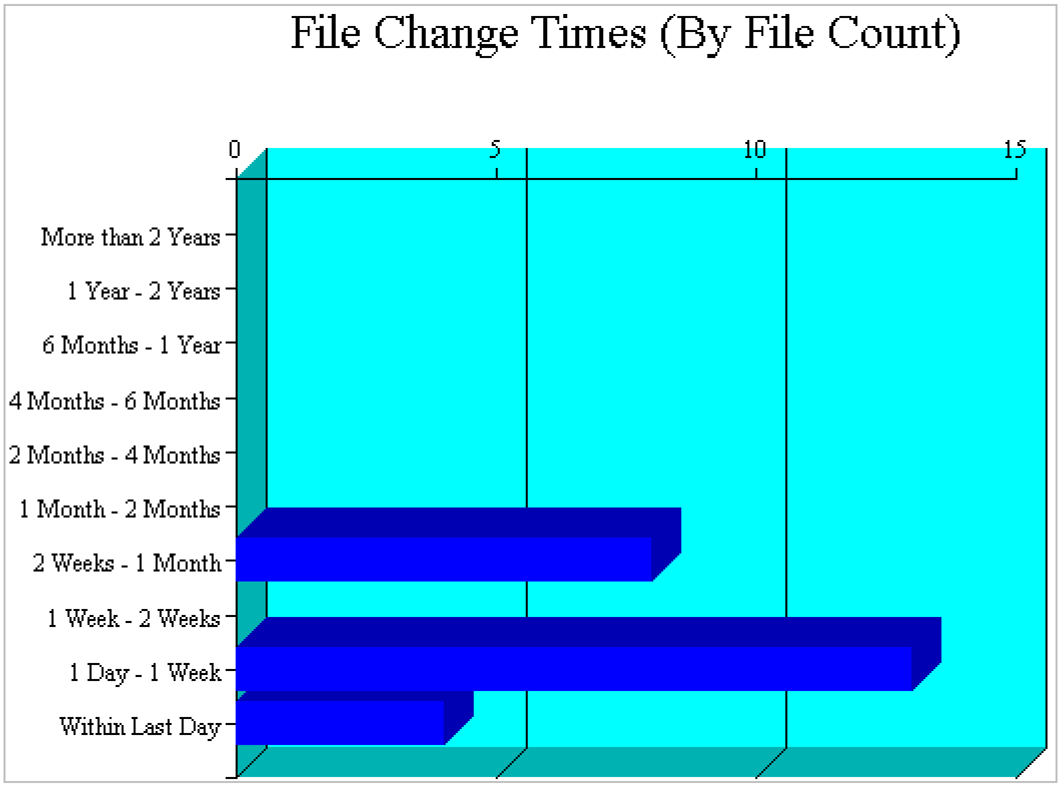


Figure 14-10 Change time profiles - File Count



Time stamps are grouped by the following time periods:

More than 2 years
1 year to 2 years
6 months to 1 year
4 months to 6 months
2 months to 4 months
1 month to 2 months
2 weeks to 1 month
1 week to 2 weeks
1 day to 1 week
Within last day

File Size Profiles

File Size Profiles reports the size of files, grouped by the following size ranges:

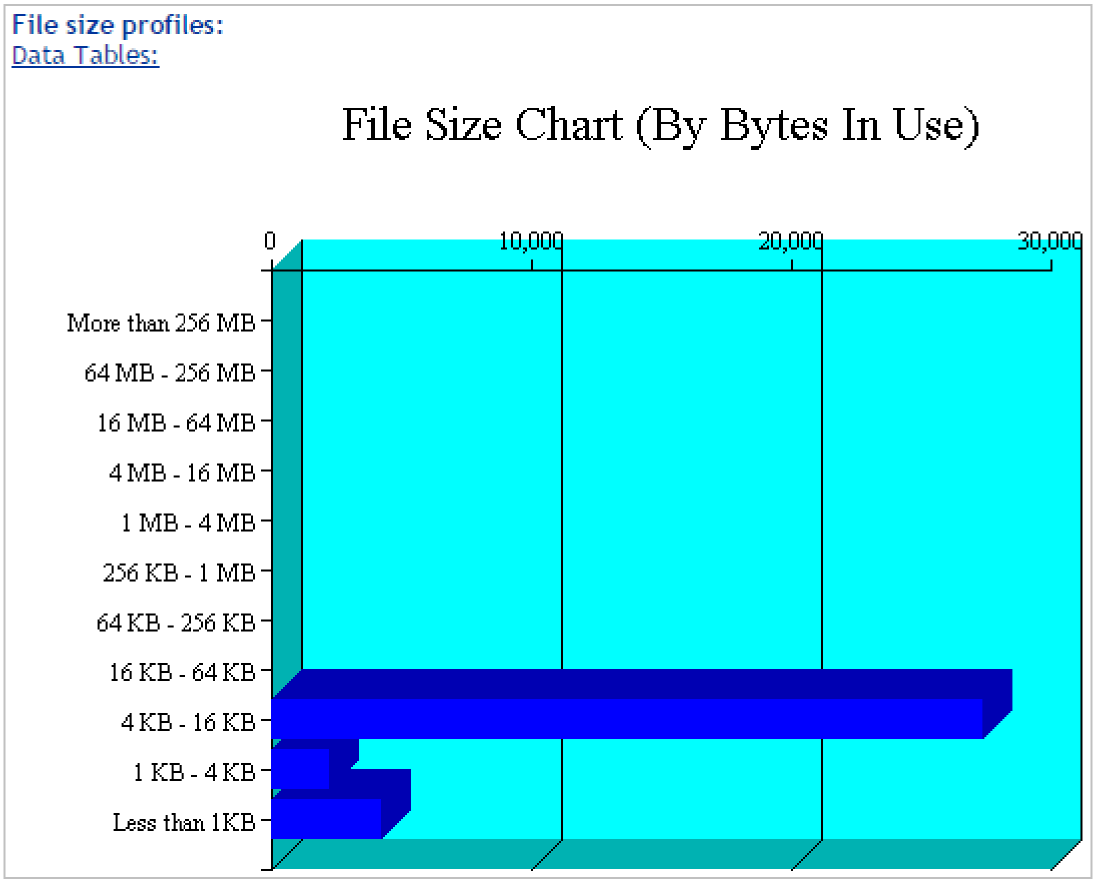
More than 256 MB
64 MB to 256 MB
16 MB to 64 MB
4 MB to 16 MB
1 MB to 4 MB
256 KB to 1 MB
64 KB to 256 KB
16 KB to 64 KB

4 KB to 16 KB

1 KB to 4 KB

Less than 1 KB

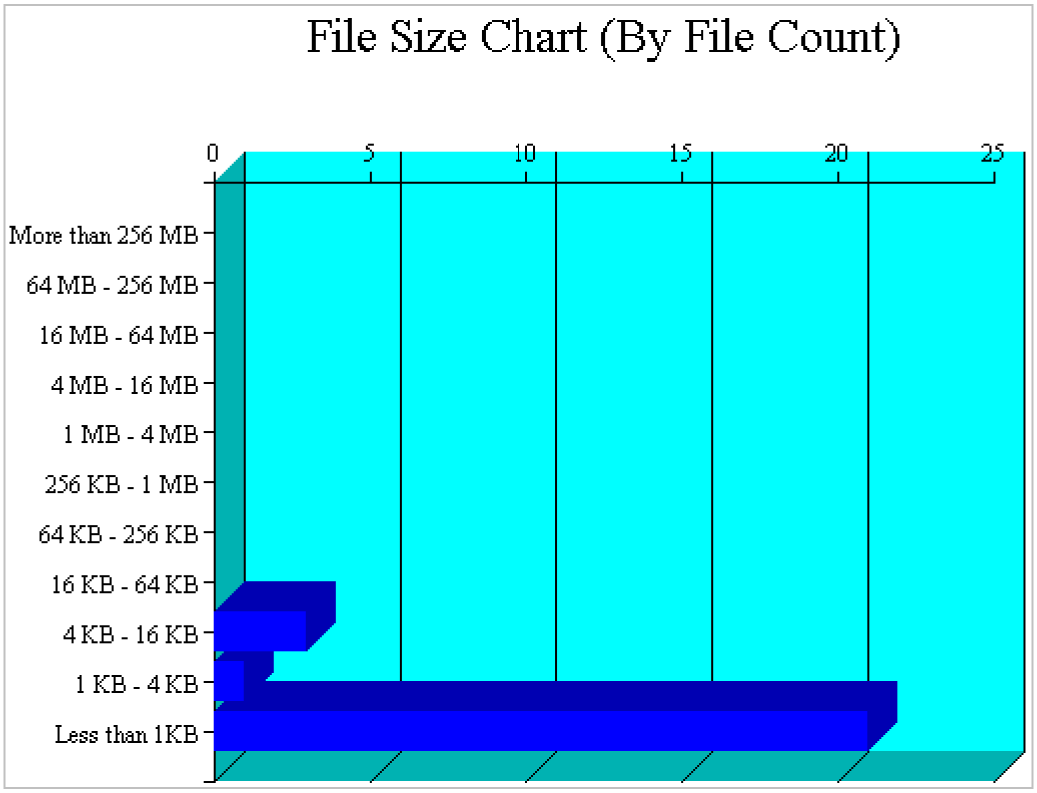
Figure 14-11 File size profiles - Bytes In Use



File size profiles:

Data Tables:

Figure 14-12 *File size profiles - File Count*



14.2.4 Tabular Profiles

Statistical data used to create the graphs is also available in tables that report statistics for the volume.

For a DST shadow volume, data is categorized for the primary area, the secondary area, and both areas combined as the shadow volume. The count for file entries for the primary area and shadow (secondary) area are linked to detail reports that list the files matching that particular category and group. From the file lists, you have the option to copy, move, or delete one or multiple files.

14.2.5 Inventory Detail Reports

An Inventory Detail report lists all of the files that match a particular category and group for a file count entry in the tabular reports in the volume inventory. You can select one or multiple files in the list, then select one of the following operations to be performed:

- Move the selected volumes to the other file tree. (This option is available only for DST shadow volumes.)
- Move the selected files to a specified path on the server.
- Copy the selected files to a specified path on the server.
- Delete the selected files.

14.2.6 Custom Scans

At the bottom of the inventory report, you can create custom scans: Customer Directory Tree Scans for NCP volumes, or Custom Shadow Volume Options for DST shadow volumes. These scans allow you to generate reports based on key statistics of interest, and perform actions on them.

- "Volume Operations for DST Shadow Volumes" on page 148
- "Search Patterns" on page 148
- "File Owner Restrictions" on page 148
- "Time Stamp Restrictions" on page 148
- "File Size Restrictions" on page 149

Volume Operations for DST Shadow Volumes

In the Custom Shadow Volume Options scan, you can perform one of the following operations for DST shadow volumes on the files that match the search criteria you specify:

- List primary area selected files
- Move selected files from primary area to shadow area.
- List shadow area selected files.
- Move selected files from shadow area to primary area.

Search Patterns

In Search Patterns you can specify wildcards and characters to select files by filenames or extensions.

File Owner Restrictions

In File Owner Restrictions select **None** or a user name. The search applies only to files where the file owner matches the specified owner.

Time Stamp Restrictions

You can specify one or multiple time stamps to consider for the search:

- Last Modified Time
- Last Accessed Time
- Last Changed Time

If no time stamp is selected, time stamps are not considered in the search criteria.

If a time stamp is selected, you can specify one or multiple time ranges to consider for the search:

Within last day
1 day to 1 week
1 week to 2 weeks
2 weeks to 1 month
1 month to 2 months
2 months to 4 months

4 months to 6 months
6 months to 1 year
1 year to 2 years
More than 2 years

File Size Restrictions

You can specify one or multiple ranges of file sizes to consider for the search:

Less than 1 KB
1 KB to 4 KB
4 KB to 16 KB
16 KB to 64 KB
64 KB to 256 KB
256 KB to 1 MB
1 MB to 4 MB
4 MB to 16 MB
16 MB to 64 MB
64 MB to 256 MB
More than 256 MB

14.3 Viewing Statistics for the Volume

1. In Novell Remote Manager, access the volume inventory for the NCP volume or shadow volume.

   For information, see Section 14.1, “Accessing the Volume Inventory,” on page 133.

2. In the inventory summary area, click a link to go directly to one of the following reports, or scroll to view the reports.

   For information about each statistical report, see Section 14.2, “Understanding the Volume Inventory,” on page 134.

   - Available space trend graph
   - File type profiles
   - File owner profiles
   - Last modified profiles
   - Last accessed profiles
   - Change time profiles
   - File size profiles
   - Links to specific reports
   - Custom directory tree scan (NCP volume or NSS volume), or Custom shadow volume options (DST shadow volume)

3. Click the **Data Tables** link for a profile to jump directly to the tabular display of the information that was used to generate the graph.

14.4 Using Inventory Detail Reports to Move, Copy, or Delete Files on the Volume

1. In Novell Remote Manager, access the volume inventory for the shadow volume.

   For information, see Section 14.1, "Accessing the Volume Inventory," on page 133.
2. In the summary area, click **Links to Specific Reports**, or scroll down to the **Links to Specific Reports** section to view the tabular reports of information used to generate the profiles.
3. Review the following categories to locate the files of interest:
   - Last modified range
   - Last accessed range
   - Change time range
   - File size range
   - File owner
   - File extension
4. Click the link of the data entry for the files that you want to manage. Files are grouped by Primary area and by shadow (secondary) area.
5. In the Inventory Detail report select one or multiple files in the list, then do one of the following:
   - Move the selected volumes to the other file tree (primary or shadow (secondary) file tree). (This option is available only for DST shadow volumes.)
   - Move the selected files to a specified path on the server.
   - Copy the selected files to a specified path on the server.
   - Delete the selected files.

14.5 Generating a Custom Inventory Report for DST Shadow Volumes

You can customize the inventory report to limit the search sizes and times reported. The reporting criteria can be combinations of the specific categories described in Section 14.2.6, "Custom Scans," on page 148.

1. In Novell Remote Manager, access the volume inventory for the shadow volume.

   For information, see Section 14.1, "Accessing the Volume Inventory," on page 133.
2. Scroll down to the **Custom Shadow Volume Options** area at the end of the shadow volume inventory.
3. In **Volume Operations**, select one of the following actions to perform on the files that meet the search criteria you specify for the scan in later steps.
   - List primary area selected files
   - Move selected files from primary area to shadow area.
   - List shadow area selected files.
   - Move selected files from shadow area to primary area.
4. In **Search Patterns**, specify wildcards and characters to select files by filename or extension. The default is *.*, which does not restrict the search to specific filenames or extensions; all files are considered.

5 (Optional) In **File Owner Restrictions**, select **None**, or select a user name from the drop-down list.

If **None** is selected, file ownership is not considered for the search. If a user name is specified, the search applies only to files where the file owner matches the specified owner.

6 (Optional) In **Time Stamp**, specify one or multiple time stamps to be searched. If none are selected, the time stamps are not considered when searching.

- Last Modified Time
- Last Accessed Time
- Last Changed Time

7 In **Range**, if you specified a time stamp restriction, specify one or multiple ranges to be searched:

- Within last day
- 1 day to 1 week
- 1 week to 2 weeks
- 2 weeks to 1 month
- 1 month to 2 months
- 2 months to 4 months
- 4 months to 6 months
- 6 months to 1 year
- 1 year to 2 years
- More than 2 years

8 (Optional) In **File Size Restrictions**, specify one or multiple file sizes to be searched.

- Less than 1 KB
- 1 KB to 4 KB
- 4 KB to 16 KB
- 16 KB to 64 KB
- 64 KB to 256 KB
- 256 KB to 1 MB
- 1 MB to 4 MB
- 4 MB to 16 MB
- 16 MB to 64 MB
- 64 MB to 256 MB
- More than 256 MB

9 After you specify the volume operation and search criteria, click **Start Scan**.

10 If you chose to list the files, an Inventory Detail report is generated where you can move, copy, or delete files.

10a Select one or multiple files in the list, then select one of the following actions:

- **Move the selected volumes to the other file tree.** (This option is available only for DST shadow volumes.)
- **Move the selected files to a specified path on the server.**
- **Copy the selected files to a specified path on the server.**
- **Delete the selected files.**

10b Click **OK** to confirm the action.

The action is performed on the selected files, then a confirmation list of the files and the number of files moved is displayed.

If you chose to move selected files from one volume to another, the files that meet the search criteria are automatically moved, then a confirmation list of the files and the number of entries moved is displayed.

If you view the inventory chart again after the move, you can see that the files that matched the specified criteria before the move are now reported on the other volume.

15 Troubleshooting for the NCP Server and NCP Volumes

This section describes issues and possible workarounds for NCP Server and NCP volumes on Open Enterprise Server (OES) 2015 SP1 servers.

15.1 Salvaging and Purging NSS Files or Folders

Description: The following warning message is logged in `ncpserv.log` during scan of deleted files and folders for salvage and purge operation. This is observed if OES 2015 SP1 or earlier, Client for Open Enterprise Server 2 SP4 IR6 or earlier, or Micro Focus iManager 2.7.7 or earlier is used for salvage and purge operation.

```
WARNING: X file(s) not listed for salvage/purge due to 64-bit inode/zid per legacy
NCP request from conn#6 addr=192.168.1.1 logged-inUserDN=.user.novell.TREE
```

Possible Cause: During the scan, one or more deleted files or folders with 64-bit ZID number is found. NCP server on OES 2015 SP1 and earlier supports salvage and purge on deleted files or folders with 32-bit ZID number and not on deleted files or folders with 64-bit ZID number.

Action: If you want to perform salvage and purge operation on 64-bit ZID files or folders, upgrade to OES 2018, Client for Open Enterprise Server 2 SP4 (IR7), and Micro Focus iManager 3.0.2.

15.2 Mismatching VOLUME IDs in NCS and NCP for the New Volumes Created in a Cluster Pool

Description: For a new volume created in a cluster pool, the volume ID displayed by running the command `ncpcon volume /v` may be different from the volume ID present in the cluster load script. This is an intermittent issue that impacts only the newly created volumes; existing volumes stay intact.

Possible Cause: NSS quickly notifies NCP about vol IDs than NCS.

Action: It is advisable for the administrator to proactively compare the vol IDs of the newly created volumes before provisioning them to the users. If there is a mismatch, take the cluster resource offline and online again.

15.3 NCP Clients Cannot Connect to the Server

If users cannot connect to the server, all the licensed user connections might be in use.

To resolve this problem, you can view and clear connections of users with active connections that are not logged in to the server. For information about clearing connections, see the following sections:

- Section 9.6, “Clearing Not-Logged-In Connections to NCP Server,” on page 76.
- Section 9.8, “Clearing Connections to NCP Server,” on page 79

15.4 ncpcon nss Command or ncpcon volume <volume_name> Output Reports Mounted NSS Volume as "not NSS"

Possible Cause: `ncpserv.conf` file has VOLUME entries for NSS volumes that makes NCP to treat the NSS volume as POSIX volumes and not NSS volumes.

Action: If the `/etc/opt/novell/ncpserv.conf` file contains VOLUME lines that refer to the existing NSS volumes, remove those lines. Save the changes and reboot.

15.5 Error 601 When Deleting an NCP Volume

If you attempt to create a volume at the command line by using the command syntax for creating an NCP volume inside a cluster load script (`ncpcon mount MYVOL=98@"/usr/novell/myvol"`), you get a -601 error when you remove the NCP volume. This error indicates that the Volume object cannot be removed. However, the volume was removed successfully. This is a cosmetic error that occurs because the wrong command was used to create the volume.

When the command is used inside of a load script, the Volume object is intentionally not re-created each time the load script runs, regardless of the node where the cluster resource is being loaded. The Volume object is associated with the virtual cluster server, not the server where it is currently loaded.

To avoid getting the -601 error, use the `ncpcon create volume` command to create NCP volumes at the command line, which automatically creates a Volume object in eDirectory.

15.6 Cross-Protocol Locking Stops Working

Cross-protocol locking allows Samba/CIFS users and NCP users to concurrently access files by allowing only one user at any time to open the file for write. Multiple users who are accessing via NCP and Samba/CIFS can open a file for read only.

WARNING: Allowing users who access files via different protocols to concurrently open a file for write can lead to data corruption.

If cross-protocol locking is enabled for NCP Server for Linux but stops working for DST shadow volume pairs—that is, multiple users can open a file for read and write—it is probably because ShadowFS needs to be restarted. To resolve this problem, stop the shadowfs process, then start shadowfs. For information, see "Starting and Stopping ShadowFS Manually" in the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

15.7 Error on Copying or Deleting Files When Extended Attributes Are Not Enabled

When copying or deleting files that have extended attributes, Novell Client displays the error `Not enough free disk space` or `Path cannot be found`. To resolve this issue, you must enable extended attributes on the file system:

1. Run the following command to verify if extended attributes are enabled on the file system:

   ```
   tune2fs -l Device |grep Default mount options
   ```

   If the value of `Default mount options` is None, enable extended attributes on the file system.

2. To enable extended attributes on the file system, run the following commands:

   ```
   tune2fs -o user_xattr Device
   ```

   ```
   mount -o remount Device
   ```

   When extended attributes are enabled, the value of `Default mount options` is `user_xattr`.

   The value of Device is the device or path where the file system is mounted. It can be found at `/etc/fstab`.

15.8 NCP Client Fails to Map a User's Home Directory

When you have a large number of trustees and folders at the directory level, mapping the home directory fails with an error.

To solve the issue, increase theNovell Storage Services (NSS) ID cache size to set the maximum number of entries for the NSS GUID to ID and ID to GUID cache.

For example:

`nsscon nss /IDCacheSize`=256000

Default: 16384

Range: 16384 to 524288

15.9 File Level Trustees Are Deleted When a File is Modified

File level trustees might be deleted when a file is modified, depending on how the application works with files it opens for writing. Some third-party applications record changes in a temporary file in order to save internal memory or as a safety net to prevent data loss due to a power failure, system crash, or human error. When a user saves the changes, the application deletes the original file, and saves the temporary file with same name as the original file. In response to the deletion instruction, the file system deletes the original file as well as any file level trustees set on the file. The file system is not application aware; that is, it does not track the ultimate intent of the applications that you might use.

For more information, see “File-Level Trustees” in the *OES 2015 SP1: File Systems Management Guide*.

16 Security Considerations for NCP Server

This section describes security issues and recommendations for NCP Server on an Open Enterprise Server (OES) 2015 SP1 server. It is intended for security administrators or anyone who is responsible for the security of the NCP Server for Linux system. It requires a basic understanding of NCP Server. It also requires the organizational authorization and the administrative rights to effect the configuration recommendations.

16.1 UDP Port 524

NCP Server uses UDP port 524 when mounting volumes with the `ncpmount(8)` command. NCP Server opens this port in the server firewall when it is installed.

16.2 Soft Links

Although NCP Server for Linux provides limited support for hardlinks, soft links are intentionally not supported. The following soft link features can be exploited to create security problems where users can give themselves access to subdirectories where they have no rights:

- The Linux POSIX permissions set on the soft link do not need to match the permissions set on the source file or directory.
- The soft link and source file are not restricted to paths on the same volume and file system.
- Soft links can link to files or directories.
- The name of the soft link does not need to match the name of the source file.

For example, directories on an NCP volume on Linux file systems can have different inherited rights, so the link can have different effective rights than the source. Security breaches can occur if someone accidentally creates a soft link to a sensitive area of the system, such as the /etc directory. A hacker can exploit the system by creating a soft link to a password file, then overwriting its contents. Soft links can cause security problems for programs that fail to consider the possibility that the file being opened may actually be a link to a different file. This is especially dangerous when the vulnerable program is running with elevated privileges.

16.3 Hard Links

NCP Server supports hardlinks for a file on an NCP volume (NCP share on a non-NSS file system) if the destination location for the hardlink is on the same NCP volume as the source file, and any of the following conditions is met:

- If the user is supervisor equivalent of the NCP volume, or
- If the user is the owner of the file, or
- If the "Other" Read/Write mode bits are set on the file on the non-NSS file system.

Other users are unable to open hard-linked files. This is because of a hard-link security problem where users can give themselves write access to files where they should only have read access.

For example, a user has world-readable access to /etc/fileA. The user creates a hardlink to /etc/fileA and specifies a destination for the link to be a directory on the same file system where the user has read/write access, such as the user's home directory. The user now has granted himself read/write access to fileA.

NCP Server supports hardlinks for a file on an NSS volume if the destination location for the hardlink is on the same NSS volume as the source file, and any of the following conditions is met:

- If the user is supervisor equivalent of the NSS volume, or
- If the user is the owner of the file.

In addition, the Hardlinks attribute must be enabled for the NSS volume to allow hardlinks support. The hardlinks can be in the same directory or in multiple directories in the same NSS volume. When hardlinks are used, the volume's users must be enabled with Linux User Management. The NSS file system is designed to provide secure support for hardlinks on NSS volumes. For information about how the hardlinks on an NSS volume work with file ownership, trustees, trustee rights, and inherited rights, see “Understanding Hard Links” in the OES 2015 SP1: NSS File System Administration Guide for Linux.

16.4 Log Files

The following log files are located in the `/var/opt/novell/log` directory:

- `ncpserv.log`
- `ncp2nss.log`
- `ncptop.log`
- `ncpcon.log`

Log files are managed by `logrotate`. For information on usage, see its man page (`man logrotate`).

The control files for `logrotate` are:

- `/etc/logrotate.d/novell-ncpserv-log`
- `/etc/logrotate.d/novell-ncpserv-audit`
- `/etc/logrotate.d/novell-ncp2nss-log`
- `/etc/logrotate.d/novell-ncp2nss-audit`

By default, the rollover size is 16 MB and 5 compressed copies are kept.

16.5 Audit Logs

The following audit log files are available:

- `/var/opt/novell/log/ncpserv.audit.log`
- `/var/opt/novell/log/ncp2nss.audit.log`
- `/usr/novell/sys/._NETWARE/SYS.audit.log`
- `/var/log/audit`

  By default, the NSS Auditing Client Logger (vlog) utility sends its output to stdout in an XML record format. The default log file location is `/var/log/audit`. You can use VLOG options to modify the output location and logging behavior. For information, see “VLOG Options“ in the OES 2015 SP1: NSS Auditing Client Logger (VLOG) Utility Reference.

A Commands and Utilities for NCP Server and NCP Volumes

This section describes commands and utilities for NCP Server services and NCP volumes on Open Enterprise Server (OES) 2015 SP1.

A.1 NCPCON

The NCP Server Console (`ncpcon(8)`) is a management utility for NCP Server on Open Enterprise Server 2015 SP1. The man page for NCPCON is located in the `/usr/share/man/man8` directory. To view the man page when you are at the server console, enter `man ncpcon` at the terminal console prompt.

- Section A.1.20, “Managing Dynamic Storage Technology,” on page 178
- Section A.1.21, “Managing Dynamic Storage Technology on Novell Cluster Services for Linux Clusters,” on page 182

A.1.1 Syntax

The NCPCON utility can be used in three modes:

- “Interactive Mode” on page 162
- “Command Line Mode” on page 162
- “Scripting Mode” on page 162

Interactive Mode

Open a terminal console, log in as the `root` user, then enter

```
ncpcon
```

This opens the NCPCON interactive console in the terminal console where you can enter the NCP Server console commands. Enter `exit` to stop the interactive mode.

Command Line Mode

For command line mode, issue an NCP Server command at a terminal console prompt by prefacing the command with `ncpcon`:

```
ncpcon [command]
```

For example:

```
ncpcon mount sys
```

Escaping the quote character is not required when entering the command from the NCPCON prompt or console command prompt. For example, the send command is entered as follows from the NCPCON prompt:

```
send "hello world" to all
```

For example, the send command is entered as follows from the console command prompt:

```
ncpcon send "hello world" to all
```

Scripting Mode

For scripting mode, if the file path or trustee name contains space, enclose them with double quotation marks:

```
ncpcon "[command]"
```

For example:

```
ncpcon rights add vol1:"dir 1/dir2" "test user.novell" rwcmef
ncpcon rights add "vol1:dir 1/dir2" "test user.novell" rwcmef
```

It's optional to use double quotation marks if the file path or trustee name does not contain space.

For example:

```
ncpcon rights add vol1:dir1/dir2 testuser.novell rwcmef
ncpcon rights add "vol1:dir1/dir2" "testuser.novell" rwcmef
```

A.1.2 Getting Help

`help [command]`

Use this command to list the `NCPCON` console commands. To get specific help for a command, type `help` and the command.

Examples

```
help
```

```
help mount
```

```
help remove volume
```

A.1.3 Starting and Stopping NCPCON Interactive Mode

`ncpcon`

Use this command to start the `NCPCON` interactive mode.

Example

```
ncpcon
```

`exit`

Use this command to exit the NCPCON application when you are in the interactive mode. The command is not used in the command line/scripting mode.

Example

```
exit
```

A.1.4 Monitoring NCP Server

Use the commands in this section to manage the NCP Server service on your OES server.

`config`

Displays the NCP Server configuration information such as the server name, server version, product version, NCP version, mixed-mode paths status (yes/no), and commit files status (yes/no).

Example

```
config
```

`stats`

Use this command to display NCP statistics, including the following:

- Server up time
- Packets in
- Packets dumped
- Packet receive buffer memory
- Packet reply buffer memory
- NCP requests

- NCP connections in use
- Connection table memory
- Mounted volumes
- Number of open files
- Local ID tracking
- File handle memory
- Volume `SYS:` file and subdirectory caching memory
- Volume `SYS:` trustee and inherited rights mask tracking memory

Example

```
stats
```

`version`

This command displays version information for all currently running Novell NCP Server components, the OES build, and the hardware platform.

Example

```
version
```

`set`

Use this command to view or set current NCP server system parameters.

Example

```
set
```

A.1.5 Managing NCP Server in a Cluster

NCPCON supports the `bind` and `unbind` commands for use with Novell Cluster Services for Linux on an OES 2015 SP1 server.

Use these commands in load or unload scripts when you want to configure the NCP access for files in a cluster resource that can be moved or failed over to another node in the cluster. NCP is required for NSS volumes, NCP volumes on Linux POSIX file systems, and Dynamic Storage Technology shadow volumes.

SLP must be configured on the server where the `bind` command is issued. When the SLP daemon (`slpd`) is not installed and running on a cluster node, any cluster resource that contains the `ncpcon bind` command goes comatose when it is migrated or failed over to the node because the bind cannot be executed without SLP. For more information on software requirements for SLP for cluster services, see "SLP" in the "OES 2015 SP1: Novell Cluster Services for Linux Administration Guide".

For information about configuring and managing Novell Cluster Services for Linux, see the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

`bind` ***`cluster_resource_name ip_address`***

Binds the specified cluster resource name. Use this command to assign an IP address to the NCP Server cluster resource name.

Example

```
bind oes_11_cluster 192.168.1.1
```

In a cluster load script, use the following syntax:

```
exit_on_error ncpcon bind --ncpservername=oes_11_cluster --
ipaddress=192.168.1.1
```

`unbind` ***`cluster_resource_name ip_address`***

Unbinds the specified cluster resource name. Use this command to remove the assignment of an IP address from the NCP Server cluster resource name.

Example

```
unbind oes_11_cluster 192.168.1.1
```

In a cluster unload script, use the following syntax:

```
ignore_error ncpcon unbind --ncpservername=oes_11_cluster --
ipaddress=192.168.1.1
```

A.1.6 Managing NCP Threads

Use the commands in this section to configure the number of concurrent NCP threads and to verify the current NCP utilization.

`ncpcon set ADDITIONAL_SSG_THREADS=<value>`

Sets the number of additional SSG threads (above the fixed 25 NCP threads) that can be used to serve incoming NCP file service requests. These threads are used when the fixed 25 NCP threads are busy and taking more than expected time to finish.

Default: 25. Valid Range: 7 to 103.

`ncpcon set CONCURRENT_ASYNC_REQUESTS=<value>`

Sets the maximum number of the Async eDirectory NCP request threads that can be created. Default: 25. Valid Range: 15 to 256.

`ncpcon threads`

Allows you to verify the current number of concurrent NCP threads running on the server. Use this command to verify the settings that you make for the `ADDITIONAL_SSG_THREADS` and `CONCURRENT_ASYNC_REQUESTS` settings.

Example - NCP SSG Thread Statistics

```
Total Number of Active SSG Threads: 13
Max Number of Additional SSG Threads (over and above fixed 25 NCP Threads): 12
Total Number of NCP Streams: 20
Current Average Load per Thread: 1.54
Peak Number of Active SSG Threads: 25
Peak Number of NCP Streams: 2148
Peak Average Load per Thread: 85.92
```

Total Number of Active SSG Threads: The currently active SSG threads.

Max Number of Additional SSG Threads (above the fixed 25 NCP threads): When all 25 fixed SSG threads are exhausted, this number defines the additional number of threads that can be created to serve other incoming NCP file service requests. This value can be modified by using the `ncpcon set ADDITIONAL_SSG_THREADS=value` command. Default=25. Valid Range: 7 to 103.

Total Number of NCP Streams: The current number of NCP connections that have been handled by the Active SSG threads.

Current Average Load per Thread: The current average load of NCP connections on the Active SSG threads.

Peak Number of Active SSG Threads: The highest number (peak) of the Active SSG threads.

Peak Number of NCP Streams: The highest number (peak) of NCP streams.

Peak Average Load per Thread: The highest number (peak) of streams per thread.

Example - Async (eDir) Threads and Requests Statistics

```
Number of Running Threads: 0
Max Thread Size: 25
Thread Peak Size: 25
Number of Queued Requests: 0
Queued Requests Peak Size: 174
```

Number of Running Threads: The currently running number of Async threads that can handle eDirectory requests.

Max Thread Size: The maximum number of the Async threads that can be created. This value can be modified by using the `ncpcon set CONCURRENT_ASYNC_REQUESTS=value` command. Default: 25. Valid Range: 15 to 256.

Thread Peak Size: The highest number (peak) of Async threads the server required so far. This number is reset when the service is restarted.

Number of Queued Requests: The number of queued eDirectory requests (after the Async threads are exhausted).

Queued Requests Peak Size: The highest number (peak) of eDirectory requests that have been queued so far (after the Async threads are exhausted).

A.1.7 Displaying NCP Volume Information

volumes

Use this command to print information about mounted volumes.

Examples:

```
ncpcon volumes
```

This command displays a list of currently mounted NCP volumes.

```
ncpcon volume volume_name
```

This command displays details of the specified volume.

```
ncpcon volumes /v
```

This command displays a list of currently mounted NCP volumes along with the NCP volume IDs.

```
ncpcon volumes /s
```

Displays volume size details.

A.1.8 Managing Audit Settings

ncpcon set AUDITING_SUPPORT=<value>

This parameter indicates whether auditing support is enabled for NCP. The default value is 0 and it indicates that auditing is turned off.

Default: 0. Valid Values: 0 and 1.

A.1.9 Managing Log Settings

ncpcon set LOG_LOCK_STATISTICS=<value>

When an NCP volume lock is held more than the configured time, NCP server displays a message in the `ncpserv.log` file with the relevant details.

Default: 0. Valid Values: 0 to 10000 msec.

A.1.10 Managing NCP Volumes

Use the commands in this section to create, manage, or remove NCP volumes for Ext3 and Reiser file systems on your OES 2015 SP1 Linux server. NCP volumes use the Novell Trustee Model for controlling user access to files. Users access the volume by using the Novell Client.

`change volume ncp_volname [option]`

Display the current volume options setting for the specified volume, or change the setting for a specified option on the specified volume. Issuing the command is a toggle for the setting, turning it on or off, depending on its current value.

You must dismount the volume before you can change its options settings with this command.

This command cannot be added to a cluster load script.

Option

`Inherit_POSIX_Permissions <on|off>`

This is disabled by default. When this setting is disabled, only the root user and the owner of the file can access the volume as local users in a Linux environment. Disabling the POSIX inheritance is the most secure setting because NCP volumes use the Novell Trustee Model for file system access control.

If this option is enabled on a volume, the POSIX permissions are permitted to be inherited from parent directories. If POSIX inheritance is enabled, local access in the Linux environment by users who are not authenticated via NetIQ eDirectory can create security problems.

Examples

To view the current setting, enter the following at the console command prompt:

```
ncpcon change volume sys
```

To enable Inherit POSIX Permissions on the `sys:` volume, start NCPCON by entering `ncpcon` at the console command prompt, then enter the following at the `ncpcon` prompt:

```
dismount sys

change volume sys Inherit_POSIX_Permissions on

mount sys

exit
```

`create volume` ***`ncp_volumename path`***

Use this command to create an NCP volume by defining an NCP share on an existing POSIX file system on your Linux server. This command creates a Volume object in NetIQ eDirectory, and associates the volume name to a path on your server when using file system types other than the Novell Storage Services (NSS) file system.

This command does not remove or delete data in the mount point location. It adds the NCP volume's volume name and mount information to the NCP Server configuration file `(/etc/opt/novell/ncpserv.conf`).

Replace *ncp_volumename* with the name for the volume.

Replace *path* with the path to an existing folder on the Linux server that is used as the mount point for the NCP volume. The folder must be on a Linux POSIX file system volume.

After creating the NCP volume, you must mount it to make it accessible to NCP clients.

Example

```
create volume vol1 /media/ncpvolumes/vol1
```

dismount <*ncp_volumename* | all>

Use this command to dismount a specified NCP volume on your Linux server, or to dismount all NCP volumes on your Linux server.

Examples

To dismount the NCP volume named `VOL1`, enter

```
dismount VOL1
```

To dismount all NCP volumes, enter

```
dismount all
```

mmount < all | volumename | volumename=volume_id,path=/volume_mntpoint >

Use this command to mount an NCP volume on your Linux server. This command makes the NCP volume accessible to NCP clients.

Replace *volumename* with the name of the volume, such as `VOL1`. To mount all volumes, replace the volume name with `all`.

Replace *volume_id* with a value from 0 to 254 as the server volume ID. It is not necessary to manually specify a volume ID for a locally mounted volume. NCP automatically assigns unique volume IDs to locally mounted NCP volumes and NSS volumes in increasing order, from 0 to 254. IDs 0 and 1 are reserved for the sys and _admin volumes. When the command is used in a cluster resource script, the volume ID must be specified to ensure that the volume ID is unique across all cluster nodes where the volume will be mounted. By convention in clusters, the volume IDs are assigned in decreasing order, from 254 to 0.

For an NCP volume created on a Linux POSIX file system, replace */volume_mntpoint* with the Linux path of the mount point for the NCP share. Typically, this path is mount point of the Linux volume; that is, the share is created at the root of the Linux volume.

If an NCP volume is mounted locally, the mount path is stored in the `/etc/fstab` file, so it is not necessary to specify a mount path. For example:

```
ncpcon mount VOL1
```

The mount path for the NCP volume is required in a cluster resource. For example, if you use NSSMU to create and NCP enable a clustered Linux LVM volume '`myvol`' with a mount point of `/usr/novell/myvol`, the NCP volume name (share name) is `MYVOL`, and the resource load script includes the following definitions for variables used in the command:

```
# define the mount point path of the Linux volume

MOUNT_PATH=/usr/novell/myvol

# define the NCP volume name

NCP_VOLUME=MYVOL

exit_on_error ncpcon mount $NCP_VOL=253,path=$MOUNT_PATH
```

For an NSS volume, the default mount path is `/media/nss/<nss_volume_name>`. For example, if you create a volume named USERS, the default mount path is `/media/nss/USERS`. If you use the default path for NSS volumes, it is not necessary to include the path option for local mounts:

```
ncpcon mount USERS
```

A volume ID must be specified in a cluster load script:

```
exit_on_error ncpcon mount USERS=252
```

In a cluster, you cannot rename the mount point path. The default mount point path of `/media/nss/<volume_name>` applies.

```
exit_on_error ncpcon mount volumename=volume_ID
```

For example:

```
exit_on_error ncpcon mount USERS=252
```

The volume is mounted at `/media/nss/USERS`.

remove volume *ncp_volumename*

Use this command to remove the NCP volume and path association. This command does not remove or delete data from the mount location. This command removes the NCP volume mount information from `/etc/opt/novell/ncpserv.conf` configuration file.

Example

```
remove volume VOL1
```

volumeS, volume *volumename*

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.

Examples

```
volumes
```

```
volume VOL1
```

volume data

Displays a list of currently mounted NCP volumes and information about them. For example, if the volume is a Dynamic Storage Technology shadow volume pair, it identifies the Linux paths of its primary and secondary volumes.

Example

```
volume data
```

disable write <*volume name*>

[Broadcast message]

This command disables write permission on files in the specified volume. The broadcast message is optional, but if any message is sent to all the clients accessing the specified volume.

NOTE: Executing this command closes any files that are opened for writing.

Example

```
disable write VOL1 Closing all open files on this volume.
```

enable write <*volume name*>

[Broadcast message]

Use this command to enable write permissions on a volume that has been previously disabled for writing by using the `disable write` command.

The broadcast message is optional, but if any message is sent to all the clients accessing the specified volume.

Example

```
enable write VOL1 Files on this volume can now be edited.
```

A.1.11 Managing File System Trustees and Trustee Rights for NCP Volumes

Use the commands in this section to manage file system trustees and trustee rights for NCP volumes for Linux POSIX file systems on your OES 2015 SP1 server. NCP volumes use the Novell Trustee Model for controlling user access to files.

`rights <view` ***`path`*** **`|`** **`add`** ***`path fdn options`*** **`|`** **`remove`** ***`path fdn`*** **`>`**

Allows you to view, add, or remove trustees and trustee rights for a specified path. Replace *fdn* with the typeless fully distinguished name (username.context) of the trustee, such as bob.example. Replace *`options`* with all, none, or the combination of rights to assign for the specified trustee. List the rights together without spaces or commas, such as RF. If the file path or trustee names contain spaces, ensure to enclose them within double or single quotes. For visibility, users need the Read and File Scan rights.

Options

all

All rights

none

No rights

S

Supervisor

R

Read

W

Write

C

Create

E

Erase

M

Modify

F

File scan

A

Access control

Examples

```
rights view sys:login
```

```
rights view "vol1:login dir1/dir2"
```

```
rights view "vol1:/login/dir 1/", rights view 'vol1:/login/dir 1/'
```

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

```
rights add "vol1:dir 1" bob.example RF
```

```
rights add "vol1:dir1" "bob christo.example" RF
```

```
rights add "vol1:dir 1" "bob christo.example" RF, rights add 'vol1:dir 1' 'bob
christo.example' RF
```

```
rights remove users:bob bob:example
```

```
rights remove "vol1:dir 1" bob.example
```

```
rights remove vol1:dir1 "bob christo.example"
```

```
rights remove "vol1:dir 1" "bob christo.example", rights remove 'vol1:dir 1'
'bob christo.example'
```

`irm <view` ***`path`*** **`|`** **`set`** ***`path mask`*** **`>`**

Displays or sets the inherited rights mask on the specified path. Specify both the NCP volume and directory in the NetWare path format, such as `volname:dir1/dir2`. Replace *`mask`* with the mask options all, none, or the combination of rights to block from being inherited. List the rights together without spaces or commas, such as SAE. If the file path or trustee names contain spaces, ensure to enclose them within double or single quotes.

MASK OPTIONS

all

All rights

none

No rights

S

Supervisor

R

Read

W

Write

C

Create

E

Erase

M

Modify

F

File scan

A

Access control

Examples

```
irm view sys:login
```

```
irm view "vol1:login dir1/dir2"
```

```
irm view "vol1:/login/dir 1/", irm view 'vol1:/login/dir 1/'
```

```
irm set vol1: SA
```

```
irm set vol1:dir1 RF
```

```
irm set "vol1:dir 1/dir 2" RF, irm set 'vol1:dir 1/dir 2' RF
```

A.1.12 Managing NSS Volumes in a Cluster

Use the following load script to mount NSS volumes in a cluster resource.

```
ncpcon mount <VOLUMENAME>=<VOLUMEID>
ncpcon mount /opt=ns=LONG <VOLUMENAME>=<VOLUMEID>
ncpcon mount /opt=ns=UNIX <VOLUMENAME>=<VOLUMEID>
```

A.1.13 Renaming a Mount Point Path for a Clustered NSS Volume

You can modify the load and unload scripts to specify a non-standard mountpoint path for a clustered NSS volume. It requires using Linux commands in the scripts. For instructions, see: Renaming the Mount Point Path for a Clustered NSS Volume.

A.1.14 Managing TCP Connections

This parameter allows you to configure the keep-alive timeout for all the TCP client connections accepted by the NCP server. Based on this parameter, the TCP keep-alive packet is sent by the server if the client is inactive for the configured amount of time.

This parameter also helps the NCP server to clear unwanted connections. The actual time taken to clear the unwanted NCP connections also depends on other system-wide TCP keep-alive parameters, like `net.ipv4.tcp_keepalive_probes` and `net.ipv4.tcp_keepalive_intv`.These parameters can be controlled using the `sysctl` command.

```
ncpcon set NCP_TCP_KEEPALIVE_INTERVAL=<value>
```

Default: 8 minutes. Valid Range: 3 minutes to 240 minutes.

A.1.15 Purging Deleted Files on NSS Volumes on Linux

`purge volume` ***`nss_volumename`***

Use this command to purge or permanently remove deleted files from an NSS volume on Linux. This command works only with NSS volumes where the Salvage attribute has been previously enabled.

Example

```
purge volume vol1
```

A.1.16 Managing User Login

Use the commands in this section to enable or disable login for NCP clients to the Linux server.

`disable login`

Use this command to prevent NCP clients from logging in to the Linux server.

Example

```
disable login
```

`enable login`

Use this command to allow NCP clients to log in to the Linux server.

Example

```
enable login
```

A.1.17 Sending Messages to Logged-In Users

`send "`*`text_message`*`" to <`*`station`*` | `*`station1,station2`*`... | all>`

Use this command to send a message to logged-in NCP clients. Replace *text_message* with a message of up to 252 characters and spaces. Specify multiple logged-in stations by separating the connection numbers with commas and no spaces. Specify **all** to send the message to all logged-in users.

To find the connection number assigned to a user's connection, use the `connection` commands in Section A.1.18, "Managing NCP Server Connections," on page 173.

Example

To issue the command at the ncpcon prompt:

```
send "Hello, world" to 1
send "Hello, world" to 1,2,4
send "Hello, world" to all
```

To issue the command at the terminal console prompt:

```
ncpcon send "Hello, world" to 1
ncpcon send "Hello, world" to 1,2,4
ncpcon send "Hello, world" to all
```

A.1.18 Managing NCP Server Connections

Use the `connection` commands in this section to display the NCP Server connection information for all current connections, or for a given connection. You can also display a list of the connections and clear the connections. The general syntax is:

```
connection [list | connection_number | clear connection_number | clearALL except
connection_number]
```

`connection`

Displays an overview of current NCP Server connection information.

Parameter	Description
Connection Slots Allocated	Displays the number of slots currently allocated for use. As connection slots are required on this server that exceed the current number of slots displayed here, new slots are allocated. Depending on the server's memory, connection slots are usually allocated in blocks of 16. Connection slots are allocated as needed by users and other services.
Connection Slots Being Used	Displays the number of connection slots currently in use. As this number matches or exceeds the Connection Slots Allocated entry, more connection slots are allocated to the connection table.
Signing Level	Displays the level at which NCP packet signature signing is set on the server. NCP packet signatures prevent packet forgery by requiring the server and the workstation to sign each NCP packet. A higher packet signature number impacts the performance of your server. At some point, the need for security might outweigh certain performance issues.
Login State	Displays whether users are allowed to log in to the server. To disable users from being able to log in to the server (for server maintenance or other reasons), enter `disable login` at the NCPCON prompt, or enter `ncpcon disable login` at a terminal console prompt. To allow users to log in to the server, enter `enable login` at the NCPCON prompt, or enter `ncpcon enable login` at a terminal console prompt.
Licensed Connections	Displays the number of connections that are currently licensed. Licensed connections are authenticated, logged in, and consume a license. An unlicensed connection does not consume a license and can be authenticated or not. An unlicensed, authenticated connection can access the eDirectory database but cannot access any other resources.
Not Logged In Connections	Clears all user connections that are open, but not currently authenticated to the server. Use this parameter to clear all user that are not logged in.

Example

```
connection
```

`connection list`

Displays a list of all current NCP Server connections.

Parameter	Description
Station	Shows the connection number for each connection. Connection 0 is the connection used by the server. The server's operating system uses connection numbers to control each station's communication with other stations. Remote Manager does not distinguish connections that don't count against the server's connection limit.
Login Time	Shows the login day, date, and time for the connection.
Reads & Writes	Shows the number of reads and writes (in bytes) made by the connection.

Parameter	Description
Requests	Shows the number of NCP requests made by the connection.
Name	Shows the name of the user, server, service, or login status and links to specific information about that user connection such as the login time, connection number, network address, login status, number of NCP requests, files in use, and security equivalence. Connections with an asterisk (*) displayed next to the name indicate an unlicensed connection (it does not consume a license). These licenses can be either authenticated or not authenticated. An unlicensed, authenticated connection can access the NetIQ eDirectory database but not other server resources. From this detailed Connection Information page, you can also clear the connection or send a message to the user.

Example

```
connection list

... Executing "connections list"

                            "Active NCP Connections"
                                  Bytes     Bytes
Station  "Login Time"             Read      Written   Requests Name
 ...
*4       Sep 02 2014 02:56:18 pm  0         0         3
.CN=ncpuser0001.O=novell.T=PRA-LM-OES2015-TREE.
 5       Sep 02 2014 02:56:18 pm  2098177000 1049601000 58856
.CN=ncpuser0001.O=novell.T=PRA-LM-OES2015-TREE.
 6       Not Available            0         0         1        NOT LOGGED IN
 ...

... completed OK [elapsed time = 5 msecs 250 usecs]
```

connection list /h

The switch /h interprets the number of bytes read or written in human readable format, that is, KB/MB/GB based on the size.

Examples

```
connection list /h

... Executing "connections list /h"

                            "Active NCP Connections"
                                  Bytes     Bytes
Station  "Login Time"             Read      Written   Requests Name
...
*4       Sep 02 2014 02:56:18 pm  0         0         3
.CN=ncpuser0001.O=novell.T=PRA-LM-OES2015-TREE.
 5       Sep 02 2014 02:56:18 pm  1.95GB    1000.97MB 58856
.CN=ncpuser0001.O=novell.T=PRA-LM-OES2015-TREE.
 6       Not Available            0         0         1        NOT LOGGED IN
...

... completed OK [elapsed time = 3 msecs 526 usecs]
```

`connection` *`connection_number`*

Displays detailed information about a specified NCP Server connection. Replace *connection_number* with the station of interest. You can find the station's connection number from the report displayed by issuing the `connection list` command.

Parameter	Description
Connection Number	The station number for the connection.
Name	Shows the eDirectory context of the logged in user.
Login Time	Shows the login day, date, and time for the connection.
Network Address	Shows the IP address where the connection originates.
Status	Shows whether the connection is Authenticated or Not Logged In.
Privileges	Shows whether the connection has privileges, such as Supervisor or Console Operator.
Security Equivalence	Shows the name of the user, server, or service if it is logged in.
Open Files	Shows the files open for the connection.

Example

```
connection 1
```

`connection clear` *`connection_number`*

Clears the NCP Server connection for a specified station. Replace *connection_number* with the station of interest. You can find the station's connection number from the report displayed by issuing the `connection list` command.

Example

```
connection clear 1
```

connection clearALL, connection clearALL except <connection_number>

These parameters help the NCP server to clear all user connections that are open. You can optionally specify connection numbers that you do not want to close in the exception list. NCP server exempts those connections from closing. Specify multiple connection numbers by separating them with commas.

clearALL except <connection_number>

This command will clear all connections except:

1. Connections that are mentioned in the exception list.
2. NCP server object connections.
3. Not Logged In connections (User connections that are open, but not currently authenticated to the server).

Even if you clear user connections using this command, connections get reestablished automatically. To use this command effectively, first disable users from being able to log in to the server, enter `disable login` at the NCPCON prompt, or enter `ncpcon disable login` at a terminal console prompt.

IMPORTANT: Use this command prudently. Otherwise, it might lead to unexpected complications.

Examples

To issue the command at the NCPCON prompt:

```
connection clearALL
connection clearALL except 1
connection clearALL except 1,2
```

To issue the command at a terminal console prompt:

```
ncpcon connection clearALL
ncpcon connection clearALL except 1
ncpcon connection clearALL except 1,2
```

A.1.19 Viewing or Closing Open Files

`files operation <v=`*`volumename`*` | f=`*`filename`*` | c=`*`connection_number`*`>`

Use this command to list or close open files on an NCP volume by volume, filename, or connection number. If the file path or trustee names contain spaces, ensure to enclose them within double or single quotes.

To find the connection number assigned to a user's connection, use the `connection` commands in Section A.1.18, "Managing NCP Server Connections," on page 173.

Operation Options

`list`

Lists the open files for a specified NCP volume by volume, filename, or connection number.

`close`

Closes the open files for a specified NCP volume by volume, filename, or connection number.

Options

`v=`*`volumename`*

Replaces *volumename* with the name of the NCP volume.

`f=`*`filename`*

Replaces *filename* with path on the Linux file system of the file you want to close, such as `/usr/novell/sys/filename.ext`.

`c=`*`connection_number`*

Replaces *connection_number* with the station number of the connection whose open files you want to close.

Examples

```
files list v=sys

files list f=/usr/novell/sys/test.txt

files list "f=/usr/bob christo/novell/sys/test.txt"

files list c=9

files close v=sys

files close f=/usr/novell/sys/test.txt

files close 'f=/usr/bob christo/novell/sys/test.txt'

files close c=9
```

A.1.20 Managing Dynamic Storage Technology

NCPCON supports the commands in this section for use with Novell Dynamic Storage Technology. For information about configuring and managing shadow volumes and file systems, see the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

`create shadow_volume <primary_volumename> <shadow_path>`

Creates a non-clustered shadow association between a primary NSS volume and secondary NSS volume, and adds the `SHADOW_VOLUME` mount information to the `/etc/opt/novell/ncpserv.conf` file. If the file path or trustee names contain spaces, ensure to enclose them within double or single quotes.

When you issue the command from the NCP Console, you do not need to restart `ndsd` in order for the changes to take effect. When you issue the command from a Linux prompt, you must restart `ndsd` in order for the changes to take effect.

Options

primary_volumename

Specifies the volume name for the primary NSS volume, such as `VOL1`.

shadow_path

Specifies the Linux path of the mount location for the secondary NSS volume, such as `/media/nss/ARCVOL1`.

Examples

```
create shadow_volume VOL1 /home/shadows/VOL1
```

Creates a shadow volume where `VOL1` is the primary storage area and `/home/shadows/VOL1` is its mount point as a shadow volume.

```
create shadow_volume VOL1 "/home/bob christo/shadows/VOL1", create
shadow_volume VOL1 '/home/bob christo/shadows/VOL1'
```

Creates a shadow volume where VOL1 is the primary storage area and `/home/bob christo/shadows/VOL1` is its mount point as a shadow volume.

`remove shadow_volume [/l] [/i] [/f] <primary_volumename>`

Removes the non-clustered shadow relationship between a primary NSS volume and a secondary NSS volume, and removes the `SHADOW_VOLUME` command from the `/etc/opt/novell/ncpserv.conf` file. You must unmount the volume before you issue the command.

IMPORTANT: You can use this command as part of the process to unlink the primary and secondary volumes of a non-clustered DST shadow volume. For information, see "Removing the Shadow Relationship for a Non-Clustered DST Shadow Volume" in the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

Typically, you specify the `/l` option, which leaves the files in place on the primary volume and secondary volume, and removes the shadow relationship. This is equivalent to the **Volume Tasks > Remove Shadow Action Options > Remove Shadow** option in Novell Remote Manager.

When the `/l` option is not used, the command attempts to move all files on the secondary volume to the primary volume, and then removes the shadow relationship between the two volumes. Ensure that the primary volume has sufficient space to accommodate the files before you unmount the volume and issue the remove command. Moving the files can take some time, depending on how much data must be moved. If a file move fails, the unlinking of the shadow relationship also fails. You can use the `/i` option to ignore file move errors and allow the unlinking to succeed. After the files on the secondary volume have been moved to the primary volume, the shadow relationship is removed, and a summary report is created and displayed.

Options

primary_volumename

Specifies the volume name for the primary NSS volume, such as `VOL1`.

/l

Leaves the files in place on the two volumes and removes the shadow relationship.

/i

Ignores any file move errors that might occur if you issue the command without the `/l` option, and allows the unlinking of the shadow relationship to succeed.

For example, if there are duplicate files on the volumes, the duplicate instance on the secondary volume cannot be moved to the primary volume, and the shadow relationship cannot be unlinked. Using the `/i` option ignores the file move error and allows the relationship to be unlinked.

/f

Provides a full detail report of actions taken. Use this option to understand which file moves might be failing.

Examples

Issue the following commands from the NCP Console, or add `ncpcon` at the beginning of the command when issuing it from a script or at a terminal console prompt.

```
ncpcon remove shadow_volume /i /f VOL1
```

Removes the shadow relationship for shadow volume `VOL1`, and moves all files from the secondary storage area to the primary storage area. You must dismount `VOL1` before you issue this command. File move errors are ignored. Full details of the actions taken are reported.

```
remove shadow_volume /l VOL1
```

Removes the shadow relationship for shadow volume `VOL1`, and leaves files where they currently are on the secondary storage area and the primary storage area. You must dismount `VOL1` before you issue this command.

`shadow` ***`volumename`*** **`operation=<lp | ls | mp | ms> [options]`**

Allows you to list files on the shadow volume, or to move files between the primary storage area and the secondary storage area based on specified criteria. All files on the selected shadow volume that match the criteria are moved. Use the command from within cron jobs to automate data partitioning. If the file path or trustee names contain spaces, ensure to enclose them within double or single quotes.

Operation Options

lp

Lists primary files. Lists all files currently residing on the primary storage area.

ls

Lists shadow files. Lists all files currently residing on the secondary storage area.

mp

Moves files to primary. Moves files that match the specified criteria to the primary storage area from the secondary storage area.

ms

Moves files to shadow. Moves files that match the specified criteria to the secondary storage area from the primary storage area.

Operations

`pattern="`*`searchPattern`*`"`

Specifies the file pattern to match against.

`owner="`*`username.context`*`"`

Specifies the NetIQ eDirectory username and context of the owner of the files to match against.

`uid=`*`uidValue`*

Specifies the Linux user ID to match against.

`time=[time_field]`

Specifies which time field to match against, where the *time_field* is:

```
[m][a][c]
```

- **m:** Last time modified (content)
- **a:** Last time accessed
- **c:** Last time changed (metadata)

`range=[`*`time_period`*`]`

Specifies which time period to match against, where the *time_period* is:

```
[a][b][c][d][e][f][g][h][i][j]
```

- **a:** Within last day
- **b:** 1 day to 1 week
- **c:** 1 week to 2 weeks
- **d:** 2 weeks to 1 month
- **e:** 1 month to 2 months
- **f:** 2 months to 4 months
- **g:** 4 months to 6 months
- **h:** 6 months to 1 year
- **i:** 1 year to 2 years
- **j:** More than 2 years

`size=[`*`size_differential`*`]`

Specifies the size differential to match against, where the *size_differential* is:

```
[a][b][c][d][e][f][g][h][i][j][k]
```

- **a:** Less than 1 KB
- **b:** 1 KB to 4 KB
- **c:** 4 KB to 16 KB
- **d:** 16 KB to 64 KB
- **e:** 64 KB to 256 KB
- **f:** 256 KB to 1 MB
- **g:** 1 MB to 4 MB
- **h:** 4 MB to 16 MB
- **i:** 16 MB to 64 MB
- **j:** 64 MB to 256 MB
- **k:** More than 256 MB

`output="`*`filename`*`"`

Output the search results to the specified file.

Examples

`shadow vol1 operation=ls pattern="*.exe"`

Lists all files of type EXE that currently reside on the secondary storage area for the shadow volume `vol1`.

`shadow vol1 operation=lp size=g`

Lists all files of sizes between 1 MB to 4 MB that currently reside on the primary storage area for the shadow volume `vol1`.

`shadow vol1 operation=ms range=j`

Moves all files on the primary storage area that have not been modified, accessed, or changed in more than 2 years from the primary storage area to the secondary storage area for the shadow volume `vol1`.

`shift "`*`volumename:\path\filename`*`" [primary | shadow]`

Returns the specified file's location as being on the primary storage area or secondary storage area. Specify the primary or secondary options to move the specified file from its current location to the specified storage area.

The `shift` command works only at the command line, and not in ncpcon interactive mode. Enter the command as the root user at a terminal console prompt.

```
ncpcon shift "volumename:\path\filename" [primary | shadow]
```

OPTIONS

primary

Moves the specified file from the secondary storage area to the primary storage area. The file must be closed when you issue the command; otherwise, the command fails.

shadow

Moves the specified file from the primary storage area to the secondary storage area. The file must be closed when you issue the command; otherwise, the command fails.

Examples

Enter the commands as the root user at a terminal console prompt.

`ncpcon shift VOL1: "path\textfile.txt"`

Shows the specified file's storage area location in the shadow volume as primary (the primary storage area) or shadow (the secondary storage area) for the shadow volume `sys`.

`ncpcon shift "vol1:\usr\bob christo\textfile.txt"`, `ncpcon shift 'vol1:\usr\bob christo\textfile.txt'`

Shows the specified file's storage area location in the shadow volume as primary (the primary storage area) or shadow (the secondary storage area) for the shadow volume vol1.

`ncpcon shift VOL1: "path\textfile.txt" primary`

Moves the specified file's storage area location from the secondary storage area to the primary storage area for the shadow volume `sys`.

`ncpcon shift "vol1:\usr\bob christo\textfile.txt" primary`, `ncpcon shift 'vol1:\usr\bob christo\textfile.txt' primary`

Moves the specified file's storage area location from the secondary storage area to the primary storage area for the shadow volume vol1.

```
ncpcon shift VOL1: "path\textfile.txt" shadow
```

Moves the specified file’s storage area location from the primary storage area to the secondary storage area for the shadow volume `sys`.

```
ncpcon shift "vol1:\usr\bob christo\textfile.txt" shadow, ncpcon shift 'vol1:\usr\bob christo\textfile.txt' shadow
```

Moves the specified file’s storage area location from the primary storage area to the secondary storage area for the shadow volume vol1.

A.1.21 Managing Dynamic Storage Technology on Novell Cluster Services for Linux Clusters

NCPCON supports the commands in this section for use with Novell Dynamic Storage Technology in combination with Novell Cluster Services for Linux clusters. For information about configuring and managing shadow volumes and file systems in a cluster, see the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

Use the following syntax in cluster load scripts to mount the volume in a cluster. With clustering, no changes are needed to the `ncpserv.conf` file for shadowing. The primary volume information is also not added to the `ncpserv.conf` file.

Scenario 1: Primary NSS and Shadow NSS

```
ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename
```

Use this command in a cluster load script when the primary volume is an NSS volume and the secondary volume is an NSS volume. Both NSS volumes must already exist and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

Example

```
ncpcon mount VOL1=254,SHADOWVOLUME=ARCHIVE1
```

Mounts the NSS volume named `VOL1` with a volume ID of 254. The primary volume is an existing NSS volume named VOL1 (`/media/nss/VOL1`). The secondary volume is an existing NSS volume named ARCHIVE1 (`/media/nss/ARCHIVE1`).

Scenario 2: Primary Non-NSS and Shadow Non-NSS (Not Supported)

```
ncpcon mount volumename=volID,SHADOWPATH=shadowpath,path=primarypath
```

Use this command when the primary volume is a non-NSS volume and the secondary volume is a non-NSS volume.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

Example

```
ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARCHIVE1,path=/media/ncpvolumes/VOL1
```

Mounts the NCP volume named `VOL1` with a volume ID of 254. The primary volume’s path is `/media/ncpvolumes/VOL1`. The secondary volume’s path is `/media/ncpvolumes/ARCHIVE1`.

Scenario 3: Primary Non-NSS and Shadow NSS (Not Supported)

ncpcon mount *volumename*=*volID*,SHADOWVOLUME=*shadow_volumename*,path=*primarypath*

Use this command when the primary volume is a non-NSS volume and the secondary volume is an NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

Example

```
ncpcon mount VOL1=254,SHADOWVOLUME=ARCHIVE1,path=/media/ncpvolumes/VOL1
```

Mounts the NCP volume named `VOL1` with a volume ID of 254. The primary volume's path is `/media/ncpvolumes/VOL1`. The secondary volume is an existing NSS volume named ARCHIVE1 (mounted at `/media/nss/ARCHIVE1`).

Scenario 4: Primary NSS and Shadow Non-NSS (Not Supported)

ncpcon mount *volumename*=*volID*,SHADOWPATH=*shadowpath*

Use this command when the primary volume is an NSS volume and the secondary volume is a non-NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

Example

```
ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARCHIVE1
```

Mounts an NSS volume named `VOL1` with a volume ID of 254. The primary volume is an existing NSS volume named VOL1 (`/media/nss/VOL1`). The secondary volume is an NCP volume named ARCHIVE1 that is mounted at `/media/ncpvolumes/ARCHIVE1`.

Managing Quotas for Dynamic Storage Technology Volumes

NCPCON supports the ncpcon quotas command for Novell Dynamic Storage Technology volume pairs. For information, see the OES 2015 SP1: Dynamic Storage Technology Administration Guide.

You can run NCPCON console commands without entering the console by prefacing the command with `ncpcon`.

quotas help

Displays command help at the command prompt.

quotas view <*nss_volume_name*> <d|u> [c]

Shows the assigned NSS directory quotas or user quotas for a specified NSS volume that is used in a DST volume pair. Replace *nss_volume_name* with the name (such as VOL1) of the primary volume or the secondary volume.

Specify either directory (`d`) or user (`u`) after the volume name to indicate the type of quotas to display. You can use the combined (`c`) option to display the specified type of quotas for both volumes.

Options

c

(Optional) Shows a combined view for the specified type of quotas on the primary volume and secondary volume of a DST shadow volume pair.

d

Applies the operation to NSS directory quotas.

u

Applies the operation to NSS user quotas.

Examples

`ncpcon quotas view VOL_D u`

Shows the user quotas for NSS volume `VOL_D`. `VOL_D` can be the primary volume or secondary volume in a DST shadow volume pair.

`ncpcon quotas view VOL1 d C`

Shows a combined view of the directory quotas on the primary volume and secondary volume of a specified DST shadow volume.

quotas sync <ALL|MISSING|PERCENT> <*nss_volume_name*> [*percent_value*] <d|u> [q]

Synchronizes the NSS directory quotas or user quotas from the primary volume to the secondary volume of a DST shadow volume pair. Replace *nss_volume_name* with the name (such as VOL1) of the primary volume.

You can specify to use the same settings, or specify a percentage to set smaller or larger quotas on the secondary volume. You can duplicate all settings, or duplicate settings only where they do not exist.

Specify either directory (`d`) or user (`u`) after the volume name to indicate the type of quotas to synchronize.

Operations

ALL

For all of the directory quotas or user quotas (whichever type is specified) that are currently set on the primary volume, duplicates the quotas settings on the secondary volume.

MISSING

For each of the directory quotas or user quotas (whichever type is specified) that are currently set on the primary volume, if a quota is not set on the secondary volume, duplicates the quota setting on the secondary volume. This option does not overwrite existing quotas on the secondary volume.

PERCENT

For each of the directory quotas or user quotas (whichever type is specified) that are currently set on the primary volume, sets the quotas settings on the secondary volume as a specified percentage of the quota that exists on the primary volume. The percentage value must also be specified after the volume name.

A percent value of 100 is a one-to-one quota assignment. A percent value of 50 assigns a quota that is one-half the size of the quota set on the primary volume. A percent value of 200 assigns a quota that is twice the size of the quota set on the primary volume.

Options

d

Applies the operation to NSS directory quotas.

u

Applies the operation to NSS user quotas.

percent_value

Required if the PERCENT operation is used. Specifies the value to use when calculating the quota for the secondary volume based on a percentage of the primary volume's quota.

q

(Optional) Indicates quiet mode. No output appears in the execution window.

Examples

```
ncpcon quotas sync ALL VOL_D u
```

For all of the NSS user quotas that are currently set on the primary volume VOL D, duplicates the quotas setting on the secondary volume of a DST shadow volume pair.

```
ncpcon quotas sync PERCENT VOL1 50 d
```

For each of the NSS directory quotas that are currently set on the primary volume `VOL1`, sets a quota that is one-half that size on the secondary volume of a DST shadow volume pair.

```
ncpcon quotas sync MISSING VOL1 u
```

For each of the NSS user quotas that are currently set on the primary volume `VOL1`, if a quota does not exist on the secondary volume, duplicates the quota setting on the secondary volume of a DST shadow volume pair.

A.2 NCPCON SET Parameters

NCPCON provides several `SET` parameters that can be used to customize your NCP Server configuration. The parameters can be changed by entering `set` *`parameter_name`* while in the NCPCON utility. You can also enter `ncpcon set` *`parameter_name`* at the Linux command line.

The following sections identify the global NCP Server parameters with their default values and valid options:

- Section A.2.1, "Directory Cache Management for NCP Server," on page 186
- Section A.2.2, "Dynamic Storage Technology for NCP Server," on page 187
- Section A.2.3, "Locks Management for File Access on NCP Server," on page 188
- Section A.2.4, "Logs of NCP Server Events," on page 189
- Section A.2.5, "NCP Communications," on page 190
- Section A.2.6, "NCP Server Environment," on page 190
- Section A.2.7, "NCP Volumes," on page 191
- Section A.2.8, "NCP Volumes Low-Space Warning," on page 192
- Section A.2.9, "Enabling or Disabling UID Updates," on page 192
- Section A.2.10, "Enabling or Disabling Logging eDirectory Object Rename or Delete Events," on page 193
- Section A.2.11, "Augmented Size of NCP Verbs 87_20 and 89_20 Replies," on page 194

A.2.1 Directory Cache Management for NCP Server

Parameter Name and Description	Default Value	Value Options
MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY Controls the maximum number of file entries that can be cached by the system for a given folder in the directory cache. The NCP engine attempts to cache all files in a subdirectory for better performance, but sometimes memory is insufficient, so the NCP engine handles instances where only some of the file metadata is cached. Changing this parameter might improve or worsen performance, depending on your usage patterns.	10240	Minimum is 512 files.
MAXIMUM_CACHED_FILES_PER_VOLUME Controls the maximum number of file entries that can be cached by the system for a given volume in the directory cache. The NCP engine attempts to cache as many files as possible for better performance, but sometimes memory is insufficient, so the NCP engine handles instances where only some of the file metadata is cached. Changing this parameter might improve or worsen performance, depending on your usage patterns.	256000	Minimum is 2048 files.
MAXIMUM_LAZY_CLOSE_FILES Controls the maximum number of file handles that can be lazy closed in the directory cache. When the NCP engine opens files for a client, it manages one Linux file handle for each file that is opened, regardless of how many clients open the same file. When a file is closed by the client, the NCP engine waits before closing the file just in case a client wants to reopen the file. This is called a “lazy close.” This parameter controls how many files can be in a lazy close state at one time. If the configured maximum lazy close files number has been reached, the files that are closed by a client also have their Linux file handles immediately closed. Linux limits how many file handles can be in use at one time (64,000), so setting this number too high can have negative consequences.	4096	16 to 64000
MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME Controls the maximum number of folder entries that can be cached by the system for a volume in the directory cache.	102400	4096
LOG_CACHE_STATISTICS Controls whether cache statistics are logged in the `ncpserv.log` file.	0	0 - Disable 1 - Enable

A.2.2 Dynamic Storage Technology for NCP Server

For information about configuring global policies for DST, see the *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.

Parameter Name and Description	Default Value	Value Options
DUPLICATE_SHADOW_FILE_ACTION Controls how duplicate files conflicts are handled.	0	0 - Show duplicate shadow files (default) 1 - Hide duplicate shadow files 2 - Rename duplicate shadow files 3 - Delete duplicate files from shadow area 4 - Move duplicate shadow files to `/._DUPLICATE_FILES`
DUPLICATE_SHADOW_FILE_BROADCAST Controls whether broadcast messages are sent to NCP users whenever duplicate files conflicts occur.	1	0 - Disable 1 - Enable
REPLICATE_PRIMARY_TREE_TO_SHADOW Controls how the primary tree is replicated from the primary tree to the shadow tree. By default, it is disabled, and paths are replicated to the secondary storage area gradually as data is moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location.	0	0 - Disable 1 - Enable
SHIFT_ACCESSED_SHADOW_FILES Controls whether files are moved from the secondary volume to the primary volume if the volume is accessed twice during a specified elapsed time. Use SHIFT_DAYS_SINCE_LAST_ACCESS to specify the time period. The file is moved after it is closed.	0	0 - Disable 1 - Enable
SHIFT_MODIFIED_SHADOW_FILES Controls whether files are moved from the secondary volume to the primary volume if the file is modified. The file is moved after it is closed.	1	0 - Disable 1 - Enable
SHIFT_DAYS_SINCE_LAST_ACCESS Specifies the number of elapsed days during which a file must be accessed twice before it is moved. This applies only if SHIFT_ACCESSED_SHADOW_FILES is enabled.	1	0 - Disable 1 to 365 (in days)

A.2.3 Locks Management for File Access on NCP Server

Parameter Name and Description	Default Value	Value Options
CROSS_PROTOCOL_LOCKS Controls cross-protocol file locking support between NCP and other protocols, including Novell Samba, Novell CIFS, and Novell AFP. Cross-protocol locks help prevent the same file from being concurrently accessed for modifications with multiple protocols. Each recognizes when the other has the file in use. Turning this option on decreases performance, so do not turn it on unless you plan on sharing files across multiple protocol clients.	1	1 - Enable 0 - Disable
OPLOCK_SUPPORT_LEVEL Controls NCP opportunistic locking. Oplocks are locks that allow the client to cache file data for better performance.	2	0 - Disable 1 - Exclusive locks 2 - Shared and exclusive locks
LOCK_RANGE_MASK	1	By default this parameter is turned on. Setting the parameter value to 0 turns off this parameter and does not permit locking beyond the 0x7fffffffffffffff region.

NCP Server has an internal byte-ranging mechanism to prevent potential data corruption when files on NSS and NCP volumes are accessed by NCP clients. Cross-protocol file locking uses the Linux Advisory byte-range lock to prevent potential data corruption when files are accessed by non-NCP file access protocols and by other applications that directly access the files with POSIX APIs. By default, cross-protocol file locking is enabled (CROSS_PROTOCOL_LOCKS = 1) on OES 2015 SP1 servers. Cross-protocol file locking is enforced globally for all NCP and NSS volumes on the server.

Non-NCP file access protocols include Novell Samba, Novell CIFS, and Novell AFP. Applications include any application or service that accesses data on an NCP volume or NSS volume, such as SSH, FTP, restore, scripts, antivirus, database, management tools, and so on.

For example, when ConsoleOne is used to administer the GroupWise database, GroupWise agents directly access the files. You must enable CROSS_PROTOCOL_LOCKS in order for the Linux Advisory byte-range locks to work and prevent any potential data corruption.

NOTE: Disabling cross-protocol file locking can cause data corruption if any application or non-NCP file access protocol accesses the same data that is accessed via NCP. We recommend that you do not disable cross-protocol file locking, even if NCP is the only active file access protocol.

For better performance, you can disable cross-protocol file locking if you are not using non-NCP file access protocols and the files are not directly accessed by other applications. However, this is not recommended, because disabling cross-protocol file locking can cause data corruption.

A.2.4 Logs of NCP Server Events

***Table A-1** Server Parameter Information for Logging NCP Server Events*

Parameter Name and Description	Default Value	Value Options
LOG_LEVEL Controls the nature and types of messages that are logged to the /var/opt/novell/log/ncpserv.log file.	WARN	Each level logs entries for its level and the levels listed above it. NOTHING – Disable logging. ERROR – Log only error messages WARNING – Log warning and error messages INFO – Log informational, warning and error messages. DEBUG – Log informational, warning, debug and error messages. ALL – Log all messages.
LOG_CACHE_STATISTICS Controls whether cache statistics are logged in the ncpserv.log file. Turning this setting on causes the NCP engine's directory cache to output statistics to a log file. Information such as the number of cached files, number of cached directories, number of open files, etc. is logged.	0	0 - Disable 1 - Enable
LOG_IDBROKER_ERRORS Controls whether ID broker errors are logged in the ncpserv.log file.	0	0 - Disable 1 - Enable
LOG_MEMORY_STATISTICS Controls whether memory statistics are logged in the ncpserv.log file.	0	0 - Disable 1 - Enable

A.2.5 NCP Communications

Table A-2 Server Parameter Information for Communications

Parameter Name and Description	Default Value	Value Options
FIRST_WATCHDOG_PACKET Controls how long to wait in minutes of inactivity before checking to see if an NCP connection is still alive. The server sends an NCP ping packet to the client if it detects no client activity for a specified amount of time. By doing this, the server tries to keep the connection alive. You can configure this parameter if there is any mechanism implemented between the server and the client that would break idle connections.	0	0 - Disable 1-120(minutes) - Enable
NCP_TCP_KEEPALIVE_INTERVAL If the client is inactive for a configured amount of time, the server sends a TCP packet to the client to check if the client is still connected to the server or not. If the server does not get an acknowledgement from the client, then the server identifies that the client is not available and clears all the information related to the specific client connection.	8 minutes	3 to 240 (minutes)
DISABLE_BROADCAST Controls the ability to broadcast messages from the NCP Server.	0	0 - Disable 1 - Enable

A.2.6 NCP Server Environment

Table A-3 Server Parameter Information for the NCP Server Environment

Parameter Name and Description	Default Value	Value Options
LOCAL_CODE_PAGE Controls which base code page is used by the NCP Server. This setting defines the local code page used for file and subdirectory names, except for case 89 NCPs that use UTF-8. This value should be set to match the majority of your clients. Syntax: `LOCAL_CODE_PAGE` *`code_page`* For example: LOCAL_CODE_PAGE CP437 You can get the complete list by typing the following command at the linux command line: `iconv - - list | more`	CP437	Valid language codes Commonly used values are: CP437 for the standard English character set. CP850 for European character sets. CP932 for Japanese CP949 for Korean CP866 for Russian GBK for simplified Chinese BIG5 for traditional Chinese

Parameter Name and Description	Default Value	Value Options
NCP_FILE_SERVER_NAME This parameter is set by eDirectory when the NCP Server is installed, and must not be modified arbitrarily. For information, see Section 3.12, "Modifying the NCP File Server Name," on page 40.	Server hostname	This setting must match the server hostname, such as `server1`.

A.2.7 NCP Volumes

Table A-4 *Server Parameter Information for Volume and File Management*

Parameter Name and Description	Default Value	Value Options
COMMIT_FILE This parameter assures an NCP client that all data previously written to a file has been written to disk. Because files must be stored on the physical storage medium before certain actions are attempted, this call provides a checkpoint that guarantees that the file has been flushed from cache and written to disk. When this parameter is enabled, it calls the Linux `fsync` command to flush data from cache and write it to the disk, then it returns success to the calling function. When this parameter is disabled (the default setting), nothing is done, but it returns success to the calling function.	0	0 - Disable 1 - Enable
EXECUTE_ATTRIBUTE_SUPPORT With this setting turned on, the NCP "execute only" attribute can be associated with the user mode execute bit on a file or subdirectory. With this setting turned on, NCP clients can set or clear this bit. The Novell Client for Linux uses this bit to represent the user mode execute bit on a file or subdirectory.	1	0 - Disable 1 - Enable
KEEP_NSS_FILE_DELETOR_IDS This option is for retaining the deletor ID when a file is deleted on NSS volumes. NCP notifies NSS to provide the identity of the user who initiated the delete. This information is then retained by NSS and available when the file is salvaged, assuming that the Salvage attribute is enabled for the NSS volume when the file is deleted and salvaged.	1	0 - Disable 1 - Enable
SENDFILE_SUPPORT This option allows the NCP Server to send file read data to the client directly from the Linux Kernel Ring 0 environment, rather than copying it to Ring 3 and then back to Ring 0. Turning on this option gives you a slight performance improvement.	0	0 - Disable 1 - Enable

Parameter Name and Description	Default Value	Value Options
SYNC_TRUSTEES_TO_NSS_AT_VOLUME_MOUNT Controls trustee resynchronization for an NSS volume when it is mounted for NCP.	0	0 - Disable 1 - Enable
VOLUME_GONE_WARN_USERS Controls whether a message is broadcast to warn users when the volume path is no longer present.	1	0 - Disable 1 - Enable

A.2.8 NCP Volumes Low-Space Warning

Table A-5 Server Parameter Information for Volume Low-Space Warning

Parameter Name and Description	Default Value	Value Options
VOLUME_EMPTY_WARN_USERS Controls whether a message is broadcast to warn users when no volume space is available.	1	0 - Disable 1 - Enable
VOLUME_LOW_WARN_USERS Controls whether a message is broadcast to warn users when volume space is low.	1	0 - Disable 1 - Enable
VOLUME_LOW_WARNING_RESET_THRESHOLD Sets the high watermark threshold (in blocks), which is the level where the low watermark threshold is reset, and users no longer receive the low-space message. An NSS block is 4 KB.	128	0 to 100000
VOLUME_LOW_WARNING_THRESHOLD Sets the low watermark threshold (in blocks) that indicates space is low. An NSS block is 4 KB.	64	0 to 100000

A.2.9 Enabling or Disabling UID Updates

Use the commands in this section to enable or disable the maintenance thread to update UIDs. If users are LUM-enabled, you should update UIDs at least once in every 3 or 4 days.

Table A-6 Server Parameter Information for Enabling or Disabling UID Updates

Parameter Name and Description	Default Value	Value Options
UID_UPDATE_ENABLED Controls the maintenance thread to update UIDs. 0: Disables UID updates. You can disable UID updates only if all users are non-LUM users. 1: Enables periodic UID updates. Set the frequency of updates by using the UID_UPDATE_PERIOD parameter. 2: Enables a one-time UID update. After updating, the maintenance thread resets the parameter to the previous value.	1	0 - Disable 1 - Enable periodic updates 2 - Enable one-time update
UID_UPDATE_PERIOD Sets the frequency in hours. This option is applicable only if UID_UPDATE_ENABLED is set to 1. The maintenance thread completes the previous cycle and then updates according to the new value set. For example, if the previous value of UID_UPDATE_PERIOD was 45 minutes and the new value set is 30 minutes, the maintenance thread completes the 45-minute cycle first and then updates every 30 minutes.	Default and minimum value: 0.5 (30 minutes or half of an hour)	Maximum: No limits

Examples

```
ncpcon set UID_UPDATE_ENABLED=0
```

The maintenance thread does not update UIDs.

```
ncpcon set UID_UPDATE_ENABLED=1
ncpcon set UID_UPDATE_PERIOD=0.5
```

The maintenance thread updates UIDs every 30 minutes.

```
ncpcon set UID_UPDATE_ENABLED=2
```

Triggers an immediate one-time update of the UID, then resets the value to 1.

A.2.10 Enabling or Disabling Logging eDirectory Object Rename or Delete Events

When an object is deleted or renamed in eDirectory, NCP sends a notification to NSS via IPC and logs the event in the `/opt/novell/ncpserv/sbin/objecthistory.txt` file. Beginning with OES2015 SP1, this file is renamed to `objecthistory.log`, moved to `/var/opt/novell/log/` directory, and added to the log rotation. You can choose to disable or enable logging of object history events.

Table A-7 Server Parameter Information for Enabling or Disabling Logging eDirectory Object Rename or Delete Events

Parameter Name and Description	Default Value	Value Options
LOG_OBJECT_HISTORY = <value> 0: Disables logging rename or delete eDirectory object events. 1: Enables logging rename or delete eDirectory object events.	1	0 - Disable 1 - Enable

Examples

```
ncpcon set LOG_OBJECT_HISTORY = 1
ncpcon set LOG_OBJECT_HISTORY = 0
```

A.2.11 Augmented Size of NCP Verbs 87_20 and 89_20 Replies

Certain NCP verb replies require 64K buffers to be allocated internally from the memory subsystem. If there are a number of such requests, a chunk of memory is allocated and processed for each request.

Continuous allocation and deallocation of a huge chunk of memory buffers makes the memory subsystem busy.

To offload the memory subsystem, a buffer pool is created when the NCP server starts, and a 64K buffer is allocated from the buffer pool for processing and storing the reply data.

Suggestions for configuring the `CONN_LBUF_POOL_SIZE` parameter.

Specify the memory pool size in MB.

If it is expected that the maximum of "n" number of connections will actively access the NCP server during the peak time at any single point of time, set CONN_LBUF_POOL_SIZE to n/32.

This calculation is based on the assumption that only half of those connections require a 64K buffer to store the reply.

NOTE: Although this parameter can be configured dynamically, it will be effective only after the next restart of `ndsd`.

Until `ndsd` is restarted, the existing buffer pool will remain intact and will not be changed to accommodate the new size value.

Pool minimum size: 10 MB

Pool maximum size: 1024 MB

Pool default size: 64 MB

A.3 NCP2NSS Command

This is a daemon that interfaces between the NCP Server and NSS File System which happens via an IPC channel internally. All volumes and trustees, directory and file rename or delete related events pass through this channel. This daemon must run in order for the NCP Server to support NSS filesystem.

```
/opt/novell/ncpserv/sbin/ncp2nss
```

```
/etc/init.d/ncp2nss {[re]start|stop|status}
```

A.4 ShadowFS Command

This daemon is part of DST. If the ddaemon is started and running then it will make the DST volume pair available for applications running on an OES server, for example, GroupWise Server or FTP server. Subsequently the merge view of both primary and secondary volumes can be accessed transparently at the mount point `/media/shadowfs/<Primary Volume Name>` on the OES server.

```
/etc/init.d/novell-shadowfs {[re]start|stop|status}
```

A.5 Virtual NCP Server Object Script

The `/opt/novell/ncs/bin/ncs_ncpserv.py` script creates a virtual NCP Server object in NetIQ eDirectory, and associates it with none, one, or multiple NCP volumes that you specify. Having an NCP Server object makes it easier for clients to access NCP volumes on clusters. You specify the IP address of the cluster resource that you want to use to manage all of the NCP volumes and the shared LVM volumes and disks where the NCP shares reside. You must bind the NCP Server object to the IP address of that cluster resource.

Issue the command at a terminal console prompt as the `root` user. Novell cluster services must be installed and running.

./opt/novell/ncs/bin/ncs_ncpserv.py -c *ncp_server_name* -i *ip_address* [-v <*volumename* | "volumenames"]

Replace *ncp_server_name* with the name you want to use for the virtual NCP server. It can be the same or different than the cluster resource you created when you cluster-enabled the Linux POSIX volume.

Replace *ip_address* with a static IP address for the virtual server. Replace *volumename* with the name of the NCP volumes that you want to assign to this virtual NCP Server object. The virtual NCP Server object is the NCS:NCP Server attribute.

If the `-v` option is not specified, all of the NCP volumes that currently exist on the LVM volume are bound to the IP address. If you enter multiple volume names, use colons to delimit the names and put quotation marks around the list of names. The multiple volume names can be listed by the name (MY_NNCP_VOL06) or by the distinguished name (cn=CLUS_02_MY_NNCP_VOL06,o=novell), or any combination of the two methods.

Examples

To include all of the NCP volumes on the cluster resource, enter

```
./ncs_ncpserv.py -c ncp_serv01 -i 10.10.10.45
```

To specify a single NCP volume on the cluster resource, enter

```
./ncs_ncpserv.py -c ncp_serv01 -i 10.10.10.45 -v MY_NNCP_VOL05
```

To specify multiple NCP volumes on the cluster resource, enter

```
./ncs_ncpserv.py -c ncp_server02 -i 10.10.10.46 -v
"MY_NNCP_VOL06:cn=CG_02_MY_NNCP_VOL07,o=novell"
```

B Additional NCP Server Commands and Options

This section describes NCP Server commands, command line options, and configuration file options that should not be used except under direction from Novell Support.

- Section B.1, “NCP2NSS Command Options,” on page 197
- Section B.2, “NCPCON Commands and Options,” on page 197
- Section B.3, “NCPTOP Command Line Options,” on page 198

B.1 NCP2NSS Command Options

```
/opt/novell/ncpserv/sbin/ncp2nss
```

The following hidden options apply to the `ncp2nss` command:

`-d`

Used to start the NCP2NSS daemon as a foreground process instead of as a background daemon.

B.2 NCPCON Commands and Options

The commands in this section are not included in the general management commands for the NCP Server Console utility. You must be logged in as the `root` user to issue the commands.

- Section B.2.1, “Hidden Options,” on page 197
- Section B.2.2, “Hidden Commands,” on page 198

B.2.1 Hidden Options

The following options are available for NCPCON in command line mode. The syntax is

```
ncpcon [option]
```

`--@filename`

Reads from the file and executes the commands.

`--help`

Lists the syntax for command line mode and interactive mode.

`--ncpservername`

Used with `bind` and `unbind` commands.

In a cluster load script, use the following syntax:

```
exit_on_error ncpcon bind --ncpservername=<SERVER_NAME> --
ipaddress=<IP_ADDRESS>
```

For example,

```
exit_on_error ncpcon bind --ncpservername=BETA31-BETA31-SERVER --
ipaddress=192.168.100.1
```

--ipaddress

Used with `bind` and `unbind` commands.

In a cluster load script, use the following syntax:

```
exit_on_error ncpcon bind --ncpservername=<SERVER_NAME> --
ipaddress=<IP_ADDRESS>
```

For example,

```
exit_on_error ncpcon bind --ncpservername=BETA31-BETA31-SERVER --
ipaddress=192.168.100.1
```

--volid

Used with the `mount` command.

In a cluster load script, use the following syntax:

```
exit_on_error ncpcon mount volname=vol_id,path=/vol_mntpt
```

For example,

```
exit_on_error ncpcon mount USERS=254,path=/media/ncpvolumes/USERS
```

B.2.2 Hidden Commands

The commands in this section are used only for diagnostic purposes.

diag

Use this command to display NCP Server diagnostics or `ncp2nss` daemon diagnostics.

Examples:

```
diag
```

```
diag ncp2nss
```

flush volume *volume_name*

Flushes file system dirty data from the specified volume. You can add the `ncpcon flush volume volume_name` command to a cluster load script.

nss resync=*volume_name*

Resynchronizes NCP Server and NSS information for the specified volume.

nss verify=*volume_name*

Verifies NCP Server and NSS information for the specified volume.

B.3 NCPTOP Command Line Options

--d

Outputs logging information to the `ncptop.log` file.

`--h`

Displays help information.

C RPM Files for NCP Server

The following RPM files are installed for NCP (NetWare Core Protocol) Server on Open Enterprise Server (OES) 2015 SP1:

`novell-ncpenc-5.6.0-0.164.11`

Contains the NCP server shared library (libncpengine.so) that runs as part of Novell eDirectory. This component handles all client NCP requests.

`novell-ncpserv-nrm-2.4.0-0.92.9`

Contains the Novell Remote Manager for Linux plug-in (libnrm2ncp.so) provided by the NCP team.

`novell-ncp2nss-2.5.0-0.29.3`

Contains ncp2nss daemon binary which is an interface between NCP Server and NSS File System.

`novell-ncpserv-tools-2.5.0-0.29.3`

Contains NCP tools NCPCON and NCPTOP.

`novell-ncpns-5.10.0-0.179.24`

Contains libncpns, which is used for ID Broker.

D NCP Error Codes

The information on this page is intended to be used for diagnostic purposes only.

NCP does not log all error codes in the `ncpserv.log` file as logging all error codes may bloat the log file. NCP interacts with multiple components, hence investigating the log file alone is not enough to analyze the call trace. The administrators are advised to investigate packet trace along with the log file for effective analysis and troubleshooting.

The error numbers listed are NCP protocol specific errors; however, NCP also logs Linux specific error codes.

D.1 00 0x00 SUCCESS

Source: NCP Engine

Explanation: Requested operation has finished successfully.

D.2 01 0x01 NOT CONNECTED

Source: NCP Engine

Explanation: Not connected (Not valid connection).

D.3 119 0x77 BUFFER TOO SMALL

Source: NCP Engine

Explanation: The file name passed is not enough to hold and process in memory. This is a network error that can occur if the data to be passed is too large for the buffer that was declared.

Action: Verify that your network adapters and network connections are configured and working properly.

D.4 120 0x78 VOLUME FLAG NOT SET

Source: NCP Engine

Explanation: The logged-in user has limited access rights to create or open the file.

Action: For opening a file, ensure that the user is a trustee with the Read and File Scan right for the parent directory. For creating a file or subdirectory, add the Create, Write, Modify, and Erase rights as appropriate for the authorized actions. Ensure that the user has an authenticated connection to the server.

D.5 121 0x79 NO ITEMS FOUND

Source: NCP Engine

Explanation: The NCP Engine could not find any files in the cache entry.

Action: If you know the files exist, check the path and file name in the request, and try again. Ensure that you have an authenticated connection to the server.

D.6 125 0x7d CONNECTION NOT LOGGED IN

Source: NCP Engine

Explanation: The NCP Engine found that either the license has expired or the user does not have a license to log in, which will limit the user's file operations.

Action: Ensure that the user has an authenticated connection to the server, then try again.

D.7 126 0x7e NCP BOUNDARY CHECK FAILED

Source: NCP Engine

Explanation: The NCP size allocated for the function does not match the actual size of the data sent. This can occur if the request was not formatted properly, or if there was packet corruption in the transmission between the client and server.

Action: Ensure that the network equipment between the client and server are functioning properly. If it is and the error persists, it could be a problem with the requesting application.

D.8 128 0x80 LOCK FAIL

Source: NCP Engine

Explanation: The file is in use and already in locked state.

Possible Cause: The file is in use by another user that has the file open for read and write.

Action: You can ask the other user to close the file, or retry the action later.

Possible Cause: The file is locked by another process that holds the file open for writes, such as a database.

Action: You might be able to stop the other process to close the file, or retry the action later.

Possible Cause: The file is locked by another process or user session that has terminated abruptly and left the file in a locked state.

Action: If no valid user or process has the file open, delete the connection to unlock the file.

D.9 132 0x84 NO CREATE PRIVILEGE

Source: NCP Engine

Explanation: The logged-in user does not have sufficient privileges to create or open the file.

Action: Ensure that the user is a trustee with at least the Read, File Scan, and Create rights for the parent directory. Ensure that the user has an authenticated connection to the server.

D.10 135 0x87 CREATE FILE INVALID NAME

Source: NCP Engine

Explanation: The NCP engine could not validate the file name.

Action: Ensure that the file name is unique in the destination location and that the name complies with syntax and naming conventions.

D.11 136 0x88 INVALID FILE HANDLE

Source: NCP Engine

Explanation: The NCP engine displays this generic information if one or more parameters like file path or file handle provided by the client is not correct. The handle might be released and is no longer valid, or it was never initialized.

Action: Ensure that the correct name and syntax are used, and that the user has sufficient privileges to perform the requested action. Get a new file handle by opening the file again.

D.12 138 0x8a NO DELETE PRIVILEGE

Source: NCP Engine

Explanation: The logged-in user does not have sufficient privileges to delete the file, or the licensed user is not logged-in.

Action: Ensure that the user is a trustee with at least the Read, File Scan, and Create rights for the parent directory. Ensure that the user has an authenticated connection to the server.

D.13 139 0x8b NO RENAME PRIVILEGE

Source: NCP Engine

Explanation: The NCP engine could not serve the request because the logged-in user does not have sufficient privileges to rename the file.

Action: Ensure that the user is a trustee with the Modify right for the parent directory. Ensure that the user has an authenticated connection to the server.

D.14 140 0x8c NO SET PRIVILEGE

Source: NCP Engine

Explanation: The NCP Engine found that the volume does not support adding trustees to it. Ensure that the user performing the operation has sufficient privileges.

Action: The user must be a trustee with the Supervisor right or Access Control right to set rights for other users. The Access Control right does not permit the user to limit Supervisor rights.

D.15 144 0x90 ALL READ ONLY

Source: NCP Engine

Explanation: The NCP engine could not perform the file operation; read-only permission was set on the volume where the file or directory exists.

Action: If users are trustees with the Read right and File Scan right, the users do not have permission to modify the files or directories, but they can browse and view them. For users that need to make changes to files or directories, you can make them trustees and grant them the additional rights to Write, Create, Modify, and Erase in the target location.

D.16 146 0x92 ALL NAME EXIST

Source: NCP Engine

Explanation: The NCP engine could not serve the request because the target already exists.

Action: Change the name of the file being created or delete the file that is already there.

D.17 147 0x93 NO READ PRIVILEGE

Source: NCP Engine

Explanation: The NCP engine could not serve the request because the logged-in user does not have the read privilege.

Action: To give permissions, ensure that the user is a trustee with at least the Read and File Scan rights in the location and has an authenticated connection.

D.18 148 0x94 NO WRITE PRIVILEGE

Source: NCP Engine

Explanation: The NCP engine could not serve the request because the logged-in user does not have the Write privilege.

Action: To give permissions, ensure that the user is a trustee with at least the Read, File Scan, and Write rights in the location and has an authenticated connection.

D.19 150 0x96 NO ALLOC SPACE

Source: NCP Engine

Explanation: The client requested a file operation and the NCP engine could not find memory to allocate to service this request.

Action: Add extra memory or suspend some other processes in the system to free up memory.

D.20 152 0x98 INVALID VOLUME

Source: NCP Engine

Explanation: The NCP engine received a request from the NCP client to open a volume that does not exist, or the volume ID is not correct.

Action: Fix the volume name, syntax, or volume ID in the request, then try again. For administrators, you can use the `ncpcon volumes /v` command to list volume IDs to find the correct value.

If the volume is clustered, it might not be mounted on the specified server at this time. Ensure that you connect to the virtual server for the volume's cluster resource, then try again.

D.21 153 0x99 DIRECTORY FULL

Source: NCP Engine

Explanation: The NCP engine did not find enough space to perform the file operation requested by the NCP client. This can occur when the request for space would exceed a directory quota set on the destination folder or its parent directories.

Action: Add space or free up space by doing any of the following:

- Increase the directory quota.
- If salvage is enabled, purge deleted files from the salvage area.
- Delete files that are unwanted or unnecessary.

D.22 154 0x9a RENAME ACROSS VOLUME

Source: NCP Engine

Explanation: The NCP engine could not rename across volumes because the source volume and destination volume are different.

Action: Although the RENAME command can move a file between directories on the same volume, using RENAME to move a file between volumes is not allowed.

If you have sufficient privileges on both NSS volumes, you can map a drive to each volume, and then use the Novell Client's copy option to copy the file or folder between the two volumes along with the trustee and file access metadata.

D.23 155 0x9b BAD DIR HANDLE

Source: NCP Engine

Explanation: The NCP engine received an invalid source or destination directory handle from the NCP client. The handle might be released and is no longer valid, or it was never initialized.

Action: Ensure that the directory name and directory path syntax are correct, then try opening the directory again.

D.24 156 0x9c INVALID PATH

Source: NCP Engine

Possible Cause: The NCP engine has reached the maximum length of the file path, or the file path is invalid.

Action: Rename the file with a shorter name, or rename directories in the path. Verify that you used the correct syntax for the path.

Possible Cause: The NCP engine searched the cache and could not find the path requested by the NCP client. The path might not use the correct syntax, or you might have one of the following problems in the path name:

- An invalid namespace
- An invalid character
- A wildcard character in the volume name
- A volume name is used in the path name when one was not expected
- A volume name is missing in the path for a path name that requires a volume

Action: Fix the path, then try again.

D.25 156 0x9d NO SUCH EXTENSION

Source: NCP Engine

Explanation: The file extension of the file is not recognized.

D.26 160 0xa0 DIRECTORY NOT EMPTY

Source: NCP Engine

Explanation: The NCP Engine could not serve the request because the directory is not empty and it contains files or subdirectories.

Action: Delete the directory contents and then delete the directory, or use a command or tool that deletes the directory and its contents. For example, administrators can use Novell Remote Manager to delete a directory and its contents in a single operation.

D.27 162 0xa2 IO LOCKED

Source: NCP Engine

Explanation: IO is locked. An attempt was made to write to a file where data is physically locked. The file is in use and already in a locked state.

(This error code might be the result of Linux to NetWare Error Code conversion. The actual error could be in a system call.)

Possible Cause: The file is not currently locked by a user that has the file open.

Action: You can ask the other user to close the file, or retry the action later.

Possible Cause: The file is not currently locked by another process that holds the file open for Writes, such as a database.

Action: You might be able to stop the other process to close the file, or retry the action later.

Possible Cause: The file is not currently locked by another process that has terminated.

Action: If no valid user or process has the file open, delete the connection to unlock the file.

D.28 168 0xa8 ACCESS DENIED

Source: NCP Engine

Explanation: The NCP engine could not serve the request because the logged-in user does not have sufficient privileges to create the file at the destination or delete the file from the source.

Action: Ensure that the user is a trustee with the Create right in the destination location and the Erase right in the original location.

D.29 169 0xA9 LINK IN PATH

Source: NCP Engine

Explanation: The NCP Engine received and invalid file path from the client.

Possible Cause: A broken Distributed File Services junction was encountered when following the path.

Action: If the error persists, notify your system administrator.

Possible Cause: The request was made for a path that had a link type that is not supported by NCP or NSS.

Action: NSS and NCP Server support hard links to files but not to directories, data streams, and extended attributes. Hard links to files are supported only for paths within the same NSS volume.

Because of security considerations, NSS and NCP Server intentionally do not support soft links.

D.30 191 0xbf INVALID NAMESPACE

Source: NCP Engine

Explanation: The NCP engine received a request from the NCP client that contained a namespace other than Long, which is not valid.

Action: The DOS namespace is not supported on NCP volumes. If the namespace is changed to DOS, NCP volumes might not be mounted and might not be accessible from the clients.

D.31 242 0xf2 NO OBJECT READ RIGHTS

Source: NCP Engine

Explanation: An attempt was made to access a directory object's information or scan the object's properties without the necessary security permissions.

Action: If applicable, ensure sufficient rights are assigned and retry the operation.

D.32 251 0xfb UNKNOWN REQUEST

Source: NCP Engine

Explanation: An attempt was made to use an invalid parameter or connection in the request.

Action: Retry the operation with parameters (server connection, GUID size, GUID list).

D.33 253 0xfd BAD STATION NUMBER

Source: NCP Engine

Explanation: The NCP client could not connect with the NCP engine. Incorrect configuration settings caused the invalid session because an attempt was made to use a bad (undefined, unavailable, and so on) station number. This might occur if the server or process crashed while connections were active, and the connection is no longer valid.

Action: Ensure that the user has an authenticated connection to the server.

D.34 254 0xfe DIRECTORY LOCKED

Source: NCP Engine

Explanation: The directory service is locked or no writable replicas are available. The server cannot get or modify the account status at this time.

Possible Cause: Retry the operation. If the error still occurs, verify that the directory service is running and a writable replica is available.

D.35 255 0xff NO FILES FOUND

Source: NCP Engine

Explanation: The NCP engine could not find the file because the client requested file directory does not exist, or the logged-in user does not have sufficient privileges to rename or move the file.

Action: If you know the file exists, check the path and file name, ensure that the user is a trustee for the path with at least the Read right and File Scan right, and ensure the user has an authenticated connection to the server. For a clustered volume, ensure that you specify the virtual server for the cluster resource instead of the physical server in the share path.

D.36 255 0xff BAD PARAMETER

Source: NCP Engine

Explanation: The NCP engine displays this generic information if one or more parameters like file path or file handle provided by the client is not correct.

Action: Ensure that the correct name and syntax are used, and that the user has sufficient privileges to perform the requested action.

D.37 255 0xff FILE EXISTS

Source: NCP Engine

Explanation: The NCP engine could not create the file because a file or directory already exists with the same name.

Action: Provide a name for the file or directory that is unique in the target location.

D.38 255 0xff NO FILES FOUND

Source: NCP Engine

Explanation: The NCP engine could not create the file or directory because a file or directory already exists with the same name, or the logged-in user does not have sufficient privileges to create the file.

Action: Ensure that the user is a trustee with the Create right for the parent directory, and provide a name for the file or directory that is unique in the target location.

D.39 255 0xff NOT VALID CONNECTION

Source: NCP Engine

Explanation: The service at the target address was busy, down, or not responding.

Action: Retry the operation. If the error still occurs, go to the target machine and verify that the service is running.

D.40 255 0xff CREATE FILE INVALID NAME

Source: NCP Engine

Explanation: The NCP engine was not able to create the file with the specified name; either a file already exists with the same name or the file name is not valid.

Action: Ensure that the file name is unique in the destination location and that the name complies with syntax and naming conventions.