AUTHORIZED DOCUMENTATION

Novell CIFS for Linux Administration Guide

Novell®
Open Enterprise Server

2 SP2

November, 2009

www.novell.com

Legal Notices

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

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

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

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

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

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web site (http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide

This guide contains information on installing, migrating, configuring, administering, managing, and troubleshooting Novell® CIFS software specific to Windows* CIFS running on Open Enterprise Server (OES) 2 SP2 Linux.

Audience

This guide is intended for OES 2 Linux* administrators who want to use and administer the CIFS services and to access shares.

Feedback

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

Documentation Updates

For the most recent version of the *CIFS Guide*, visit the OES 2 Documentation Web site (http://www.novell.com/documentation/oes2sp1/).

Additional Documentation

For documentation on CIFS on NetWare®, see the NFAP guide.

Documentation Conventions

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

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

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

Overview of CIFS

1

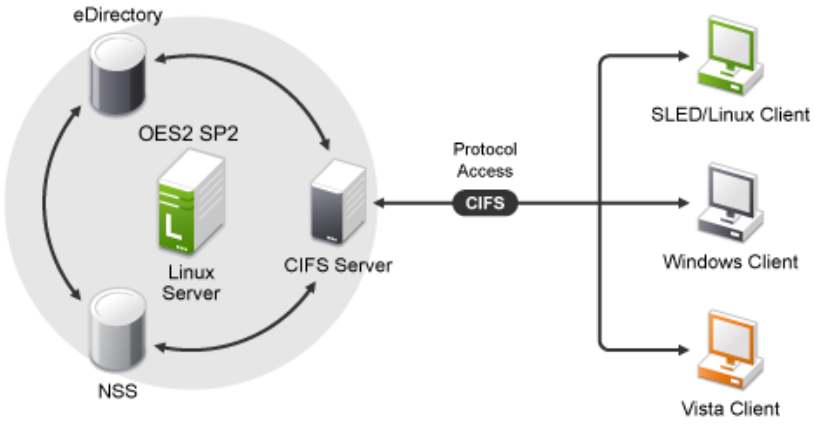
CIFS (Common Internet File System) is a network file sharing protocol that is based on the SMB (Server Message Block) protocol. File sharing is achieved through these separate but intertwined protocols for service announcement, naming, authentication, and authorization.

1.1 Understanding CIFS

Novell® CIFS runs on the Open Enterprise Server (OES) 2 SP2 Linux server, uses Novell eDirectory™ services for user authentication, and allows the Windows and Linux client users to access the server data files or other shared resources in one of the following ways:

- For Windows, through the Network Neighborhood or My Network, Windows Explorer, and mapped drives from Windows and Windows Vista* workstations.
- For Linux, through a SMB client from Linux desktops.

Figure 1-1 *Novell CIFS Conceptual Overview*



1.2 CIFS and Universal Password

Universal Password helps in management of password-based authentication schemes.The Universal password is not enabled by default. Each CIFS user must be Universal Password enabled to be able to log in to the CIFS server.

To learn more about Universal Password, including how to enable it, see "Novell Password Management" (http://www.novell.com/documentation/password_management32/pwm_administration/data/allq21t.html) in the *Novell Password Administration Guide (http://www.novell.com/documentation/password_management32/pwm_administration/data/bookinfo.html)*.

1.3 CIFS Features and Capabilities

CIFS implementation supports the following features on OES 2 SP2 Linux:

- Support for Windows 7 client
- Cross-Protocol File Locking support between AFP, CIFS, and NCP™
- Auditing support for File Access activities
- Migration capability from NetWare® to Linux
- DFS Support
- Support for Windows 2000, XP, 2003, Vista Enterprise, Vista Business, and Vista Ultimate (both 32-bit and 64-bit), and SUSE® Linux Enterprise Desktop (SLED) 10 as client operating systems. For details, see Section 3.2.3, "Client Operating System Requirements," on page 17
- Support for Universal Password
- Support for NTLMv1 authentication mode
- Integration with Novell eDirectory
- Integration with the Novell Storage Services™ (NSS) file system
- Support for Unicode* filenames
- Supports the Novell Trustee Model for file access
- Does not require Linux User Management (LUM) enabling
- Supported by Novell Cluster Services™ for high availability
- Administration and configuration through iManager

1.4 Advantages of Novell CIFS

- CIFS on OES 2 Linux simplifies overall network administration by consolidating user management through Novell eDirectory.

  All users who need access to the network are represented in eDirectory through User objects. This enables administrators to easily and effectively assign trustee rights, control access, and manage all User objects from a single location on the network.
- Support for 1500 concurrent client connections.
- Superior performance similar to NetWare® CIFS.
- Takes advantage of enhanced interoperability services provided by OES 2 Linux server.
- Enhanced Migration Tool support for NetWare CIFS users.

1.5 CIFS Server

Novell CIFS enables Windows and Linux client workstations to create, copy, delete, move, save, and open files on an OES 2 Linux server. CIFS allows read and write access from multiple client systems simultaneously. All these various file operations and sharing of resources on a network are managed from a CIFS server.

The CIFS protocol offers various services, service announcements, user authentication and authorization, and naming service running on a CIFS server. For achieving the file sharing and other services, a CIFS Server uses NetBIOS over TCP/IP (NBT) and SMB services. CIFS file sharing is achieved by a mechanism called Browsing services or advertising. For details on Browsing and other services, see Section 1.6, “CIFS Terminology,” on page 13.

1.6 CIFS Terminology

CIFS is defined by its local implementation rather than a universal specification. The following sections are terms and definitions that are part of CIFS and are widely used:

NetBIOS Names: Human-readable and visible names assigned to computers on a network. All NetBIOS computers on a network are configured by the administrator.CIFS uses NetBIOS Naming Service (NBNS) for name resolution.

Workgroup: A peer-to-peer computer network that shares files and information. Workgroups simplify network management by organizing servers and services into administrative groups. Workgroup names are defined by the NetBIOS names.

Domain Name System (DNS): An Internet service that translates domain names into IP addresses.

Browsing: The process of discovering the (NetBIOS names) of CIFS Servers that are on the network.

Browsing Services: An advertising mechanism used by a CIFS Server to announce and use the shares available in the network. This service maintains the list of available file and print services. The list is presented via the Network Neighborhood or My Network Places in Windows, Linux or SMB clients for Linux.

Local Master Browser (LMB): The workgroup leader for each individual workgroup. Also called a Master Browser.

Master Browser: A computer that is the workgroup leader for each individual workgroup. Also called a Local Master Browser or LMB.

Domain Master Browser (DMB): A computer that collects information from several Master Browsers within a domain.

Backup Browser (BB): Any computer on a network other than a Master Browser. Used to distribute the browser loads. Based on the network traffic and an election or voting process, a Backup Browser has the potential to become a Local Master Browser, if required.

OpLocks: Opportunistic locking. A locking and authentication mechanism of file sharing when there are multiple users or requests to the same share or resource on the network. OpLocks provides a means to cache a read/write operation on a file without updating the server every time.

Novell Product Terms: For definitions of Novell product terminology and other glossary terms used in this guide, such as NMAS™, NICI, NCP™, and others, visit the Novell: Glossary of Terms (http://www.novell.com/company/glossary.html).

1.7 What's Next

If you are planning to implement CIFS on your enterprise server, continue with Chapter 3, “Planning and Implementing CIFS,” on page 17 to understand the implementation requirements.

What's New

2

The following new features are implemented on Open Enterprise Server (OES) 2 Linux for CIFS:

- **Installation and Configuration through YaST:** CIFS is installed and configured through the YaST interface on OES 2 Linux. For details, see Section 4.2, "Installing and Configuring a CIFS Server through YaST," on page 23.
- **Administration and Configuration:** iManager provides an advanced level of administration and configuration of CIFS on OES 2 Linux. For details, see Section 5.1, "Using iManager to Manage CIFS," on page 31.
- **Migrating to a Linux Platform:** NetWare® CIFS can be migrated to CIFS on OES 2 Linux by using either the new Migration Tool or the miggui command line utility. For details, see Chapter 6, "Migrating CIFS from NetWare to OES 2 SP2 Linux," on page 51.

Planning and Implementing CIFS

3

Planning and implementing CIFS on an Open Enterprise Server (OES) 2 Linux server requires you to understand the information and requirements discussed in the following sections:

3.1 Planning for CIFS

The key factors to consider for implementing and enabling Novell® CIFS on your enterprise servers are:

- Upgrading from OES 2 Linux to OES 2 SP2 Linux on your enterprise servers. For details on installing CIFS on OES 2 SP2 Linux, see Chapter 4, “Installing and Setting Up CIFS,” on page 21.
- Moving from NetWare® to an OES 2 Linux setup. For details see, Chapter 6, “Migrating CIFS from NetWare to OES 2 SP2 Linux,” on page 51.

3.2 CIFS System Prerequisites

To access CIFS servers running on an OES 2 Linux server, client computers must be connected to the network, properly configured to run NBT (NetBIOS over TCP/IP), and meet the following basic minimum requirements:

3.2.1 Server Operating System Requirements

Novell Open Enterprise Server 2 Support Pack 1 and later.

3.2.2 Server Hardware Requirements

Same as the OES 2 SP2 Linux hardware requirements. For details, see “Meeting All Server Software and Hardware Requirements” in the *OES 2 SP2: Installation Guide*.

3.2.3 Client Operating System Requirements

- Windows XP SP2 and SP3.
- Windows 7 Client.

- Windows Vista Business SP1 and 64-bit SP1, Enterprise SP1 and 64-bit SP1, and Ultimate SP1 and 64-bit SP1.
- Mac Client Support.
- SUSE® Linux Enterprise Desktop versions.
- Any NFS* platform capable of NFS v2, NFS v3, or NFS v4, such as Linux, or FreeBSD*.

3.2.4 Package Dependencies

Use the following checklist to verify CIFS dependencies before proceeding:

- ❑ All Novell CIFS users must be in eDirectory™. Linux-only users are not supported.
- ❑ Novell CIFS supports only Novell Storage Services™ (NSS) volumes.
- ❑ NCP™ should be up and running for Novell CIFS to function properly.
- ❑ If your eDirectory replica is stored on an eDirectory server earlier than 8.8.3, ensure you upgrade the server using the *Security Services 2.0.6 patch* (http://download.novell.com/Download?buildid=LYlbZMAom6k~).

3.3 Constraints, Limitations, and Issues

- Section 3.3.1, “Co-existence Issues,” on page 18

3.3.1 Co-existence Issues

Do not install any of the following service combinations on the same server as Novell CIFS. Although not all of the combinations cause pattern conflict warnings, Novell does not support any of the combinations shown:

- ❑ File Server (SLES 10 - Samba).
- ❑ Novell Domain Services for Windows (DSfW).
- ❑ Any other Samba implementation.
- ❑ Xen Virtual Machines on the host.

Table 3-1 *Novell CIFS and Novell Samba Comparison*

Item	Novell CIFS	Novell Samba
Authentication	Password policy is required to allow cifs users to authenticate to eDirectory.	A Samba-compatible Password Policy is required for compatibility with Windows workgroup authentication.

Item	Novell CIFS	Novell Samba
File system support	NSS is the only file system supported for this release.	It is recommended (but not required) that you create Samba shares on NSS data volumes. NSS is fully integrated with eDirectory for easy management , and using an NSS volume allows you to take advantage of the rich data security model in NSS. You can use either iManager for the nssmu utility to create an NSS volume on an OES2 Linux server. For instruction on how to setup an NSS volume, see Managing NSS volumes in the OES2 SP2:File Systems Management Guide.
LUM and Samba enablement	LUM and Samba enablement are not required.	Users must be enabled for LUM and Samba and assigned to a Samba group.

3.4 What's Next

To proceed with CIFS installation on an OES 2 Linux server, continue with Chapter 4, “Installing and Setting Up CIFS,” on page 21.

Installing and Setting Up CIFS

4

Novell® CIFS is not installed by default when you install Open Enterprise Server (OES) 2 SP2 Linux. CIFS needs to be selected so it can be installed during OES 2 Linux installation. This section provides the CIFS installation requirements and procedures.

4.1 Preparing for CIFS Installation

4.1.1 Product Interdependencies

CIFS has product interdependencies that must be considered:

- NMAS™ (Novell Modular Authentication Services).
- NICI (Novell International Cryptographic Infrastructure).

CIFS depends on NMAS for name resolution and authentication of CIFS users. NMAS is dependent on NICI for encryption and decryption services. A problem with any of these products causes CIFS users to be denied access to an OES 2 Linux server.

4.1.2 Prerequisites

To properly install and configure CIFS, ensure that the following prerequisites are met:

- ❑ You are running an OES 2 SP2 Linux server. For more information on installing OES 2 Linux, see the *OES 2 SP2: Installation Guide*.
- ❑ You have a Universal Password. Read “Deploying Universal Password” in the *Novell Password Management Administration Guide (http://www.novell.com/documentation/password_management32/pwm_administration/data/allq21t.html)*.

  The Universal Password includes the ability to create password policies. It also removes the need to maintain two separate passwords for CIFS users.
- ❑ NMAS is installed on or added to an OES 2 Linux server that has a read/write eDirectory™ replica of the eDirectory partition where the User objects reside.

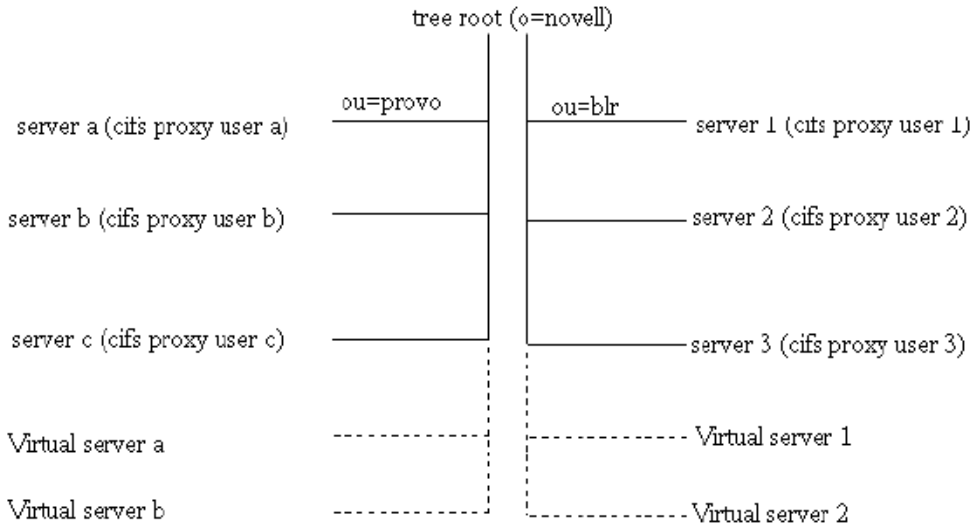
  NMAS is automatically installed. For more information on NMAS, see the *NMAS 3.2 Administration Guide* (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/a20gkue.html).

- ❑ Novell iManager 2.7.3 is installed, configured, and running. For more information on iManager installation and administration, see the *Novell iManager 2.7.3 Administration Guide*.
- ❑ Stop all the running Samba daemons before installing CIFS. Use the following commands:
  - `/etc/init.d/smb stop`
  - `/etc/init.d/nmb stop`

4.1.3 Required Rights and Permissions for a CIFS User/ Administrator

- ❑ The NDS user/administrator needs supervisor rights over the container where the server object is installed.
- ❑ The NDS user/administrator needs root permissions to install CIFS on an OES 2 Linux server.
- ❑ The NDS user/administrator needs read, write, create, modify rights over the password policies sub-container of the security container, for the following reasons:
  - Adding the CIFS default policy to the password policies.
  - Modifying policies selected for CIFS, so that the proxy user can read passwords for users attached to the policy.

Example for CIFS Cluster Rights



The *cifs proxy user a*, *cifs proxy user b*, and *cifs proxy user c* have the rights to read the eDirectory CIFS attributes under *ou=provo* (*Virtual server a* and *Virtual server b*). Hence if these virtual servers are hosted in any of these three nodes, the configuration is read by the CIFS service in the corresponding node.	The *cifs proxy user 1*, *cifs proxy user 2*, and *cifs proxy user 3* have rights to read the eDirectory CIFS attributes under *ou=blr* (*Virtual server 1* and *Virtual server 2*). Hence if these virtual servers are hosted in any of these three nodes, the configuration is read by the CIFS service in the corresponding node.

If the virtual server requires to be migrated across the branches, then the cifs proxy users have to be given explicit rights on those branches such that the CIFS attribute information can be read.

The attributes for which the cifs proxy user requires rights are, *nfapCIFSServername*, *nfapCIFSComment*, *nfapCIFSShares*, and *nfapCIFSAttach*. These attributes must have read, write, and compare rights. If the rights are defined on the branch(preferable), then the inherit rights also have to be provided.

In this example, if *Virtual server 2* is to be hosted on node server c, then *cifs proxy user c* must be provided access to read the attributes of *Virtual server 2*. The rights for the above mentioned attributes can be provided at *ou=blr* for *cifs proxy user c*. Hence the same rights holds good for hosting *Virtual server 1* too.

4.2 Installing and Configuring a CIFS Server through YaST

Follow this procedure to install and configure the CIFS services on an OES 2 SP2 Linux server in either of the following cases:

- Installing CIFS with the bundle of products during OES 2 SP2 Linux installation.
- Installing only the Novell CIFS service and its dependencies on an existing OES 2 SP2 Linux server.

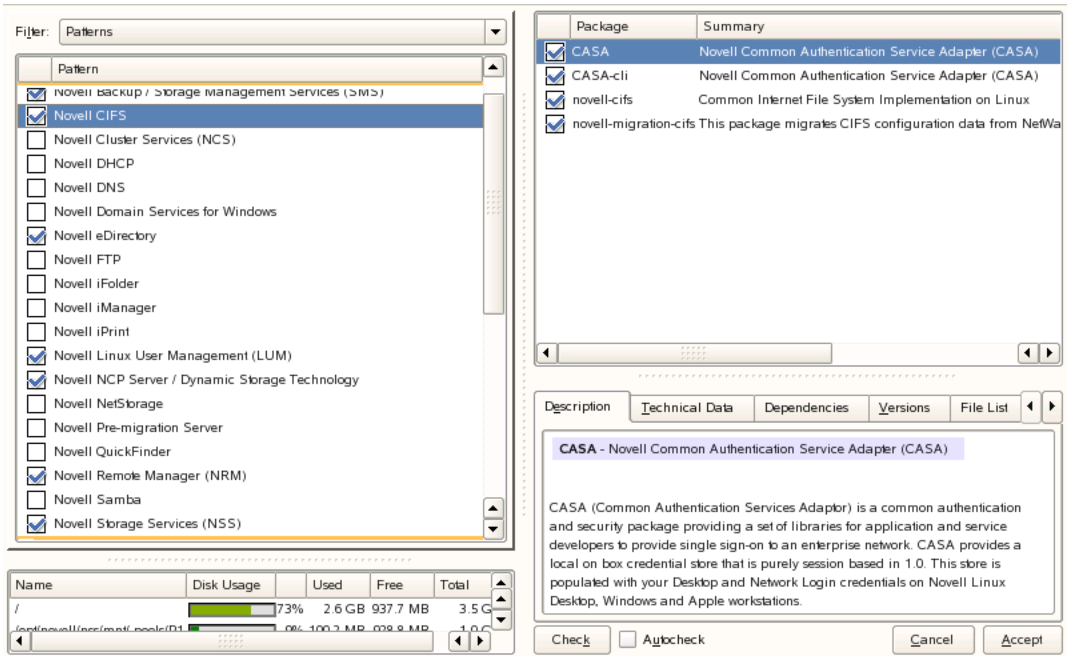
Before you begin, ensure that you have the required eDirectory admin credentials to proceed, if you are installing CIFS after installing OES 2 SP2 Linux.

1. Launch YaST, using one of the following methods:

   From your Desktop: Click *Computer* > *More Applications* > *System* > *YaST*.

   or

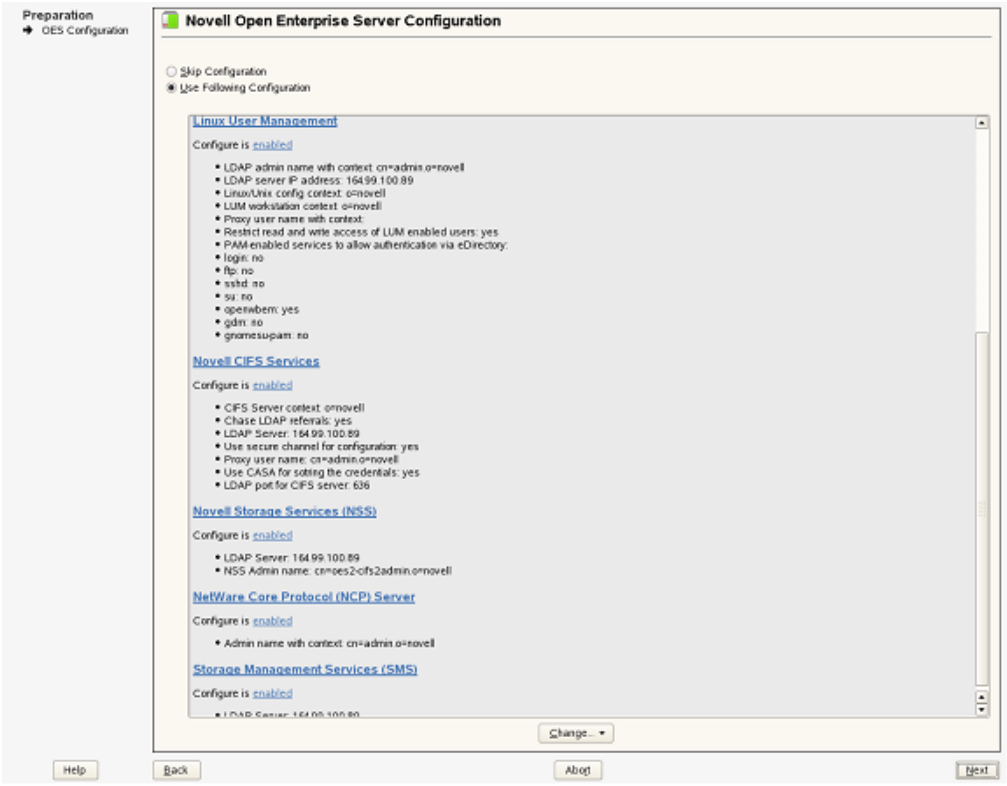
   From your Terminal: Run the `yast2` command on the server console.
2. Click *Group* > *Open Enterprise Server* > *OES Install and Configuration*.
3. Select *Novell CIFS* from the software patterns listed.



IMPORTANT: By default, the CIFS dependency packages are selected: Novell eDirectory, Novell Linux User Management (LUM), NetWare Core Protocol Server (NCP), Novell Remote Manager (NRM), and Novell Storage Services (NSS), in addition to other OES 2 SP2 default dependencies or other services dependency packages.

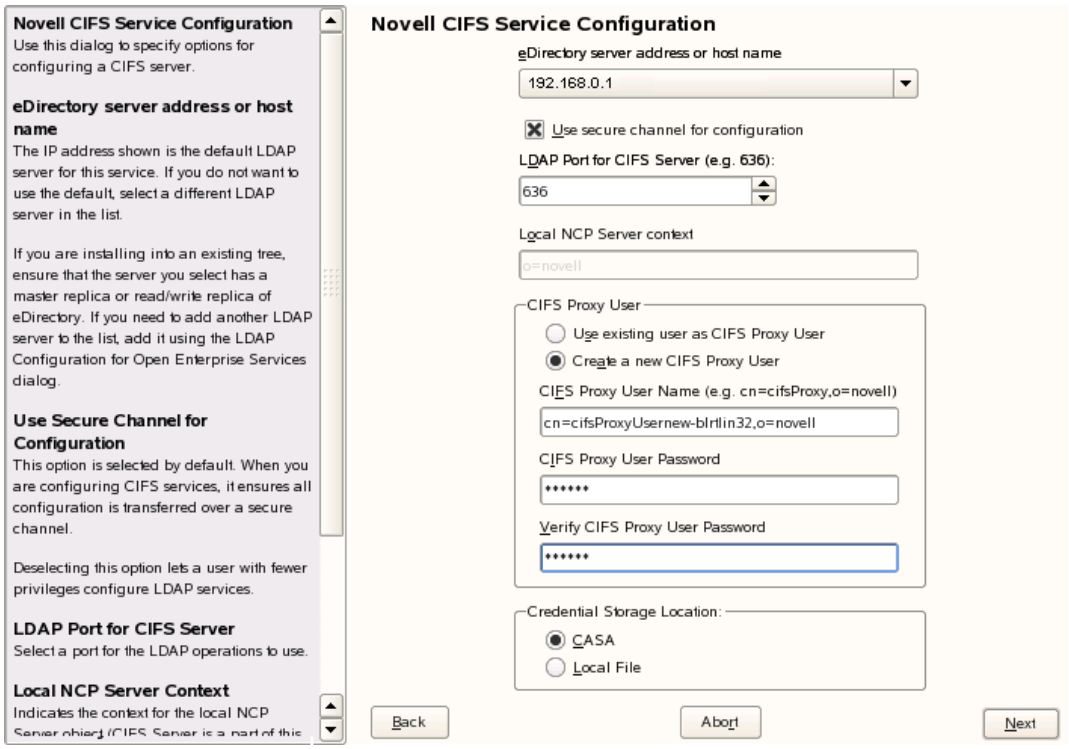
4 Click *Accept*.

The subsequent pages allow the administrator to configure CIFS on OES 2.



5 To change the default configuration settings for CIFS, click on the Novell CIFS service or click *Next* to continue with the default configuration.

NOTE: If you are installing CIFS after installing OES 2 SP2, you are prompted to enter the eDirectory admin password. Enter the password and click *OK* to proceed.



6 Fill in the following fields and click *Next*:

Parameter	Description
eDirectory server address or host name	This is the default eDirectory server IP address. Select from the drop-down list to change to a different server.
Use secure channel for configuration	By default, this option is selected. This is preferred.
LDAP port for CIFS Server	The default is 636. This is preferred. Do not change the default port value during a fresh installation of the tree. **NOTE:** If the OES 2 Linux server is attached to an existing tree, the administrator can change this to another LDAP port.
Local NCP Server context	Displays the NCP™ Server context.
CIFS Proxy User Name	Create a new proxy user. Use the format cn=proxyusername,o=company.
CIFS Proxy User Password	The password specified here is set in the CIFS configuration file. It cannot be changed. The maximum length is 256 characters.
Verify CIFS Proxy User Password	Re-enter the password for verification. It should be identical to the CIFS proxy user password.
eDirectory Contexts	The default is displayed. Select or add a new context, indicating where the user resides. Use the *Add* and *Delete* buttons to add and delete contexts.

Parameter	Description
Credential Storage Location	By default, the credential is stored in CASA. It is possible to store the credentials by using the Local File option. The password file is encrypted and encoded in the credential storage location.

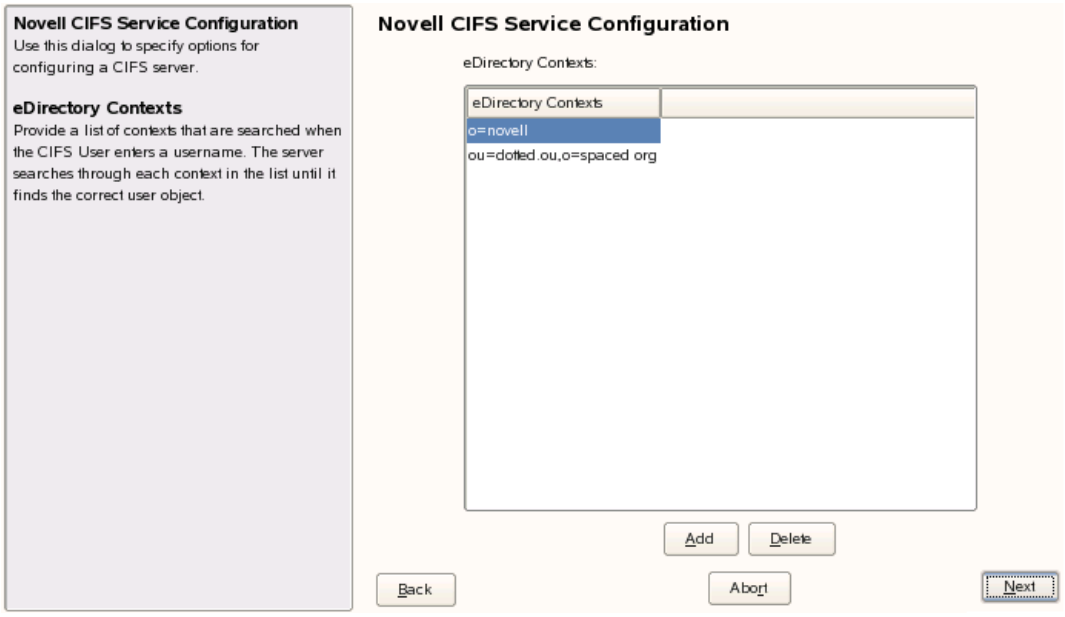
7 Select an *eDirectory context* from the available list.

If you want to add a CIFS user context, click *Add*. The format for specifying the context is as follows:

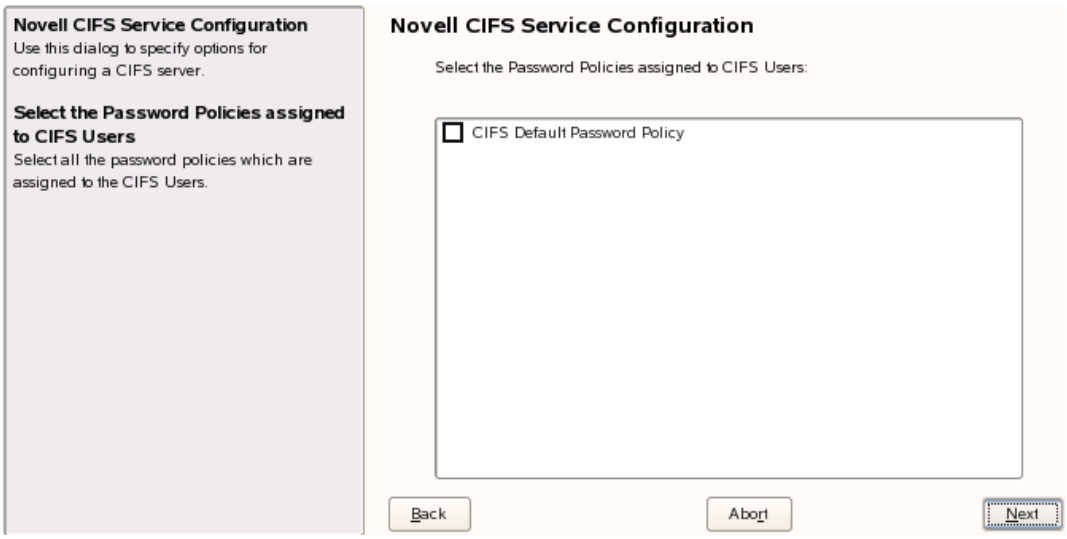
For example: `ou=eng,o=novell`

If you want to delete a CIFS user context, select a context from the available list and click *Delete*.

The CIFS user contexts are stored in `/etc/opt/novell/cifs/cifsctxs.conf`.

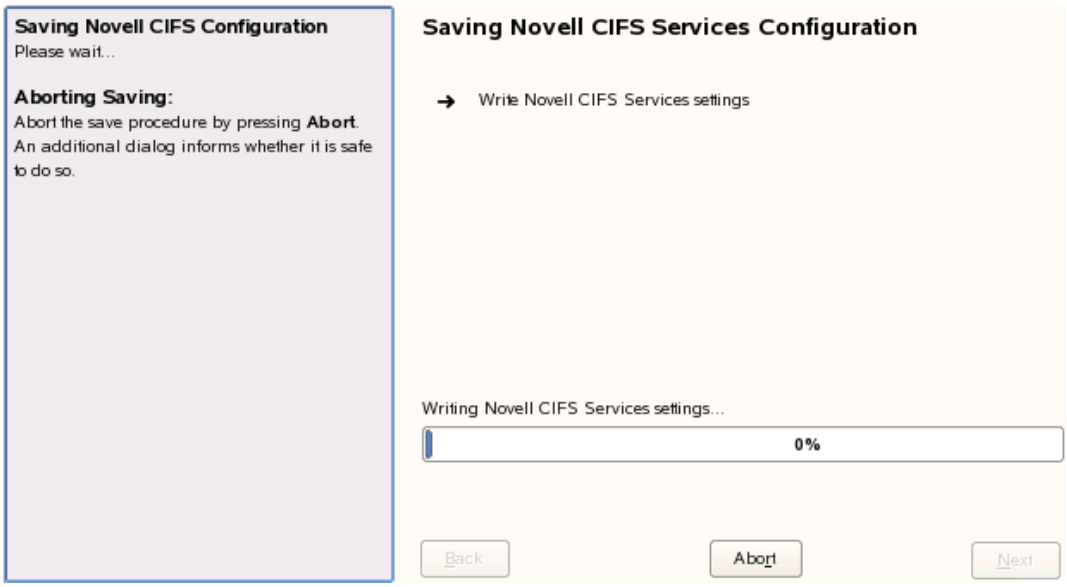


8 Select a *Password Policy* and click *Next*.



NOTE: The administrator also needs to be assigned to the CIFS password policy with a universal password assigned to it if the domain authentication is setup in the third party mode.

The CIFS configuration settings you specified are saved successfully on your OES 2 Linux server.



NOTE: Installing Novell CIFS also installs Audit and starts auditd.

4.3 Verifying Installation

Perform the following steps if you want to verify a successful installation. For troubleshooting your installation, see Section 10.1, “CIFS Installation and Configuration Issues,” on page 67.

4.3.1 Verifying Files and Folders

IMPORTANT: A file or folder loses its explicit trustee assignments if Rename/Move operations are performed on it. An administrator must re-assign trustee rights to the renamed or moved folder or file.

Run the following commands on the OES 2 server console:

1. Run the `ls /opt/novell/cifs/` command and verify that the `bin` and `schema` folders are present.
2. Run the `ls /opt/novell/cifs/bin` command and verify that the following files are present:
   - `cifs-config.sh`
   - `encrypt_password`
   - `migCifsC`
   - `migcifs.pl`
   - `novcifs`
   - `retrive_proxy_cred`
   - `getpwpolicies.sh`
   - `migCifsS`
   - `migcifs.sh`
   - `readCasaC`
   - `verify-user.sh`
3. Run ls /usr/sbin command and verify that the `cifsd` file is present.
4. Run the `ls /opt/novell/cifs/schema` command and verify that the following files are present:
   - `nfap.ldif`
   - `nfap.sch`
   - `password-policy.ldif`
5. If you selected CASA storage for storing the CIFS proxy user credentials, run the `CASAcli -l` command to verify if there is an entry for novell-cifs.

   or

   If you selected a local file for credential storage, verify the existence of the `.cifspwd.enc` file by running `ls /etc/opt/novell/cifs`.

4.3.2 Verifying the File Configuration Information

Verify whether the following files are populated with the information you specified while using YaST for configuration during installation:

1. Run `cat /etc/opt/novell/cifs/cifs.conf` and verify whether the configuration is the same as you specified during installation.
2. Run `cat /etc/opt/novell/cifs/cifsctxs.conf` and verify whether the context information is the same as you specified during installation.

4.4 Installing the CIFS iManager Plug-In

You must install the iManager plug-in for CIFS in order to access CIFS from iManager.

1. Launch iManager from your Web browser.

   For details, see "Accessing iManager" in the *Novell iManager 2.7.3 Administration Guide*.
2. Click *Configure* and go to *Plug-In Module Installation* > *Available Novell Plug-In Modules*.

   For details, see "Novell Plug-in Modules" in the *Novell iManager 2.7.3 Administration Guide*.
3. Select the CIFS plug-in *CIFS Management* from the list and click *Install*.
4. Exit iManager.
5. From OES 2 Linux server console, run one of the following commands to complete the plug-in installation:
   - `/etc/init.d/tomcat5 restart`
   - `rcnovell-tomcat5 restart`

4.5 What's Next

When the installation is complete, you can get started with CIFS administration activities. For details, see Chapter 5, "Administering the CIFS Server," on page 31.

Administering the CIFS Server

5

An administrator can start or stop CIFS and customize network access for CIFS users, enable or disable SMB signing, and perform other configuration and administration activities.

CIFS maintains a configuration file and context search information that is set up during installation. To access the CIFS share a CIFS search context is required. An eDirectory search context is created by default during the OES 2 Linux installation for all users who require access to the network. These contexts are saved in the context search file. When users specify a username, the CIFS component running on the server searches each context in the list until it finds the correct User object.

CIFS on an Open Enterprise Server (OES) 2 Linux server can be managed and administered either through iManager 2.7 or from the command line.

For details on how to install the CIFS iManager plug-in, see Section 4.4, "Installing the CIFS iManager Plug-In," on page 29.

For basic information on command line administration, see Section 5.2, "Using the Command Line to Manage CIFS," on page 43 or for complete details, see Appendix A, "NOVCIFS," on page 73.

5.1 Using iManager to Manage CIFS

You can manage CIFS services from iManager 2.7. The recommended method to configure, manage, and modify CIFS properties and parameters is using iManager.

NOTE: Admin equivalent/container admin users should be LUM enabled to manage the CIFS server through CIFS iManager plugin.

5.1.1 Prerequisites

- Install the CIFS iManager plug-in. For details, see Section 4.4, "Installing the CIFS iManager Plug-In," on page 29.
- Install CIFS on at least one OES 2 SP2 Linux server. For details on installing CIFS, see Chapter 4, "Installing and Setting Up CIFS," on page 21.
- Ensure that `ndsd` is running. Use `/etc/init.d/ndsd status` on the server console to check.

5.1.2 Selecting a Server to Manage

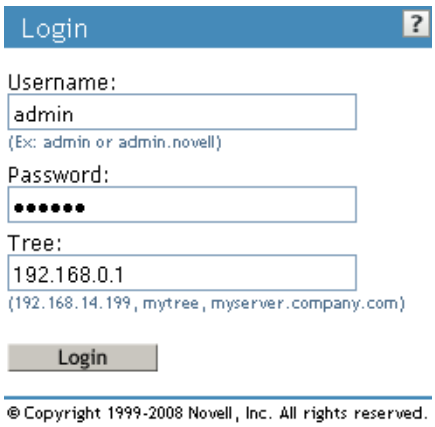
1 In a Web browser, specify the following in the address (URL) field:

`http://server_IP_address/nps/iManager.html`

For example:

`http://192.168.0.1/nps/iManager.html`

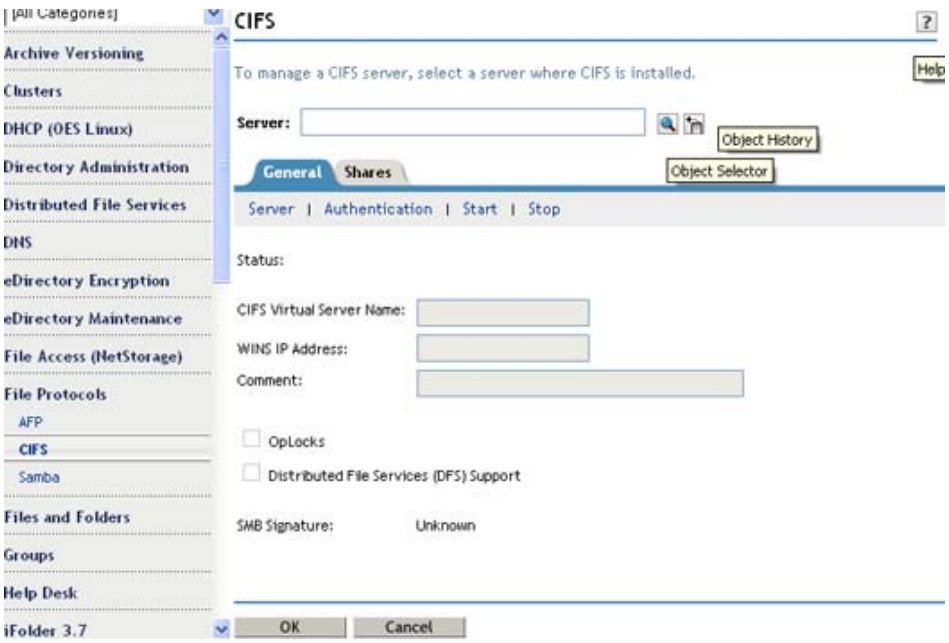
2 At the login prompt, specify the server administrator username and password and click *Login*.



For more information on iManager administration, see the *Novell iManager 2.7.3 Administration Guide*.

3 In the iManager application left frame, click *File Protocols* > *CIFS*.

The default CIFS parameters page is displayed. Use this page to configure and manage CIFS.



4 In the *Server* field, specify the OES 2 Linux server name.

or

Browse and select it from the object selector

or

Use the object history button to select it.

5 Verify the status of the server. If the CIFS server is stopped, click *Start* to start the CIFS server.

The *Status* changes to *Running* and all the CIFS properties are displayed on the screen.

If a Samba server is running, CIFS does not start. To resolve this problem, see "CIFS is not running with Samba" on page 67.

6 Continue with other administrative actions as necessary:

- Section 5.1.3, "Setting the CIFS Server and Authentication Properties," on page 33
- Section 5.1.4, "Managing CIFS Shares," on page 37
- Section 5.1.5, "Configuring a CIFS User Context," on page 41

5.1.3 Setting the CIFS Server and Authentication Properties

The server and authentication parameters can be set by using the parameters listed under the *General* and *Share* tabs on the default CIFS server page in the iManager.

For information on starting iManager and accessing the CIFS server, see Section 5.1.2, "Selecting a Server to Manage," on page 32.

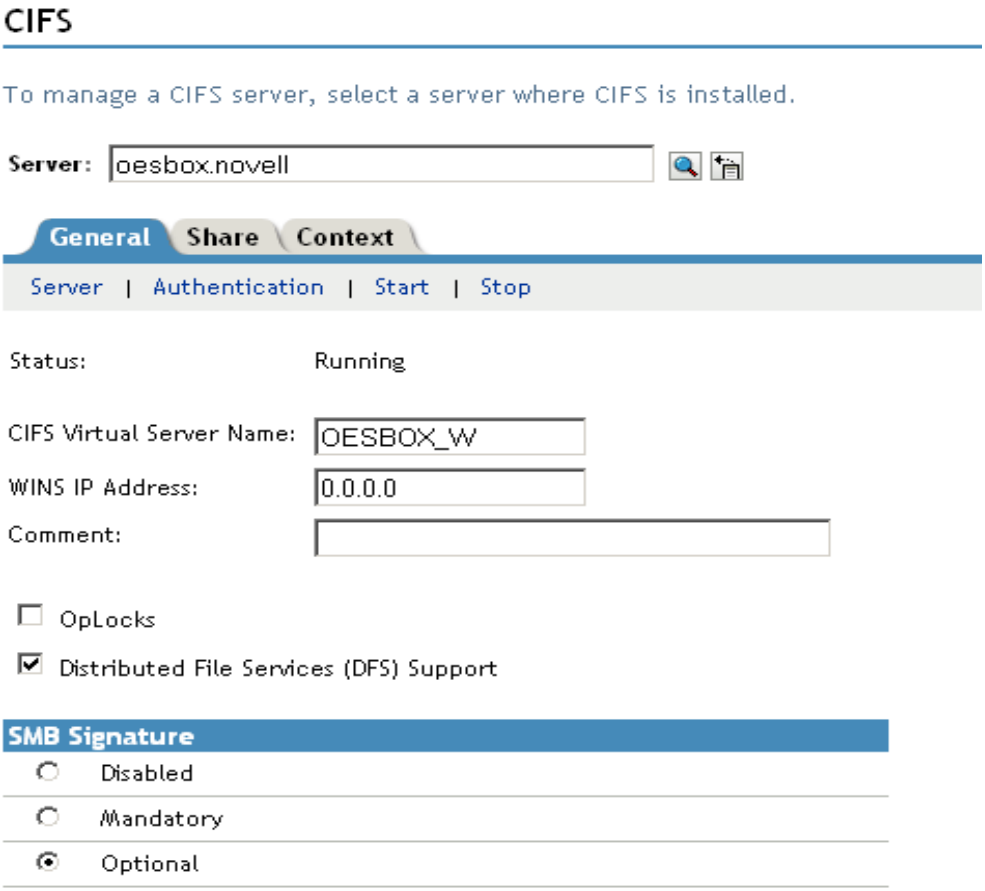
To change these parameters from command line, see Section 5.2.4, "Modifying the CIFS Configuration," on page 43

- "Setting CIFS General Server Parameters" on page 33
- "Enabling and Disabling SMB Signing" on page 35
- "Setting CIFS General Authentication Parameters" on page 35

Setting CIFS General Server Parameters

The General page contains the *Server* and *Authentication* properties tabs. By default, the Server Properties page is displayed. View or edit the server parameters on this page.

Figure 5-1 *CIFS General Server Parameters*



NOTE: For a virtual server, only CIFS Virtual Server Name, WINS IP Address, and Comment are not inherited from the real server. Hence only these parameters can be edited for CIFS on a shared pool server.

Table 5-1 *CIFS Server Page Parameters*

Parameter	Description
CIFS Virtual Server Name	The name of the server running CIFS services. The length can be a maximum of 15 characters. The default server name is the OES 2 Linux server name.
WINS IP Address	The address of the WINS server that locates the PDC, if the PDC and the server running CIFS are on different subnets.
Comment	A comment associated with the name of the server running CIFS services. This comment is displayed when viewing details. The maximum length is 47 characters. **IMPORTANT:** You should use single-byte characters in comments. Double-byte characters are not supported.

Parameter	Description
OpLocks (Opportunistic Locking)	Improves file access performance. The option is disabled by default.
Distributed File Services (DFS) Support	This option allows Distributed File Services support in CIFS. The option is disabled by default.
SMB Signature	By default, this is set to *Optional*. Select *Mandatory* or *Optional* or *Disabled*. For details, see "Enabling and Disabling SMB Signing" on page 35.

Enabling and Disabling SMB Signing

SMB signing supports message authentication, which prevents active message attacks. The authentication is provided by placing a digital signature into each SMB. The digital signature is then verified by both the client and the server. It can be set to mandatory or optional mode.

To use SMB signing mode, both the client and the server should be enabled for SMB signing. Use either Optional or Mandatory modes to enable it.

Optional mode: If SMB signing is set to the optional mode (the default mode after enabling it by using console commands), it automatically detects whether or not individual clients have SMB signing enabled. If a client does not have SMB signing enabled, the server does not use SMB signing for client communication. If a client has SMB signing enabled, the server uses SMB signing for client communication.

Mandatory mode: If you set SMB signing to mandatory mode, all clients must have SMB signing enabled or they cannot connect to the server. If SMB signing is set as mandatory on the server, clients cannot establish sessions with the server unless they have SMB signing enabled.

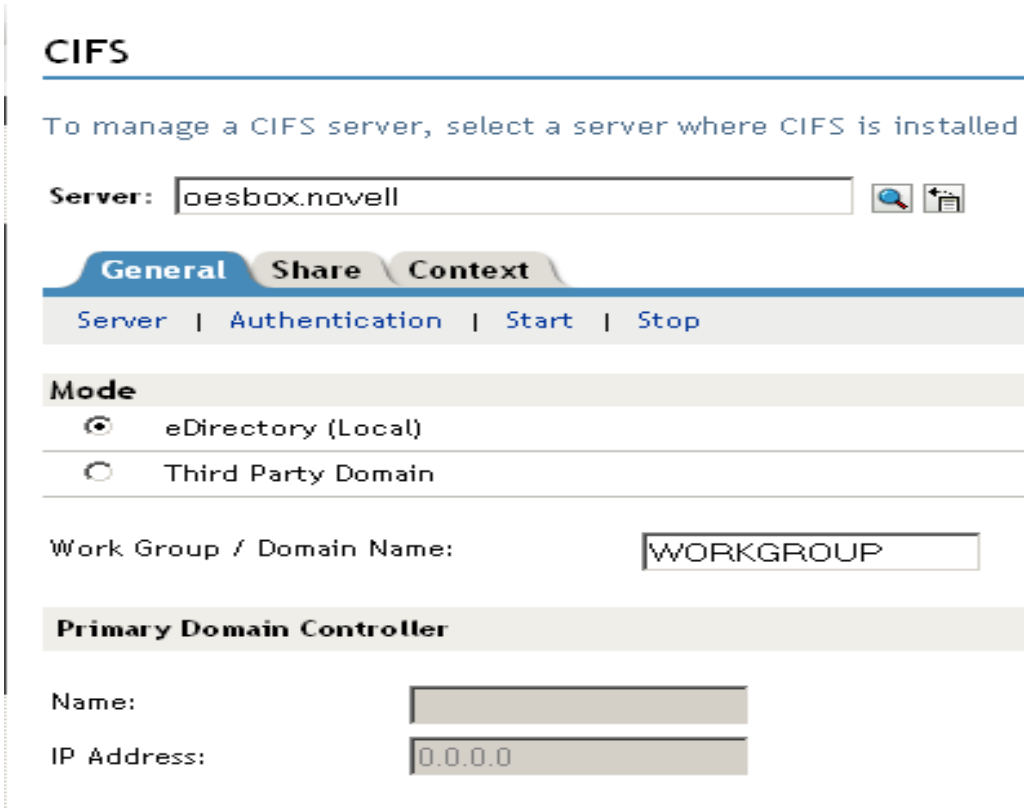
Disable mode: You can disable SMB signing by setting SMB signing to disabled mode.

IMPORTANT: After enabling or disabling SMB signing, or changing the mode to optional or mandatory, clients must reconnect in order for changes to take effect. For example, if SMB signing is enabled on the server, SMB signing is not in effect for individual clients until each of those clients reconnects.

Setting CIFS General Authentication Parameters

On the General page, select *Authentication* to view or edit the CIFS authentication parameters.

Figure 5-2 *CIFS Authentication Page Parameters*



NOTE: For a virtual server, only CIFS Virtual Server Name, WINS IP Address, and Comment are not inherited from the real server. Hence only these parameters can be edited for CIFS on a shared pool server.

Table 5-2 *CIFS Authentication Page Parameters*

Parameters	Description
Mode	Indicates the method of authentication used by CIFS. CIFS uses either eDirectory™ (local) or third-party Domain authentication mechanisms. ◆ **eDirectory (Local):** Clients are members of a workgroup. The server running CIFS services performs the user authentication. The login credentials (username and password) on an OES 2 Linux server must match the login credentials used by the client users. ◆ **Third Party Domain:** Clients are members of a domain. A Windows domain controller performs user authentication. The username and password on the domain controller must match the username and password used to log in to the Windows workstation. **IMPORTANT:** If you change the modes from Local to Third Party Domain or from Third Party Domain to Local, restart the CIFS server for the changes to take effect.
Work Group / Domain Name	The workgroup or domain to which the server belongs. Domain is a third-party domain.
Primary Domain Controller Name	The name of the PDC server. This is needed if the PDC is on a different subnet. This option should be used only when there is a valid reason for overriding WINS or DNS. This field can be changed only if *Third Party Domain* is selected.
Primary Domain Controller IP Address	The PDC server's static IP address. This is needed if the PDC is on a different subnet. This option should be used only when there is a valid reason for overriding WINS or DNS. This field can be changed only if *Third Party Domain* is selected. **IMPORTANT:** If this is not a static address, the server running CIFS services cannot contact the PDC when PDC reboots and the address changes.

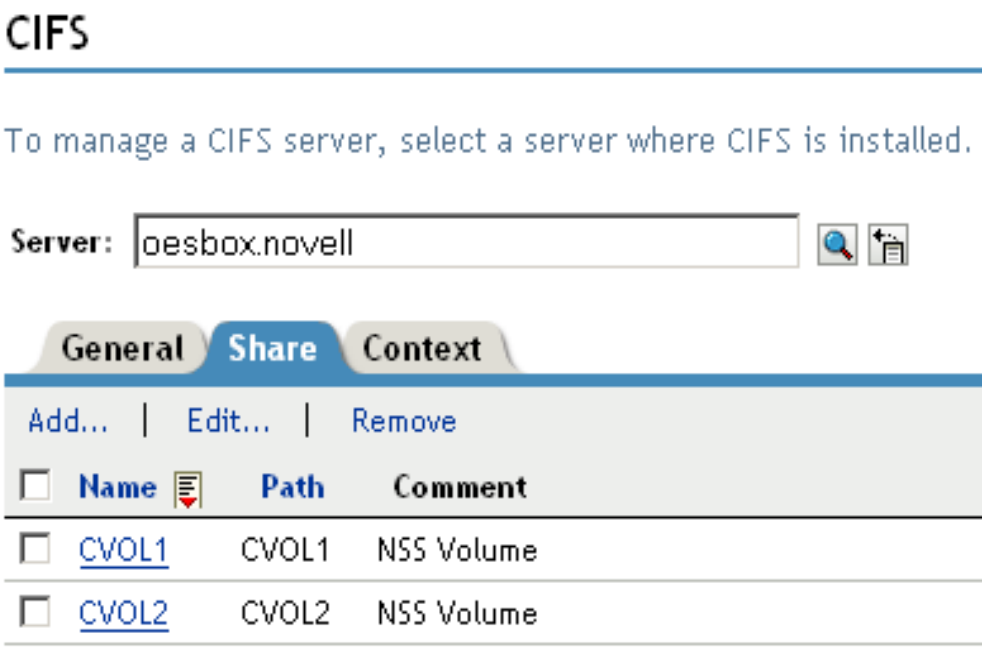
5.1.4 Managing CIFS Shares

The *Shares* tab on the default CIFS server page in iManager displays the CIFS share details. Use the Shares page to add a new share on the server to be specified as a sharepoint and to be accessible via the Network Neighborhood. NSS Volumes are added by default.

For information on starting iManager and accessing the CIFS server, see Section 5.1.2, "Selecting a Server to Manage," on page 32.

To manage CIFS Shares from command line, see Section 5.2.6, "Working with CIFS Shares," on page 45.

Figure 5-3 *CIFS Shares Page Parameters*



NOTE: If no shares are specified, all mounted volumes are displayed.

IMPORTANT: Double-byte characters are not supported in a Share name, Share path, or Comment.

Administrators can add, edit, and delete CIFS shares.

- "Adding a New CIFS Share" on page 38
- "Editing a CIFS Share" on page 39
- "Removing a CIFS Share" on page 40
- "CIFS Share Parameters" on page 41

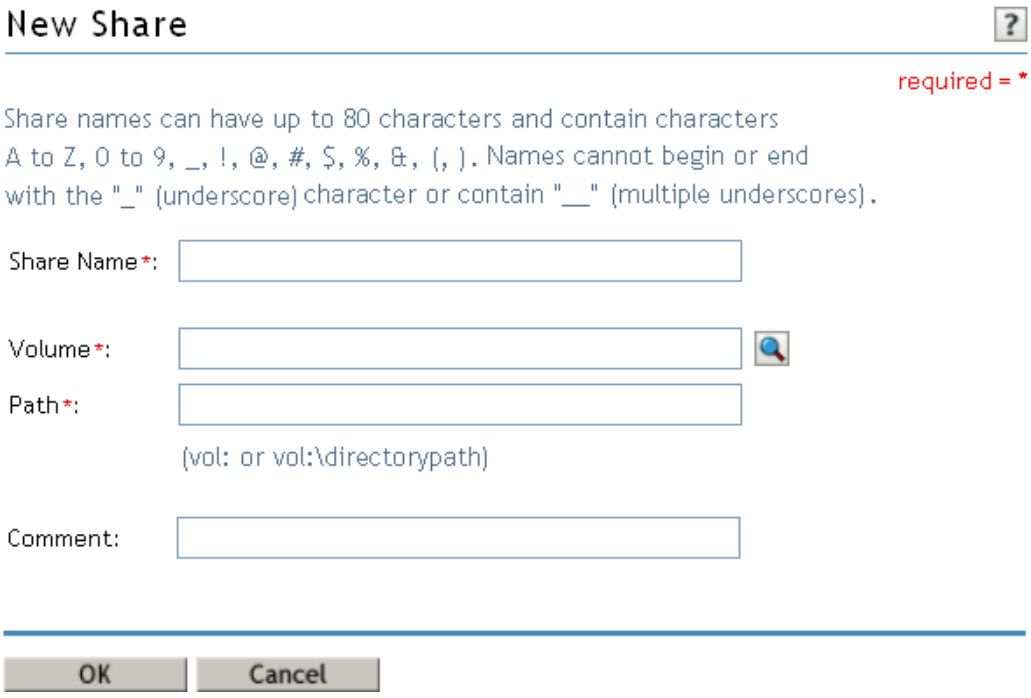
Adding a New CIFS Share

Before adding a new share, ensure that your CIFS server is started and running. For details on how to start the server, see Section 5.1.2, "Selecting a Server to Manage," on page 32.

NOTE: There is a limitation on the number of shares a CIFS server can host. For most configurations this limit is between 300 to 500 shares.

1 On the default CIFS server page in iManager click the *Shares* tab, then click *New*.

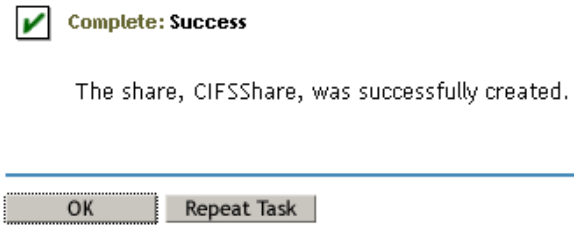
For information on starting iManager and accessing the CIFS server, see Section 5.1.2, "Selecting a Server to Manage," on page 32.



2 Specify the *Share Name, Volume, Path*, and *Comment* for the new share. For details, see Table 5-3 on page 41.

3 Click *OK* to save your changes.

On successful addition of a share, the following message is displayed.



Editing a CIFS Share

Before editing a share, ensure that your CIFS server is started and running.

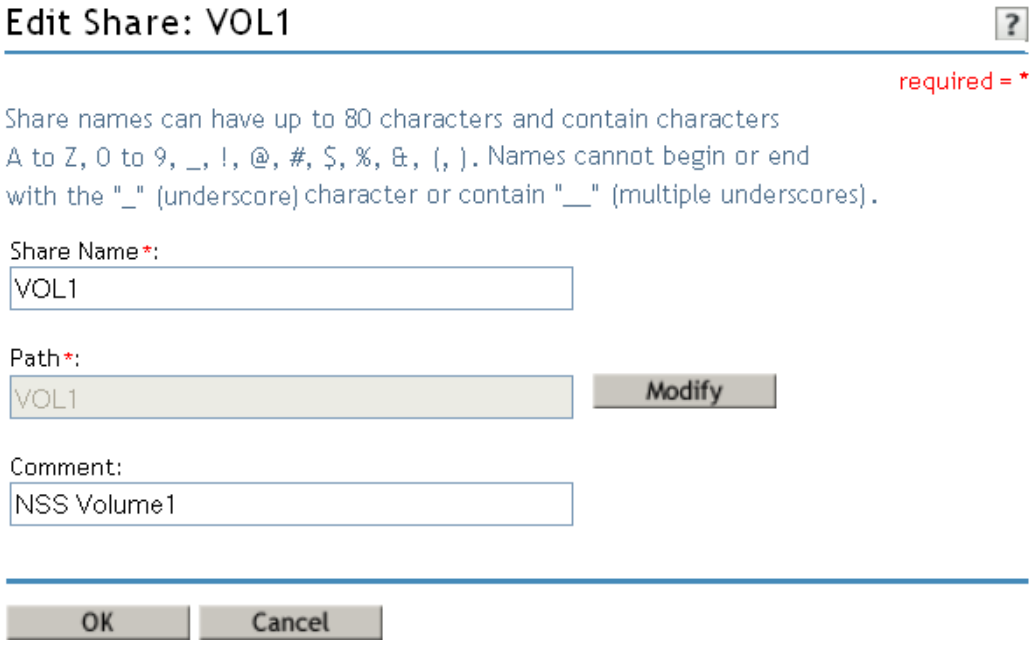
If you edit the default share name, a new share is created. However, the default share is still present with the same share name.

NOTE: All shares on a volume are removed on pool unmount.

For details on how to start the server, see Section 5.1.2, “Selecting a Server to Manage,” on page 32.

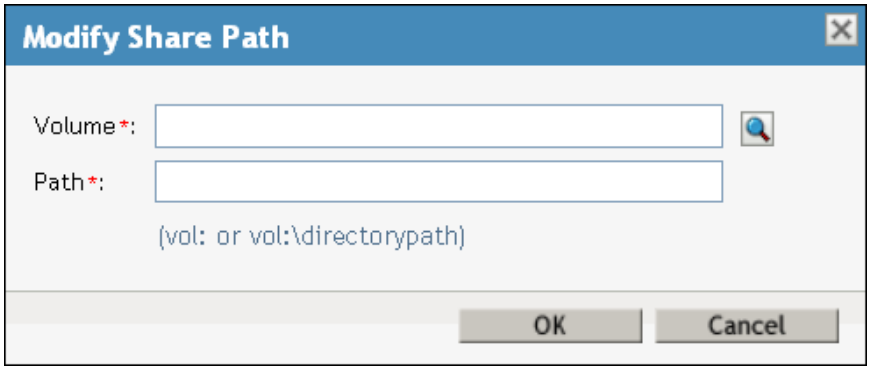
1 On the default CIFS server page in iManager click the *Share*s tab, then select a share from the list and click *Edit*, or click a particular share link to edit the share.

For information on starting iManager and accessing the CIFS server, see Section 5.1.2, “Selecting a Server to Manage,” on page 32.



2 Modify the *Share Name* or *Path* or *Comment* for the share. For details, see Table 5-3 on page 41.

3 Click the *Modify* button to modify the *Volume* and *Path* on the pop-up screen. For details, see Table 5-3 on page 41.



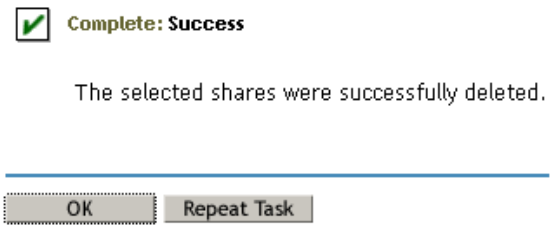
4 Click *OK* twice to save your changes.

Removing a CIFS Share

Before deleting a share, ensure that your CIFS server is started and running. For information on starting iManager and accessing the CIFS server, see Section 5.1.2, “Selecting a Server to Manage,” on page 32.

1 On the default CIFS server page in iManager click the *Share* tab, then select one or more shares from the list, then click *Remove*.

On successful deletion of the share the following message is displayed.



2 Either click *OK* to return to the main page or click *Repeat Task* to delete more shares.

CIFS Share Parameters

Use this table information to create and edit CIFS shares.

Table 5-3 *Shares Page Parameters*

Parameter	Description
Name	The name that the CIFS share uses for all the CIFS services and for display on Windows computers. For example, if you specify `Company Photos` as the share name associated with `vol1\graphics`, then Windows workstations browsing the network see `Company Photos` instead of `vol1\graphics`. A Share name can be up to 80 characters long and can contain any single-byte characters, but should not begin or end with an underscore _ or contain multiple underscores _.
Volume	The OES 2 volume name.
Path	The CIFS share path. This is the path to the server volume or directory that becomes the root of the sharepoint. This path may contain single-byte and multi-byte characters. **NOTE:** Do not end the path with a backslash (\).
Comment	A description for the sharepoint. The description appears in Network Neighborhood or My Network Places. The maximum length is 47 characters. Comment may contain single-byte and multi-byte characters..

5.1.5 Configuring a CIFS User Context

On the default CIFS server page in iManager click the *Context* tab to list, add, and delete the CIFS user contexts.

To configure a context search from the command line, see Section 5.2.7, “Configuring the CIFS Context Search File,” on page 45.

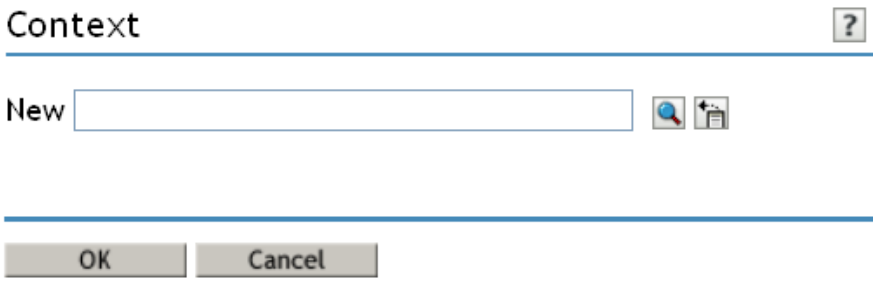
Figure 5-4 *CIFS Context Page*

- "Adding a New Context" on page 42
- "Removing a Context" on page 42

Adding a New Context

1 Click *Add* to add a new user context to CIFS.

Figure 5-5 *Add New Context*



2 Browse the Object Selector, select a context to add, then click *OK* to save.

Removing a Context

Select one or more contexts and click *Remove*.

5.1.6 Stopping CIFS

To stop a running CIFS server:

1 If the CIFS server status is *Running* on your screen, click *Stop* to stop the CIFS server.

The *Status* changes to *Stopped* and all the CIFS properties are dimmed on the screen.

5.2 Using the Command Line to Manage CIFS

Command line utilities are available to control the CIFS services. The main activities for CIFS services are described in this section. For information about specific CIFS commands, see Appendix A, "NOVCIFS," on page 73 or enter `man novcifs` at the command prompt.

- Section 5.2.1, "Starting CIFS," on page 43
- Section 5.2.2, "Stopping CIFS," on page 43
- Section 5.2.3, "Restarting CIFS," on page 43
- Section 5.2.4, "Modifying the CIFS Configuration," on page 43
- Section 5.2.5, "Anonymous Log In for CIFS," on page 44
- Section 5.2.6, "Working with CIFS Shares," on page 45
- Section 5.2.7, "Configuring the CIFS Context Search File," on page 45

5.2.1 Starting CIFS

Use the `rcnovell-cifs start` command to start CIFS.

NOTE: If a Samba server is running, CIFS does not start. To resolve this problem see "CIFS is not running with Samba" on page 67.

5.2.2 Stopping CIFS

Use the `rcnovell-cifs stop` command to stop CIFS.

5.2.3 Restarting CIFS

Use the `rcnovell-cifs restart` command to restart CIFS.

5.2.4 Modifying the CIFS Configuration

The configuration settings are taken directly from the CIFS iManager settings. The recommended method to modify CIFS configuration is using iManager. For details, see Section 5.1.3, "Setting the CIFS Server and Authentication Properties," on page 33.

Use the following steps to edit the CIFS configuration from command line:

1. Use any text editor to open the `cifs.conf` file from `/etc/opt/novell/cifs/` directory.

   IMPORTANT: It is recommended to not change the default settings in this file, unless there is an absolute need to do so.

2. Use the following information to change the configuration:
   - In the AUTHENT section, set the mode to either local or domain. Local is preferred. For example, -AUTHENT local.

     IMPORTANT: A domain mode is a third-party domain. For this mode, a Windows domain controller performs user authentication. A local mode is an eDirectory mode. For this mode, the server running CIFS services performs the user authentication.

   - In the COMMENT section, specify an appropriate user comment to associate with the sharepoint.
   - In the DOMAIN / WORKGROUP section, set the domain to use.

     IMPORTANT: For third-party domains, specify the domain name. For the local option, set the workgroup.

   - Leave the OPLOCKS [yes/no] set to yes.
   - Leave the UNICODE [yes/no] set to yes.
   - In the -PDC [PDC_NAME] [PDC_IP_ADDR] section, specify the PDC name and IP address.
   - In the -WINS [WINS_IP_ADDR] section, specify the WINS IP address. Set this if the PDC and the server running CIFS are on different subnets.
   - In the -SUBNET [subnet] section, specify the subnet value, if required.
3. Restart the CIFS server by using the `rcnovell-cifs restart` command for the configuration changes to take effect.

5.2.5 Anonymous Log In for CIFS

Anonymous log in for CIFS is used to map to the CIFS share. A username and password is not required to map to the share. Anonymous login can be enabled/disabled at server level using the following novcifs command:

```
novcifs -e [yes/no]
```

Public rights must be set on the volume (or folder) using Novell Client or iManager.

WARNING: For security considerations, do not provide supervisor rights to the public objects as it allows access to all the secured folders.

5.2.6 Working with CIFS Shares

CIFS sharepoints can be added, removed, and displayed by using the command line interface or server console. CIFS shares cannot be added to virtual server object using command line (novcifs). If the shares are added on cluster resource using command line, then all the shares are lost if the resource leaves that node.

NOTE: Whenever a CIFS service is restarted on a node that hosts a cluster resource, then the resource must be moved to offline and then got online or migrated to another node and brought back to the original node such that rebinding occurs.

You can view details about how CIFS shares are listed and configured by using any of the following commands at the server console or prompt:

To manage CIFS shares using iManager, see Section 5.1.4, “Managing CIFS Shares,” on page 37.

- “Adding a New Sharepoint” on page 74
- “Removing a Sharepoint” on page 74
- “Displaying the List of Sharepoints” on page 74
- “Displaying the Specific Sharepoint Details” on page 74
- “Enabling or Disabling SMB Signing” on page 74.

5.2.7 Configuring the CIFS Context Search File

NOTE: The recommended method is to use iManager to configure the search context. For details, see Section 5.1.5, “Configuring a CIFS User Context,” on page 41.

5.3 Locks Management for CIFS

Cross-Protocol locks help prevent the same file from being concurrently accessed for modifications. This option ensures that a file is updated correctly before another user, application, or process can access it.

- **Byte-Range Locking:** Two types of byte-range locking are used:
  - **Exclusive Lock:** The locked byte range is read/write for the holder of the lock and deny-all for all others. A write lock on a byte range is acquired by an application that intends to write data into that byte range, and does not want other applications to be able to read or write to the byte range while it is accessing that byte range. A write lock on a given byte range is exclusive. It is granted to only one requester at a time. A write lock denies other applications the ability to either read or write to the locked byte-range.
  - **Shared Lock:** Also called a non-exclusive byte-range lock. The locked byte range is read-only for the holder of the lock and deny-write for all others. A read lock on a byte range is normally acquired by an application that intends to read data from the byte range, and does not want other applications to be able to write to the byte range while it is performing the read operation. A read lock on a given byte range is sharable, which means it is granted to multiple requesters concurrently. However, it is incompatible with a concurrent write lock on the same byte range. A read lock denies other applications the ability to write to the locked byte range. In environments that implement advisory record locking

rather than mandatory record locking, a read lock simply advises other applications that they should not write to the locked byte-range, even though they are technically able to do so.

- **Oplocks:** Improves File Access performance and is disabled by default.

For more information, see "Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks" in the *OES 2 SP2: NCP Server for Linux Administration Guide*.

5.4 Third Party Authentication

Use the steps below for a third party authentication:

- Create the same user in eDirectory and third party machines with same password.
- In eDirectory, assign a CIFS Password Policy to the user.
- Assign a Universal Password for the same user.

NOTE: The windows client may be required to log in as the same user with same password to access the CIFS shares when using third party authentication.

5.5 DFS Junction Support in CIFS Linux

CIFS must be configured to support DFS junctions. By default, DFS junction support is disabled. You must enable it on host (server that hosts the junction) and target (server that is pointed by the junction) servers in order for the junctions to work. The junctions that point to subdirectories are also supported with CIFS Linux.

5.5.1 Prerequisites

- Unicode™ must be enabled.
- DFS must be enabled for CIFS on all the host and target servers.
- Both host and target CIFS servers must be running.
- The VLDB server must be running.

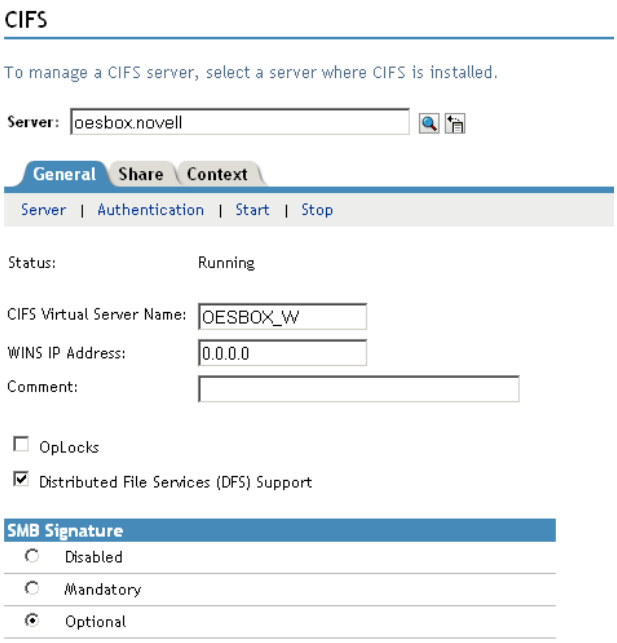
IMPORTANT: The CIFS clients accessing DFS junctions must be DFS aware. smbclient on Linux may not work appropriately in case of junctions as it is not DFS aware.

5.5.2 Enabling DFS Support

Use the instructions in this section to enable DFS junction support in CIFS Linux:

1. In iManager, click *File Protocols* > *CIFS*.
2. Browse to locate and select the server you want to manage.

Figure 5-6 *Enabling DFS Support*



3 Select the check box for *Distributed File Services (DFS) Support* to enable the DFS support in CIFS Linux.

4 Click *OK*.

5.5.3 Limitations

- Junctions in NetWare cannot point to volumes in Linux and vice versa, that is, junctions are not supported across platforms.
- DFS is available only if Unicode (UTF8 format) is enabled.
- Only CIFS shares are enabled with DFS support.

5.6 Problems Following DFS Junctions with CIFS in Windows 2000/XP Releases

- Section 5.6.1, “Windows Unable to Resolve the NetBIOS Name of the CIFS Server,” on page 48
- Section 5.6.2, “After Modifying the Junction Target, Accessing the Junction Still Leads to the Old Target,” on page 49

5.6.1 Windows Unable to Resolve the NetBIOS Name of the CIFS Server

Clients using Windows 2000 Service Pack 4 and Windows XP Service Pack 2 might have problems following DFS junctions over CIFS because of a defect in Windows. (This problem exhibits itself in a pure Windows environment.) When using DFS with CIFS, the CIFS server and Windows clients are on different IP subnets. In this case, the client must have a way to resolve the CIFS server name in order for DFS to work. This is a Microsoft/CIFS requirement, not a CIFS Linux requirement.

NOTE: This problem does not affect Windows clients that use the Novell Client™.

There are multiple ways the client can resolve the CIFS server name:

- Install the Novell Client on the client machine.
- Configure both the client and server for the same WINS server
- Configure both the client and server to use the same DNS server
- Modify the `hosts` file for all client computers with appropriate entries for any volumes on OES servers that use DFS junctions

To modify the `hosts` file on a client:

1. In a text editor, open the `hosts` file and modify the hosts file.
   - **Windows 2000:** `c:\WINNT\system32\drivers\etc\hosts`
   - **Windows XP:** `c:\windows\system32\drivers\etc\hosts`

   If you do not have `hosts` file, create the file.
2. For all the host and target servers, add a line at the end of the file that identifies the IP address and NetBIOS name of the data server.

   192.168.1.1 servername_W

   Replace *192.168.1.1* with the actual IP address and *servername* with the name of your server.

   IMPORTANT: Modifying the CIFS server name of the virtual server using iManager is not allowed. However, it is possible to modify the CIFS server name for a physical server.

   We recommend that you do not modify the CIFS server name of the physical server that is the DFS target.

   For example, suppose you have the following server:

   - Server IP address: `10.10.1.1`. If the DFS target is a cluster resource, then mention <*Cluster IP address*> or <*Cluster Resource IP address*>
   - Server name: `USERSVR`
   - NetBIOS server name: `USERSVR_W`

     If the target of the junction is a cluster resource, mention the <*Cluster IP address*> or <*Cluster Resource IP address*> and instead of server name, mention the cluster name.

   The line you add to the hosts file is:

   ```
   10.10.1.1 USERSVR_W
   ```

NOTE: The string length of the NetBIOS name should not exceed 15 chars. The hostname or the first 13 characters from the hostname, whichever is shorter is considered and appended with *_W* at the end to frame the standard NetBIOS name.

3 Save and close the `hosts` file.

4 If necessary, repeat Step 1 to Step 3 on each client computer, or create a `hosts` file and distribute it to the client machines.

5 On each client, map a network drive to the user's data volume.

Continuing the example above, the user could map to `\\10.10.1.1\VOL1` or to `\\USERSVR_W\VOL1`.

5a In the Windows Explorer file manager, click *Tools* > *Map Network Drive*.

5b In the *Folder* field, type one of the following:

`\\192.168.1.1\volumename`

`\\servername_W\volumename`

Replace `192.168.1.1` with the actual IP address or `servername` with the hostname of your server.

5c Select *Reconnect at Logon*.

5d Click *Finish*.

5.6.2 After Modifying the Junction Target, Accessing the Junction Still Leads to the Old Target

Windows does not prompt the server everytime to resolve the junction every time the junction is accessed. It prompts the server only for the first time and then caches it. When the junction is accessed the next time, Windows does not prompt CIFS server to resolve the junction but it makes use of the target location it received previously.

On restarting the Windows machine, if the same mapping is done, it points to correct location. Because there is no cached value, it prompts the CIFS server to provide the location of the target that the junction points to and gets the latest value from CIFS server.

5.7 What's Next

To learn how to use CIFS services as an end user, continue with Chapter 9, "Working with Client Computers," on page 63.

Migrating CIFS from NetWare to OES 2 SP2 Linux

6

The Open Enterprise Server (OES) 2 SP2 Migration Tool has a plug-in architecture that is made up of Linux command line utilities with a GUI wrapper. You can migrate CIFS from a NetWare® server to an OES 2 SP2 Linux server either by using the GUI Migration Tool or from the command line. For more information on NetWare CIFS, see the *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide*.

To get started with migration, see the *OES 2 SP2: Migration Tool Administration Guide*.

For more information on migrating CIFS, see "Migrating CIFS from NetWare to OES 2 SP2 Linux" in the *OES 2 SP2: Migration Tool Administration Guide*.

To access the CIFS migration man page with command information, enter `man migCifs` at the command prompt. For details on migCifs command options, see "Man Page for Migration" in the *OES 2 SP2: Migration Tool Administration Guide*.

Running CIFS in a Virtualized Environment

7

Novell CIFS runs in a virtualized environment just as it does on a physical NetWare® server, or on a physical server running Open Enterprise Server (OES) 2 Linux, and requires no special configuration or other changes.

To get started with virtualization, see "Introduction to Xen Virtualization (http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_basics.html)" in the *Virtualization with Xen (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html)* guide.

For information on setting up virtualized OES 2 Linux, see "Installing, Upgrading, or Updating OES on a Xen-based VM" in the *OES 2 SP2: Installation Guide* guide.

7.1 What's Next

To learn more about what you can do with CIFS on OES 2 Linux, continue with Chapter 5, "Administering the CIFS Server," on page 31.

Configuring CIFS with Novell Cluster Services for an NSS File System

8

Novell® Cluster Services™ 1.8.5 for Open Enterprise Server (OES) 2 Linux provides high availability, scalability, and security for your network while reducing administrative costs associated with managing client workstations.

This section describes how to set up Novell CIFS in a cluster so that Windows and Linux computers can use CIFS to access shared cluster resources on the network even when there is a server failure.

8.1 Benefits of Configuring CIFS for High Availability

With the OES 2 Linux cluster configured with CIFS protocols, users receive the following benefits of a clustered environment:

- Novell Cluster Services and Novell Storage Services™ (NSS), which are part of OES 2 Linux, combine with Novell CIFS to facilitate highly available CIFS access for users.
- Enabling and disabling CIFS for shared NSS pools has a single point of administration through the browser-based Novell iManager pool configuration or the console-based NSSMU monitoring GUI.
- The cluster-enabled CIFS share is automatically mounted and dismounted when the shared NSS pool's cluster resource is brought online and offline.
- The CIFS sessions of the users continue without interruption when the shared NSS pool is migrated or failed over to a different node in the cluster.

8.2 Cluster Terminology

The following terminology is used in this section when discussing the cluster environment:

- **Active node:** The cluster server that currently owns the cluster resource and responds to network requests made to shared volumes on that resource.
- **Passive node:** The cluster server that does not currently own the cluster resources but is available if the resource fails over or is migrated to it.
- **Active/Passive clustering:** The cluster includes active nodes and passive nodes. The passive nodes are used if an active node fails.

- **Virtual server:** A cluster-enabled pool and related services that appears to clients as a physical server but is not associated with a specific server in the cluster. This is the name of the virtual server as it appears to NCP™, AFP, and Linux Samba clients.
- **CIFS virtual server:** A cluster-enabled pool and the Novell CIFS service that appear to CIFS clients as a physical server but are not associated with a specific server in the cluster. This is the name of the virtual server as it appears to CIFS clients.
- **Cluster IP address:** Each cluster-enabled NSS pool requires its own static IP address. The IP address is used to provide access and failover capability to the cluster-enabled pool (virtual server). The IP address assigned to the pool remains assigned to the pool regardless of which server in the cluster is accessing the pool.
- **Load script:** A file that contains the cluster resource definition and commands that load services and load the NSS pool and its volumes for a given cluster resource. Load scripts are generated by default when you cluster-enable a pool, and are modified by using the Clusters plug-in for Novell Cluster Services.
- **Unload script:** A file that contains the cluster resource definition and commands that unload services and dismount the NSS pool and its volumes for a given cluster resource. Unload scripts are generated by default when you cluster-enable a pool, and are modified by using the Clusters plug-in for Novell Cluster Services.

8.3 CIFS and Cluster Services

Novell Cluster Services can be configured either during or after OES 2 SP2 installation. In a cluster, Novell CIFS for OES 2 SP2 Linux, is available only in ACTIVE/PASSIVE mode, which means that CIFS software runs on all nodes in the cluster. When a server fails, the cluster volumes that were mounted on the failed server fail over to that other node. The following sections give details about using Novell CIFS in a cluster environment:

- Section 8.3.1, “Prerequisites,” on page 56
- Section 8.3.2, “Using CIFS in a Cluster Environment,” on page 57

8.3.1 Prerequisites

Before setting up Novell CIFS in a cluster environment, ensure that you meet the following prerequisites:

- ❑ Novell Cluster Services 1.8.5 installed on OES 2 Linux servers

  For information on installing Novell Cluster Services, see “Installing Novell Cluster Services on OES 2 Linux” in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

  For information on managing Novell Cluster Services, see “Managing Clusters” in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

- ❑ Novell CIFS is installed on all the nodes in the cluster to provide high availability

  Follow the instructions in “Installing and Configuring a CIFS Server through YaST” on page 23.

8.3.2 Using CIFS in a Cluster Environment

Keep in mind the following considerations when you prepare to use CIFS in a cluster.

- Novell CIFS is not cluster-aware and is not clustered by default. You must install and configure Novell CIFS on every node in the cluster where you plan to give users CIFS access to the shared cluster resource.
- Novell CIFS runs on all nodes in the cluster at any given time.
- Novell CIFS is started at boot time on each node in the cluster. A CIFS command is added to the load script and unload script for the shared cluster resource. This allows Novell CIFS to provide or not to provide access to the shared resource through Virtual server IP.

NOTE: In CIFS, all the nodes should have similar server configuration, such as contexts and authentication mode.

The following process indicates how CIFS is enabled and used in a cluster environment:

1. **Creating Shared Pools:** To access the shared resources in the cluster environment through the CIFS protocol, you create the shared pools either by using the NSSMU utility or the iManager tool and selecting CIFS as an advertising protocol. For requirements and details about configuring shared NSS pools and volumes on Linux, see "Configuring Cluster Resources for Shared NSS Pools and Volumes" in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.
2. **Creating a Virtual Server:** When you cluster-enable an NSS pool, an NCS:NCP Server object is created for the virtual server. This contains the virtual server IP address, the virtual server name, and a comment.
3. **Creating a CIFS Virtual Server:** When you cluster-enable an NSS pool and enable that pool for CIFS by selecting CIFS as an advertising protocol, a virtual CIFS server is added to eDirectory™. This is the name the CIFS clients use to access the virtual server.
4. **Loading the CIFS Service:** When you enable CIFS for a shared NSS pool and when Novell CIFS is started at system boot, the following line is automatically added to the cluster load script for the pool's cluster resource:

   ```
   novcifs --add --vserver=virtualserverFDN --ip-addr=virtualserverip
   ```

   This command is executed when the cluster resource is brought online on an active node. You can view the load script for a cluster resource by using the Clusters plug-in for iManager. Do not manually modify the load script.
5. **Unloading the CIFS Service:** When you CIFS-enable for a shared NSS pool, the following line is automatically added to the cluster unload script for the pool's cluster resource:

   ```
   novcifs --remove --vserver=virtualserverFDN --ip-addr=virtualserverip
   ```

   This command is executed when the cluster resource is taken offline on a node. The virtual server is no longer bound to the Novell CIFS service on that node. You can view the unload script for a cluster resource by using the Clusters plug-in for iManager. Do not manually modify the unload script
6. **CIFS Attributes for the Virtual Server:** When you CIFS-enable a shared NSS pool, the following CIFS attributes are added to the NCS:NCP Server object for the virtual server:
   - nfapCIFSServerName (read access)
   - nfapCIFSAttach (read access)

- nfapCIFSComment (read access)
- nfapCIFSShares (write access)

The CIFS virtual server uses these attributes. The CIFS server proxy user must have default ACL access rights to these attributes, access rights to the virtual server, and be in the same context as the CIFS virtual server.

NOTE: If the CIFS server proxy user is in a different context, the cluster administrator should give access to these virtual server attributes for the proxy user.

8.4 Configuring CIFS in a Cluster

Perform the following tasks to configure or enable CIFS and make it available on a cluster environment:

- Section 8.4.1, “Prerequisites,” on page 58
- Section 8.4.2, “Creating Shared Pools and Accessing Sharepoints,” on page 58
- Section 8.4.3, “Using a Pre-existing Cluster Pool for CIFS,” on page 60

8.4.1 Prerequisites

- The cluster environment is set up and ready
- All nodes in the cluster are installed and configured for CIFS
- All nodes in the cluster meet CIFS standalone server setup requirements and CIFS is running
- The shared disk is configured through iSCSI or SAN and is able to create shared pools

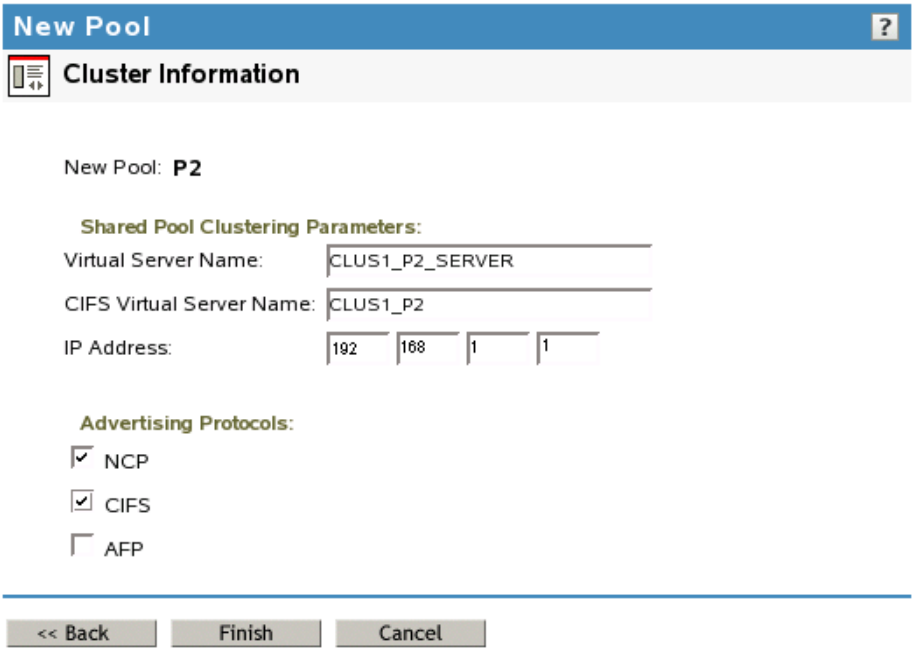
8.4.2 Creating Shared Pools and Accessing Sharepoints

You can configure, enable, and access the CIFS services by using iManager or by using NSSMU.

- “Using iManager to Create the Pool” on page 58
- “Using NSSMU to Create the Pool” on page 59

Using iManager to Create the Pool

1. Ensure that the “Prerequisites” on page 58 are met.
2. Log in to iManager, then click *Storage* > *Pools*.
3. Under *Server*, specify the cluster object or browse and select it.
4. Click *New*.
5. Specify the pool name and click *Next*.
6. Select the shared disk and allocate the pool size with a value of 0, then click *Next*.



7 Specify an *IP address*, ensure that you select *CIFS* under *Advertising Protocols*, then click *Finish*.

8 Use the `cluster status` command to verify that the created pool server is running.

For details, see "Console Commands for Novell Cluster Services" in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

9 Create volumes in the shared pools.

For details, see "Configuring Cluster Resources for Shared NSS Pools and Volumes" in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

10 Create sharepoints, provide access rights, and assign password policies for the CIFS virtual server or pool server. Use the same procedure that you used to configure the virtual or pool server CIFS through iManager.

For details, see Section 5.1, "Using iManager to Manage CIFS," on page 31, but ensure that you select only the virtual or pool server as the OES 2 server.

11 Access the sharepoints from a client workstation through the virtual server IP address or virtual server (NetBIOS) name.

For details on creating pools by using iManager, see "Using iManager to Create NSS Volumes" in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

NOTE: If the cluster object is created in a container that is in a different subtree than the one in which the nodes are present or is at a higher level than where nodes are present, then the CIFS proxy user must be manually added to the trustee list of cluster server object and required rights must be assigned to it along with the inherited rights.

Using NSSMU to Create the Pool

1 Ensure that the "Prerequisites" on page 58 are met.

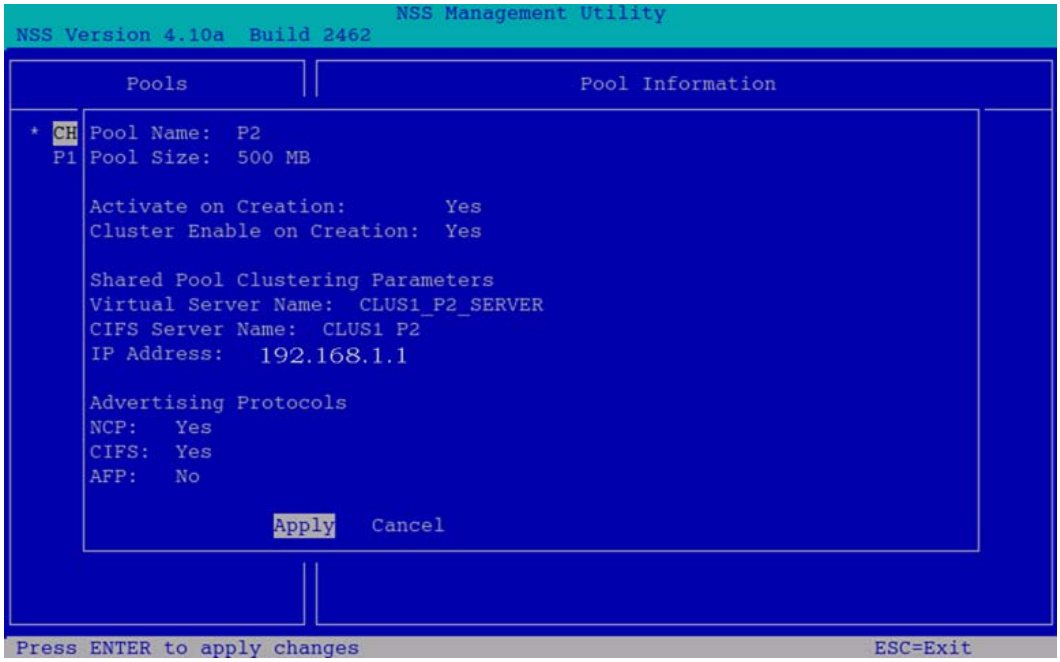
2 Start NSSMU from the server console of a cluster server.

3 Select pools from the NSSMU main menu.

4 Select the device where you want the pool to be created.

5 Specify the pool name and virtual server's or pool server's IP address.

6 Select *Yes* for CIFS under *Advertising Protocols*.



7 Select *Apply* and press Enter.

8 Use the `cluster status` command to verify that the created pool server is running.

For details, see "Console Commands for Novell Cluster Services" in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

9 Create volumes in the shared pools.

For details, see "Configuring Cluster Resources for Shared NSS Pools and Volumes in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*".

10 Create sharepoints, provide access rights, and assign password policies for the CIFS virtual server or pool server. Use the same procedure that you used to configure the virtual or pool server CIFS through iManager.

For details, see Section 5.1, "Using iManager to Manage CIFS," on page 31, but ensure that you select only the virtual or pool server as the OES 2 server.

11 Access the sharepoints from a client workstation through the virtual server IP address or virtual server (NetBIOS) name.

For details on creating pools by using NSSMU, see "Using NSSMU to Create NSS Volumes in the *OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*".

8.4.3 Using a Pre-existing Cluster Pool for CIFS

Enabling CIFS on a pre-existing cluster pool requires the following manual steps to be done by the administrator:

IMPORTANT: Ensure that Python* is installed on SUSE® Linux Enterprise Server.

1. Enable CIFS for POOL_SERVER through iManager.
2. Offline the POOL_SERVER.
3. Run the following command:

   ```
   python cifsPool.py Resource_DN CIFS_Server_Name ldaps://ldapserver:636
   Admin_DN Admin_password
   ```

   For example, `python cifsPool.py cn=POOL_SERVER,cn=clus1,o=novell CIFS_POOL ldaps://192.168.1.1:636 cn=admin,o=novell xxxxxx`

   NOTE: The length of the CIFS server name should not exceed 15 characters.

8.5 What's Next

For information about managing the CIFS services by using iManager or the command line interface, see Chapter 5, “Administering the CIFS Server,” on page 31.

For an explanation of how end users access network files from different workstations by using CIFS, see Chapter 9, “Working with Client Computers,” on page 63.

Working with Client Computers

9

If CIFS is properly configured, the users on your network can perform the following tasks:

9.1 Configuring Client to Use NTLMv1 Authentication Mode

CIFS on OES 2 SP2 supports only NTLMv1. NTLMv2 is enabled by default in Windows Vista and is optionally enabled in Windows XP. The following steps lets you configure the client to use NTLMv1 authentication mode:

1. Open the *Control Panel*.
2. Go to *Administrative Tools* > *Local Security Policies* > *Local Policies* > *Security Options* > *Network Security: LAN Manager authentication level*.
3. Select the *Send LM & NTLM - use NTLMV2 session security if negotiated setting*.
4. Click *OK* or *Apply* to save the settings.

9.2 Accessing Files from a Client Computer

From a client computer, you can access files and folders through Windows, Windows Vista, or Linux. Use one of the following methods to access the CIFS server from your clients:

9.2.1 Accessing Files from a Windows or Windows Vista Client

Prerequisite

Accessing files from a Windows computer requires NetBIOS over TCP/IP to be enabled on the Windows computer. If you have disabled NetBIOS over TCP/IP, you won’t be able to access files and directories through CIFS.

IMPORTANT: The *Search* option in Win7 mapped drive does not work as designed. You will see windows client searching for some time. However, it is not searching but the client is waiting for the server's response.

Procedure to Access Files

1. Specify your username (no context) and local password to log in to the computer.
2. Access the network by clicking the network icon.

   In Windows 2000 or XP, click *My Network Places*. In Vista, click *Network*.
3. Browse to the workgroup or domain specified during the CIFS software installation.
4. Select the server running CIFS.

   Although it is the same computer, the CIFS server name is not the same as the Open Enterprise Server (OES) 2 Linux server name. For more information, ask your network administrator.

   TIP: You can specify the server name or the server IP address in *Find Computer* to quickly access the server running CIFS software.
5. Browse to the desired folder or file.

NOTE: Windows users can also be managed through a Windows Domain Controller.

Procedure to access the content of DFS junctions

Windows 7 and Windows Vista clients need to do the following setting in order to access the content of DFS junctions:

- In *Administrative Tools* > *Local Security Policy* > *Local Policies* > *Security Options*, set the *LAN Manager authentication Level* to send LM and NTLM responses.

9.2.2 Accessing Files from a Linux Desktop

You can access files either by using an IP address or a NETBIOS name. If your Linux client is a SUSE® Linux Enterprise Desktop (SLED) 10 desktop, you can also use nautilus to access the files.:

- "Using an IP Address to Access Files" on page 64
- "Using a NETBIOS Name to Access Files" on page 65
- "Using nautilus to Access Files" on page 65

Using an IP Address to Access Files

1. Run this command from the command prompt:

   `smbclient://<SERVER_IP_ADDRESS>/<VOLUME_NAME> -U<user_name> -p 139`
2. Enter the password when prompted.

For example,

```
trml-prompt:~ # smbclient //192.168.103.158/V1 -Uari -p 139
session request to 192.168.103.158 failed (Called name not present)
session request to 192 failed (Called name not present)
Password: (enter password here)
OS=[SUSE LINUX 10.1SUSE LINUX 10.1WORKGROUP] Server=[]
```

```
smb: \>
```

Using a NETBIOS Name to Access Files

1. Run this command from the command prompt:

   ```
   smb://<SERVER_NAME>/<VOLUME_NAME> -U<user_name> -p 139
   ```

2. Enter the password when prompted.

Using nautilus to Access Files

1. Run this command from the command prompt:

   ```
   smb://<SERVER_IP_ADDRESS>/<VOLUME_NAME>
   ```

2. Enter the username and password when prompted.

9.3 Mapping Drives and Mounting Volumes

You can map drives for accessing the CIFS share names from a Windows or Windows Vista client and mount the volumes from a linux client.

- Section 9.3.1, “Mapping Drives from a Windows Client,” on page 65
- Section 9.3.2, “Mapping Files from a Windows Vista Client,” on page 65
- Section 9.3.3, “Mounting Volumes from a Linux Client,” on page 66

9.3.1 Mapping Drives from a Windows Client

From a Windows 2000 or XP client computer, you can map drives and create shortcuts that are retained after rebooting.

1. Right click on the *My Computer* icon.
2. Click *Map Network Drive*.

   There are several ways to access *Map Network Drive*. For example, you can use the *Tools* menu in Windows Explorer or you can right-click *Network Neighborhood*.
3. Browse to or specify the following path:

   ```
   \\server_running_Novell_CIFS\sharepoint | volume | directory\
   ```
4. Select the server running CIFS.

   Although it is the same computer, the CIFS server name is not the same as the OES 2 Linux server name. For more information, contact your network administrator.
5. Specify the user name and password to login.
6. Click *OK* to proceed.

9.3.2 Mapping Files from a Windows Vista Client

1. From the Windows explorer, either right click on the *Computer* icon, from the left-pane or go to the *Tools* menu.
2. Select *Map Network Drive*.
3. Specify a *Drive* to map.

4 Specify a path or Browse to the desired folder to map to the Drive. In this case, a CIFS share name, for example `\\server_running_Novell_CIFS\sharepoint | volume | directory\`.

5 Click *Connect using a different user name* link.

6 Specify the user name and password to login.

7 Click *OK* to proceed.

9.3.3 Mounting Volumes from a Linux Client

1 Login as a `root` administrator.

2 From your OES 2 server console, enter one of the three commands:

- `smbmount`

  For example, `smbmount //<ip_address>/<share_name> <mount_point> -ousername=<username>,password=<password>`

  or

- `mount -t smbfs`

  NOTE: It is not recommended to use smbfs to mount CIFS shares.

  or

- `mount -t cifs`

  For example, `mount -t cifs - ousername=<username>,password=<password> //<ip_address>/<share_name> <mount_point>`

3 Login to the specific share name in the mounted volume with the required credentials.

Troubleshooting CIFS 10

10.1 CIFS Installation and Configuration Issues

10.1.1 CIFS is not coming up after installation

Description: CIFS status is listed as stopped after a successful installation.

Cause: You might have installed CIFS alone after installing Open Enterprise Server (OES) 2 SP2 Linux.

Action: Restart the OES 2 SP2 server for the installation and configuration settings to take effect.

10.1.2 CIFS stops after installation and throws an error *669*, “*schema not extended*”

Cause: A proxy user account is present.

Action: Delete the CIFS proxy user account and let the installer create the user.

10.1.3 CIFS is not running with Samba

Description: CIFS server does not come up if the Samba server is running.

Cause: CIFS cannot coexist with samba daemons.

Action: Login as root. Use the following commands to stop the Samba daemons and restart the CIFS server.

- `/etc/init.d/smb stop`
- `/etc/init.d/nmb stop`
- `/etc/init.d/rcnovell-cifs start`

10.2 CIFS Log In Issues

10.2.1 CIFS does not log in and throws “Password has expired” error

Error: Password has expired.

Cause: Password expiry is set for security purposes. The password has expired.

Action: Reset the password and try to log in again.

10.3 CIFS Loading Issues

10.3.1 CIFS is not starting

Cause: The proxy user password was changed in eDirectory™ by using iManager or command line interdace.

Action: Reconfigure the CIFS services through YaST. Use the same proxy user and the changed password or create a new proxy user.

1. Launch *YaST* on the OES 2 Linux Server.
2. Open the *Novell CIFS Service Configuration* screen.
3. Change the password in the *CIFS Proxy User Password* field.

   NOTE: Specify a password that adheres to the password policy restrictions.

4. Retype the password in the *Verify CIFS Proxy User Password* field.
5. Click *Next* and continue with the remaining configuration steps in Section 4.2, “Installing and Configuring a CIFS Server through YaST,” on page 23.

10.3.2 Newly created NSS volumes are not being shared in CIFS

Description: When a new volume is created in a cluster/non-cluster environment, the dynamic detection of the NSS share does not happen.

Cause: eDirectory server might be restarted without restarting CIFS.

Action: Restart the CIFS service whenever eDirectory service is restarted.

Or

Description: Cluster resource gets into commatos mode when migrating the cluster resource.

Error: 22101. An invalid path.

Cause: eDirectory server might be restarted without restarting CIFS.

Action: Restart the CIFS service whenever eDirectory service is restarted.

Or

Description: Trustee updation not working in CIFS.

Error: Users are unable to access data for which they have access.

Cause: eDirectory server might be restarted without restarting CIFS.

Action: Restart the CIFS service whenever eDirectory service is restarted.

10.4 CIFS Migration Issues

10.4.1 After migration, CIFS is not running

Description: Migration is complete. However, CIFS is not running.

Cause: Configuration settings are not updated on the OES2 SP2 server.

Action: Restart OES2 SP2 server for migration to be effective.

10.4.2 Different Tree migration is not available in the Migration tool

Description: The Different Tree scenario is not supported in the Migration Tool.

Action: Use the following workaround:

1. Migrate the File System from the source server to the target server, using the Different Tree scenario.

   For detailed information see, Migrating Data to a Server in a Different Tree in the *OES 2 SP2: Migration Tool Administration Guide*.

2. Reconfigure CIFS by using YaST on the target server.

   For detailed YaST configuration steps, see Section 4.2, "Installing and Configuring a CIFS Server through YaST," on page 23.

10.5 Junction Target Changes Require DFSUTIL Command Execution to Clear the Cache

Cause: The Windows client caches junction locations when it starts.If you modify the junction target location, the client continues to point to the old junction target path.

Action: To refresh the Windows environment, do the following:

1. Download the DFSUTIL utility from the Microsoft* download site.

2 Disconnect from the mapped drive and clear the cache using the following DFSUTIL commands:

```
DFSUTIL /PKTFLUSH
DFSUTIL /SPCFLUSH
```

3 Map the drive to the new target.

Security Guidelines for CIFS

11

You can use several protection mechanisms to counteract potential security vulnerabilities for CIFS on Open Enterprise Server (OES) 2 Linux:

11.1 Using Credentials

When you set the password for the CIFS proxy user during YaST configuration, make sure you choose a password according to password policy restrictions. Choose a password that has combination of alphanumeric characters, capital letters, small letters, and adheres to the password policy restrictions.

11.2 Using CASA

Select CASA as the secret store during YaST configuration of CIFS.

11.3 Using VPN Connections

Use VPN or other secure connections while accessing confidential CIFS shares through the Internet, because CIFS packets are not encrypted.

11.4 Using SMB Signing

For a secure connection, set the SMB signing option to *optional* in iManager. For details on how to set it, see “Enabling and Disabling SMB Signing” on page 35.

11.5 Other Security Considerations

OES 2 Linux provides Universal Password security. For details, see “How to Secure Universal Password” in the *Novell Password Management Administration Guide* (http://www.novell.com/documentation/password_management32/pwm_administration/data/bwjorxp.html).

NOVCIFS

A

This section describes the command line utilities that work on an Open Enterprise Server (OES) 2 Linux server for running the CIFS services.

To access a man page with the command information, enter `man novcifs` at the command prompt.

novcifs(8)

Name

novcifs - A client interface program that communicates with the `cifsd` daemon for Novell OES 2 Linux. For `novcifs` to be running, the user must log in as `root`.

Syntax

Displaying the List of Sharepoints

```
novcifs [-sl | --share --list]
```

Displaying the Specific Sharepoint Details

```
novcifs [-sln SHARENAME | --share --list --name=SHARENAME]
```

Adding a New Sharepoint

```
novcifs [-sap PATH -n SHARENAME -m CONNECTION-LIMIT -c COMMENT |
--share --add --path=PATH --name=SHARENAME --conn-limit=CONNECTION-LIMIT --
comment=COMMENT]
```

Removing a Sharepoint

```
novcifs [-srn SHARENAME | --share --remove --name=SHARENAME]
```

Enabling or Disabling the Debug Log (for Developers)

```
novcifs [-b yes|no | --enable-debug=yes|no]
```

Enabling or Disabling the Info Log

```
novcifs [-f yes|no |--enable-info=yes|no]
```

Enabling or Disabling SMB Signing

```
novcifs [-g yes|no|optional|force | --enable-smbsigning=yes|no|optional|force]
```

Enabling or Disabling Anonymous Log In for CIFS

```
novcifs -e [yes|no]
```

Adding or Removing DNS Names (other than hostnames) for Advertising

```
novcifs --add --dns-name="<DNS_NAME>" --ip-addr=IP_ADDR
novcifs --remove --dns-name="<DNS_NAME>" --ip-addr=IP_ADDR
```

Displaying Operational Parameters

```
novcifs [-o | --oper-params]
```

Adding a Virtual Server to the Shared Pool

```
novcifs [-av VIRTUALSERVERFDN -I VIRTUALSERVERIP | --add --
vserver=VIRTUALSERVERFDN --ip-addr=VIRTUALSERVERIP]
```

Removing a Virtual Server from the Shared Pool

```
novcifs [-rv VIRTUALSERVERFDN -I VIRTUALSERVERIP | --remove --
vserver=VIRTUALSERVERFDN --ip-addr=VIRTUALSERVERIP]
```

Displaying the Active Client Connection Count on the CIFS Server

```
novcifs [-C | --conn-count]
```

Options

Usage Options

-s | --share

An argument to manipulate a sharepoint.

-l | --list

Displays the list of sharepoints.

-a | --add

Adds a new sharepoint or virtual server.

-p PATHNAME | --path=*PATHNAME*

Specifies a volume based path to add for the sharepoint. This path is not an absolute path.

-n SHARENAME | --name=*SHARENAME*

Specifies the CIFS sharename while adding or removing the sharepoint.

-m *CONNECTION-LIMIT* | --conn-limit=*CONNECTION-LIMIT*

Specifies the connection limit of the CIFS sharepoint to add.

-c COMMENT | --comment=*COMMENT*

Specifies a CIFS sharepoint comment to add.

-C | --conn-count

Displays the active connection count.

-r | --remove

Removes the sharepoint or virtual server.

-v VIRTUALSERVERFDN | --vserver=*VIRTUALSERVERFDN*

Specifies the virtual server FDN to add or remove.

-I *VIRTUALSERVERIP* | --ip-addr=*VIRTUALSERVERIP*

Specifies the virtual server IP address to add or remove.

-o | --oper-params

Displays the operational parameters, such as enabled or disabled, for different CIFS configurations.

-f `yes|no` | --enable-info=`yes|no`

Enables or disables the info log status.

-g `yes|no|optional|force` | --enable-smbsigning=`yes|no|optional|force`

Enables or disables the SMB signature.

`yes` for enabling.
`no` for disabling.
`optional` for optional enabling.
`force` for mandatory enabling.

This is an add-on functionality.

-b `yes|no` | --enable-debug=`yes|no`

Enables or disables the debug log.

Help Options

-h | --help

Displays the help information for CIFS commands, syntax, and exits.

-u | --usage

Displays the usage information for the commands and exits.

Files

/etc/opt/novell/cifs/cifs.conf

CIFS configuration file.

/etc/opt/novell/cifs/cifsctxs.conf

CIFS context file.

/etc/opt/novell/cifs/.cifspwd.enc

Encrypted CIFS proxy user file.

/etc/init.d/novell-cifs

Initialization script for CIFS. You should use this script to start and stop CIFS, rather than running it directly.

/var/opt/novell/log/cifs.log

CIFS server log file.

Examples

`/etc/init.d/novell-cifs start` runs this program in the standard way.

`/usr/sbin/novcifs` runs the client interface program directly.

`VOL1:dir1` or `VOL1:/dir1` is a volume based path.

Authors

See Also

migCifs(8)

Report Bugs

To report problems with this software or its documentation, visit http://bugzilla.novell.com.

Comparing CIFS on NetWare and CIFS on Linux

B

This section compares features and capabilities of Novell® CIFS on the NetWare® and Linux platforms for Novell Open Enterprise Server 2 SP2 servers.

Table B-1 *CIFS services on NetWare and OES 2 Linux*

Service	NetWare	OES 2 Linux
64-Bit Support	No	Yes
Distributed File Services for NSS Volumes	Yes	Yes
OpLocks	Yes	Yes
Cross Protocol Locking	Yes	Yes
NSS Support	Yes	Yes
CIFS-enabled shared NSS pool/ volume in a NetWare-to-NetWare or Linux-to-Linux cluster	Yes	Yes
CIFS-enabled shared NSS pool/ volume in a mixed NetWare-to-Linux cluster	No	No
iManager Support and Administration tool	Yes	Yes
File and Record Locking	Yes	Yes
Domain Emulation	Yes	Future
Monitoring	No	Future
Xen* Virtualized Host Server Environment	NA	No
Xen Virtualized Guest Server Environment	Yes	Yes
Multi-processor/Multicore Server Support	No	Yes
Multi-File System Support	No	Future
NTLMv2/Kerberos*	No	Future

Documentation Updates

C

C.1 January 2010

- The following note is inlcuded in the Section 4.2, “Installing and Configuring a CIFS Server through YaST,” on page 23

  NOTE: Installing Novell CIFS also installs Audit and starts auditd.

C.2 November 2009

- Front file is updated with date, version, and copyright.
- Section 10.3.2, “Newly created NSS volumes are not being shared in CIFS,” on page 68 is added in the Chapter 10, “Troubleshooting CIFS,” on page 67.
- Section 10.2, “CIFS Log In Issues,” on page 68 is added in the Chapter 10, “Troubleshooting CIFS,” on page 67.
- Appendix A, “NOVCIFS,” on page 73 is updated with new command line utilities.
- Section 9.1, “Configuring Client to Use NTLMv1 Authentication Mode,” on page 63 is added in the Chapter 9, “Working with Client Computers,” on page 63.
- Editorial Comments are incorporated.
- The following note is added in the Chapter 5, “Administering the CIFS Server,” on page 31:

  NOTE: The string length of the NetBIOS name should not exceed 15 chars. The hostname or the first 13 characters from the hostname, whichever is shorter is considered and appended with *_W* at the end to frame the standard NetBIOS name.

- Section 5.4, “Third Party Authentication,” on page 46 is added to Chapter 5, “Administering the CIFS Server,” on page 31.
- Table 5-3 on page 41 is revised.
- The following content is updated in Section 5.2.6, “Working with CIFS Shares,” on page 45:

  CIFS shares cannot be added to virtual server object using command line (novcifs). If the shares are added on cluster resource using command line, then all the shares are lost if the resource leaves that node.

- Section 5.1, “Using iManager to Manage CIFS,” on page 31 is revised with graphics and content.
- Section 5.3, “Locks Management for CIFS,” on page 45 is added to Chapter 5, “Administering the CIFS Server,” on page 31.
- Section 5.5, “DFS Junction Support in CIFS Linux,” on page 46 is added to Chapter 5, “Administering the CIFS Server,” on page 31.

- Oplocks and Distributed File Services description is included in Table 5-1 on page 34.
- Section 5.6, “Problems Following DFS Junctions with CIFS in Windows 2000/XP Releases,” on page 47 is added to Chapter 5, “Administering the CIFS Server,” on page 31.

C.3 November 2008

- All chapters and sections are new additions to OES 2 SP1 release.