Open Enterprise Server 11 SP3
Novell CIFS Administration Guide

July 2016

Novell

Legal Notice

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

Copyright © 2014 - 2016 Novell, Inc. All Rights Reserved.

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) 11 SP3 server.

Audience

This guide is intended for OES 11 SP3 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.

Documentation Updates

For the most recent version of the *CIFS Guide*, visit the OES 11 Documentation Web site.

Additional Documentation

For documentation on CIFS on NetWare, see the Native File Access Protocols Guide (http://www.novell.com/documentation/nw65/file_afp_cifs_nfs_nw/data/h9izvdye.html#h9izvdye).

1 Overview of CIFS

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 this but intertwined with other protocols for service announcement, naming, authentication, and authorization.

1.1 Understanding CIFS

The Common Internet File System (CIFS), also known as Server Message Block (SMB), is an application-layer network protocol used for providing shared access to files on a Local Area Network (LAN). It relies on NetBIOS over TCP (NBT) for reliable transport. Although file sharing is the primary purpose of CIFS, there are other functions that CIFS is commonly associated with. Some of them include service announcements, name resolution, user authentication, authorization, and browsing for other CIFS servers in the network.

Novell CIFS runs on the Open Enterprise Server (OES) 11 SP3 server, uses NetIQ eDirectory services for user authentication, and allows Windows, Linux, and Mac 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 workstations.
- For Linux, through an SMB client from Linux desktops.

Figure 1-1 Novell CIFS Conceptual Overview
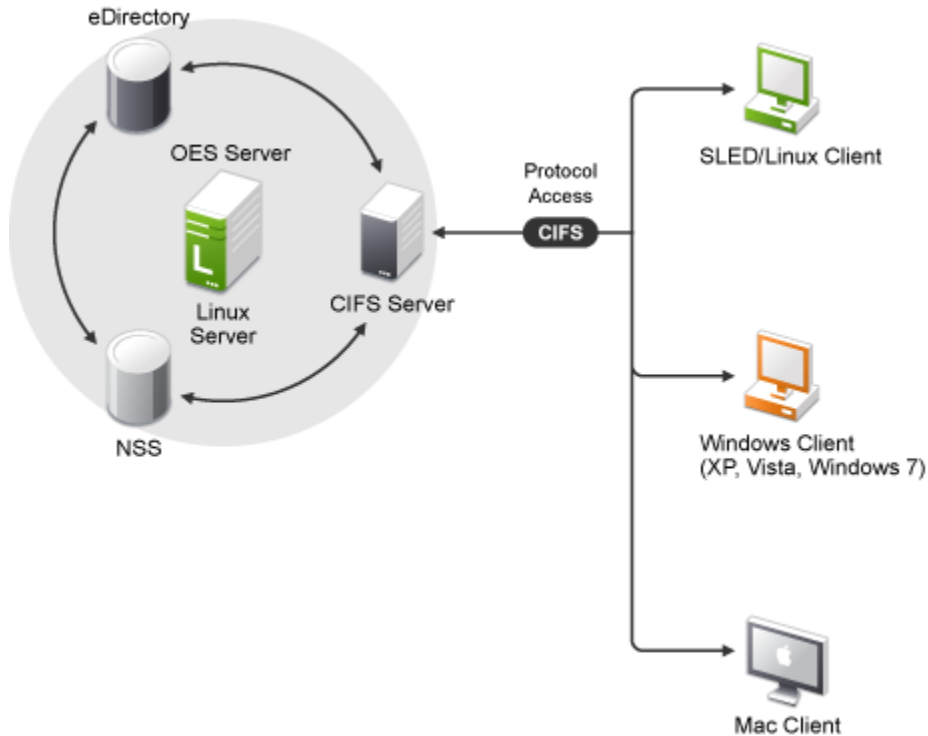
Novell CIFS enables Windows, Linux, and Mac client workstations to create, copy, delete, move, save, and open files on an OES 11 SP3 server. CIFS allows read and write access from multiple client systems simultaneously. All these various file operations and sharing of resources on a network are managed from a CIFS server.

1.2   CIFS and Universal Password

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

To learn more about Universal Password, including how to enable it, see Deploying Universal Password in the *Novell Password Management Administration Guide*.

1.3   CIFS Features and Capabilities

The CIFS implementation supports the following features on OES 11 SP3:

Table 1-1 *CIFS Feature List*

Feature	Description
Client Support	Support for clients from Windows 7 onwards.
	Support for Linux clients from SLED 11 onwards (CIFS filesystem only).
	Support for Mac clients from 10.10 onwards.
Integration and Support for Novell Technologies	Integration with NetIQ eDirectory.
	Integration with the Novell Storage Services (NSS) file system.
	Support for DST shadow volume pair access. For more information, see Section 6.5, "Dynamic Storage Technology for CIFS Server," on page 60.
	Support for DFS junctions. For more information, see Section 6.6, "DFS Junction Support in CIFS Linux," on page 61.
Subtree Search	Subtree search or contextless login enables CIFS to search for a user in the entire base context of a tree.
	For more information, see Section 6.7, "Subtree Search," on page 62.
Cross-Protocol File Locking	Cross-Protocol locks help prevent the same file from being concurrently accessed for modifications from different users/clients accessing over different protocols (CIFS, NCP, and AFP).
	This option ensures that a file is updated correctly before another user, application, or process can access it.
	For more information, see Section 6.3, "Locks Management for CIFS," on page 55.
Migration	Migration capability from NetWare to Linux. For more information, see Chapter 7, "Migrating CIFS to OES 11 SP3," on page 65.
Universal Password	Support for Universal Password. For more information, see Password Management Security Consideration.
Authentication Modes	CIFS supports NMAS authentication method
	Support for NTLMv1 and NTLMv2 authentication mode. For more information, see Table 6-2 on page 45.
	Support for Third-Party Authentication.
File Access	Supports the Novell Trustee Model for file access.
	For more information, see "Novell Trustee Model" in the OES 11 SP3: NSS File System Administration Guide for Linux.
Client-side caching (Offline Files support)	Stores frequently used information on the client's machine. For more information, see Section 6.8, "Enabling Offline Files Support," on page 63.

Feature	Description
High Availability	Supported by Novell Cluster Services for high availability. For more information, see Chapter 9, "Configuring CIFS with Novell Cluster Services for an NSS File System," on page 69.
Administration and Configuration	Performed through iManager. For more information, see Section 6.1, "Using iManager to Manage CIFS," on page 39.
User Management	CIFS does not require Linux User Management (LUM) enabling.

1.4 Limitations

- SMBv2 is not supported in this OES 11 SP3 release.
- SMB on TCP/IP through Port 445 is not available.

1.5 What's Next

If you are planning to implement CIFS on your enterprise server, continue with Chapter 4, "Planning and Implementing CIFS," on page 21.

2 What's New or Changed in Novell CIFS

This section describes enhancements and changes in Novell CIFS since the initial release Novell Open Enterprise Server (OES) 11.

2.1 What's New (OES11 SP3)

Besides bug fixes, there are no other changes for this component.

2.2 What's New (OES11 SP2 May 2016 Patches)

novcifs Command Changes

Using command line, you can enable or disable DFS support for the CIFS server. By default, this option is disabled.

2.3 What's New (OES11 SP2 May 2014 Patches)

CIFS NMAS Authentication Method for Linux Supports Grace Logins

In spite of the user having grace logins left, the CIFS NMAS Authentication method for Linux does not authenticate a user when the user password has expired. This functionality has been modified to enable a user to login using the old password till the grace login count is exhausted.

Immediately after applying the patch, execute the procedure as explained in section "Patches:" in the *OES 11 SP3: Novell CIFS for Linux Administration Guide*.

2.4 What's New (OES 11 SP1 January 2014 Patches)

Interoperability with Partnering Vendors

Interoperability with some antivirus and Hierarchical Storage Management (HSM) partner products has been improved in OES 11 SP1.

2.5 What's New (OES 11 SP2)

The CIFS service in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, OES 11 SP2 provides the following enhancements and changes for CIFS:

Changes to the CIFS Delete Mechanism

The file and folder delete functions for the NSS file system in Novell CIFS were modified to use the POSIX APIs. This change leads to generating three new Vigil NSS auditing events, namely, OPEN, MODIFY, and CLOSE when CIFS protocol is used to delete a file or folder on an NSS file system. These are generated in addition to the DELETE event.

Enhanced Open Connections and Files Monitoring

- The CIFS service now provides the capability to monitor open files and CIFS connections.

  You can monitor the CIFS service using the newly added command line options in the `novcifs` utility or the **Manage CIFS Services** option in NRM. For more information, see "CIFS Monitoring and Management" in the OES 11 SP2: Novell CIFS for Linux Administration Guide.

- The novcifs long option for active connection count has been changed in OES11 SP2 from `-C | --conn-count` to `-C | --Conn`.

CLI Commands to View the NetBIOS Name of Servers and Change the Behavior of Exporting Volumes by Default

With the new command options introduced in `novcifs`, administrators can choose to export all mounted volumes as shares or export only the required volumes as shares.

`novcifs --list-servers`

Displays the NetBIOS name of physical and virtual CIFS servers.

`novcifs --share-vols-default=SERVER_NAME --value=yes|no`

Enables or disables all volumes being exported as shares by default.

For more information, see "Viewing the NetBIOS Names of Servers and Changing the Behavior of Exporting Volumes by Default" under novcifs(8) in the OES 11 SP2: Novell CIFS for Linux Administration Guide.

Pass-through Information Levels Capability

The Novell CIFS server now implements the pass-through information levels capability. This is a configurable option and is turned off by default. It can be enabled or disabled using the `novcifs --info-level-passthru=yes|no` command.

Pass-through Information Levels are used to set or to query file or folder information on the server. These Information Levels allow SMB clients to directly query Information Levels that are native to the underlying object store or file system.

User-level quota is not supported if this option is disabled.

For more information, see "Enabling or Disabling the Pass-through Information Levels Capability" under novcifs(8) in the OES 11 SP2: Novell CIFS for Linux Administration Guide.

Support for DOS Names

The CIFS Service now supports file operations using the short file name format to accommodate applications that require file names to be in the 8.3 name format, for example, ABPXPS~1.PPT.

2.6 What's New or Changed in Novell CIFS (OES 11 SP1)

Novell CIFS in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, OES 11 SP1 provides the following enhancements and changes for CIFS:

Ability to View Trustees/IRM Assigned to Files and Folders

Novell CIFS will now be able to display the list of trustees associated with the specified file or folder as per the CIFS cache record, import the trustee information from the `trustee_database.xml` file associated with the specified volume into the CIFS cache, and display the count of new, modified, and removed trustees for the specified volume. For more information, see "Viewing the Trustees Associated with a File or Folder,""Synchronizing the Trustee List for a Volume," and "Viewing Statistics of Trustees for a Volume" in the OES 11 SP1: Novell CIFS for Linux Administration Guide.

2.7 What's New or Changed in Novell CIFS (OES 11)

This section describes enhancements and changes to Novell CIFS for Novell Open Enterprise Server (OES) 11.

Detection of Cluster Resources/Volumes/Shares upon CIFS Restart

It is now possible to restart CIFS service in a cluster setup when cluster resources are active.

Monitoring Running Status of CIFS Server

You can now use the monitor command with the `rcnovell-cifs` script to check the CIFS server status. When `rcnovell-cifs monitor` is invoked, it returns the status of CIFS if it is already running otherwise (dead/not running) it starts a new instance and returns the status. For more information, see Configuring CIFS with Novell Cluster Services for an NSS File System in the OES 11: Novell CIFS for Linux Administration Guide.

Large Number of Open Files Support

Novell CIFS will now be able to increase the file id pool size from 65k to 600k. In addition, you can also dump file handle statistics and directory cache statistics. For more information, see "Enabling CIFS File Id Pool" and "Dumping File Handle Statistics" in the OES 11 SP1: Novell CIFS for Linux Administration Guide.

Blocking Invalid User Authentication Requests

Novell CIFS will now be able to cache the invalid user logins for a specific timeout period. Further authentication requests from the same user name will be ignored based on the configured timeout period. For more information, see "Enabling Invalid User Caching" in the OES 11 SP1: Novell CIFS for Linux Administration Guide.

3 CIFS Monitoring and Management

In the Novell Open Enterprise Server 11 SP3 release, the new commands introduced in the `novcifs` utility let you to manage open files and CIFS connections.

3.1 Overview of CIFS Monitoring and Management

With the file monitoring options you can view details of open files and close open files within a volume, by connection and file handles associated with a file.

3.2 Using CIFS Monitoring and Management

novcifs - A command line utility to configure, monitor, and manage the CIFS service (`cifsd` daemon). To run the `novcifs` utility from the command line, you must log in as root. For more information, see Appendix A, "Command Line Utility for CIFS," on page 99.

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

You can also monitor and manage the CIFS service using the **Manage CIFS Services** menu option provided in NRM.

3.3 Monitoring Connections

Table 3-1 *Connection Monitoring command options*

Option	Description
`-C, --Conn`	Displays the count of active connections.
`-Cl, --Conn --list`	Lists all CIFS connections.
`-Cn CONNECTION_ID, --Conn --connection=CONNECTION_ID`	Displays details of the specified connection ID.

By querying or listing all open connections, you can find how many sessions are open at any given time. The details include session ID, client IP address, user name, user login time, consolidated list of read/write requests, access mode, and total number of other requests received.

You can also drill down to extract per-connection details such as the group that the user is a member of.

The **Privileges** field displaying Supervisor for the logged in user implies that the user has Supervisor privileges for Entry Rights over NCP Server object. The user with such privileges gets full access to all the mounted volumes irrespective of user rights at file system level.

3.3.1 Access Modes

Connection details include access modes in which the CIFS server opened the file on behalf of the user.

This field displays information that the CIFS server has interpreted from the data received as part of both the Access Mask and Share Access fields in the SMB_COM_NT_CREATE_ANDX request.

Desired Access: Specifies the access modes that the client has requested.

RD: Indicates the right to read data from the file.

WR: Indicates the right to write data into the file.

Share Access: Specifies the sharing modes that the client has requested; that is, how the file should be shared with other users.

DR: Indicates that the right to read data from the file is denied.

DW: Indicates that the right to write data into the file is denied.

DD: Indicates that the right to delete or rename the file is denied for all other connections.

ND: Indicates that the right to delete or rename the file is denied for this connection.

3.4 Monitoring Files

Table 3-2 *File Monitoring command options*

Option	Description
`-Flp FILE_PATH, --Files --list --path=FILE_PATH`	Lists users who opened the file with the specified file path.
`-Flv VOLUME_NAME, --Files --list --volume=VOLUME_NAME`	Lists users and the files opened by them on the specified volume. **NOTE:** Listing all files on a volume is a time-consuming operation if too many files are open, so use this option sparingly.
`-Fln CONNECTION_ID, --Files --list --connection=CONNECTION_ID`	Lists files opened by the user session with the specified connection ID.
`-FCp FILE_PATH, --Files --Close --path=FILE_PATH`	Closes an open file with the specified file path.
`-FCn CONNECTION_ID, --Files --Close --connection=CONNECTION_ID`	Closes the files opened by the user session with the specified connection ID.
`-FCv VOLUME_NAME, --Files --Close --volume=VOLUME_NAME`	Closes all open files on the specified volume.

You use the file listing options to view the following:

- All open files within a particular volume
- All open files by connection
- All users who have open file handles for a particular file

You use the file closing options to close the following:

- ◆ All open files within a particular volume
- ◆ All open files by a particular connection
- ◆ All open file handles associated with a particular file

If a user tries to perform any operation on an open file that was closed by using this utility, the changes might appear the next time the file is opened. This depends on the application. The data that was saved before the file was closed will be intact.

IMPORTANT: This is not the recommended way to close files. It is provided as a tool to administrators to force close open files.

4 Planning and Implementing CIFS

In planning for and implementing CIFS on an Open Enterprise Server (OES) 11 SP3 server, ensure that you understand the information and requirements in the following sections:

4.1 Planning for CIFS

The key factors to consider for implementing and enabling Novell CIFS on your enterprise servers include the following:

- Upgrading from OES 2 SP3 Linux to OES 11 SP3 on your enterprise servers. For details, see "Upgrading to OES 11 SP3 " in the *OES 11 SP3: Installation Guide*.
- Migrating from NetWare to an OES 11 SP3 setup. For details see, Chapter 7, "Migrating CIFS to OES 11 SP3," on page 65.

4.2 Preparing for CIFS Installation

4.2.1 Prerequisites

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

❒ CIFS users must have universal password enabled. For more information, see Deploying Universal Password in the *Novell Password Management Administration Guide*.

The Universal Password includes the ability to create password policies. It also removes the need to maintain two separate passwords for CIFS users.

❒ Samba and Novell CIFS can not run on the same system. Stop all of the running Samba daemons before installing CIFS. Use the following commands:

- `/etc/init.d/smb stop`
- `/etc/init.d/nmb stop`

4.2.2 Required eDirectory Rights and Permissions

Rights Needed for CIFS Install Time Administrator

The install administrator must have the following rights to add the Common Proxy user as a trustee of CIFS user contexts and NCP server object of the system where CIFS is being configured.

Target Object	Required Rights
User Contexts selected at install time.	Compare, Read, Write on ACL Attribute.
Local NCP Server object.	Compare, Read, Write on ACL Attribute.

Rights Needed for CIFS Proxy User

The CIFS Proxy user must have the following rights for the CIFS server to read and update CIFS server configuration in eDirectory.

Target Object	Required Rights
User Contexts (`/etc/opt/novell/cifs/cifsctxs.conf` file).	Inheritable Read and Compare on CN attribute.

Target Object	Required Rights
Local NCP Server Object.	Read and Compare rights on [All Attribute Rights].
	Supervisor rights on CIFS specific attributes listed below:

- ◆ nfapCIFSServerName
- ◆ nfapCIFSComment
- ◆ nfapCIFSWorkGroup
- ◆ nfapCIFSPDCName
- ◆ nfapCIFSAuthent
- ◆ nfapCIFSDialect
- ◆ nfapCIFSDebug
- ◆ nfapCIFSUnicode
- ◆ nfapCIFSOpLocks
- ◆ nfapCIFSAsync
- ◆ nfapCIFSWalk
- ◆ nfapCIFSPDCAddr
- ◆ nfapCIFSWINSAddr
- ◆ nfapCIFSAttach
- ◆ nfapCIFSNDSUserContext
- ◆ nfapCIFSUserContext
- ◆ nfapCIFSShares
- ◆ nfapCIFSDFS
- ◆ nfapCIFSLoginScripts
- ◆ nfapCIFSShareVolsByDefault
- ◆ nfapCIFSDomainDN
- ◆ nfapCIFSBeginRID
- ◆ nfapCIFSEndRID
- ◆ nfapCIFSPDCEnable
- ◆ nfapCIFSSignatures
- ◆ nfapLoginScript
- ◆ nfapCIFSRID
- ◆ nfapCIFSComment
- ◆ nfapCIFSNextRID
- ◆ nfapCIFSDomainSID
- ◆ nfapCIFSPDC
- ◆ nfapCIFSDCList
- ◆ nfapCIFSDCGroup
- ◆ nfapCIFSDomainEpoch

Rights Needed for CIFS Administrator

The CIFS administrator requires the following rights to manage the CIFS server.

Target Object	Required Rights
User Contexts being added for authentication.	Compare, Read, Write on ACL Attribute.

4.3 CIFS System Prerequisites

To access CIFS servers running on an OES 11 SP3 server, ensure that your setup meets the following basic minimum requirements:

- Section 4.3.1, "Server Operating System Requirements," on page 24
- Section 4.3.2, "Server Hardware Requirements," on page 24
- Section 4.3.3, "Client Operating System Requirements," on page 24
- Section 4.3.4, "CIFS Prerequisite Checklist," on page 24

4.3.1 Server Operating System Requirements

SUSE Linux Enterprise Server 11 SP4.

4.3.2 Server Hardware Requirements

For details, see "Meeting All Server Software and Hardware Requirements" in the *OES 11 SP3: Installation Guide*.

4.3.3 Client Operating System Requirements

- Windows 7
- Windows 8
- Mac Client 10.10 onwards
- SUSE Linux Enterprise Desktop 11 onwards (CIFS file system only)

4.3.4 CIFS Prerequisite Checklist

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 in order for Novell CIFS to function properly.
- ❒ If any CIFS user objects are on eDirectory servers running 8.7 or earlier, ensure that you upgrade the server using the *Security Services 2.0.6 patch* (http://download.novell.com/Download?buildid=LYlbZMAom6k~).

4.4 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 the following SLES and OES patterns:

❒ SLES File Server Pattern

❒ OES patterns Novell Domain Services for Windows (DSfW) and Novell Samba

❒ Any other SMB implementation

❒ Xen Virtualization Host pattern

4.5 What's Next

To proceed with CIFS installation on an OES 11 SP3 server, continue with Chapter 5, "Installing and Setting Up CIFS," on page 27.

5 Installing and Setting Up CIFS

This section describes how to install and configure Novell CIFS. CIFS should be selected to be installed during the OES 11 SP3 installation.

5.1 Installing CIFS during the OES 11 SP3 Installation

1 In the YaST install for OES, on the **Installation Settings** page, click **Software** to go to the **Software Selections** page.

For information about the entire OES 11 SP3 installation process, see the OES 11 SP3: Installation Guide.

2 From the **OES Services** option, select **Novell CIFS**, then click **Accept**.

The following additional services are automatically selected:

- Novell Backup / Storage Management Services (SMS)
- NetIQ eDirectory
- Novell Linux User Management (LUM)
- Novell NCP Server / Dynamic Storage Technology
- Novell Remote Manager (NRM)
- Novell Storage Services (NSS)
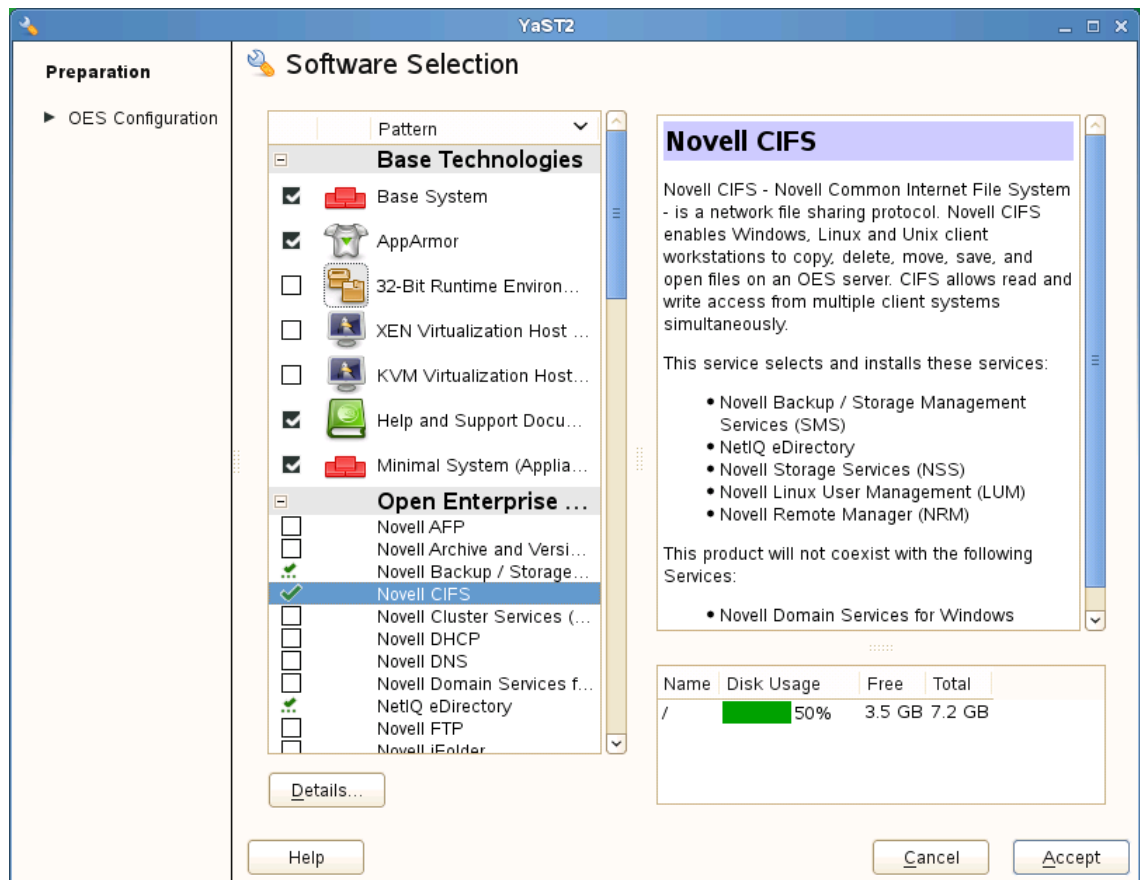
3 Select an appropriate install option.

Typical Configuration: A two-click express installation with minimal user inputs. This method collects only essential information to proceed with the OES configuration and uses default values for most options. In case you want to modify the default configuration parameters; in the OES install summary screen, click the respective links and modify them.

Custom Configuration: This method of OES configuration requires inputs for all parameters.
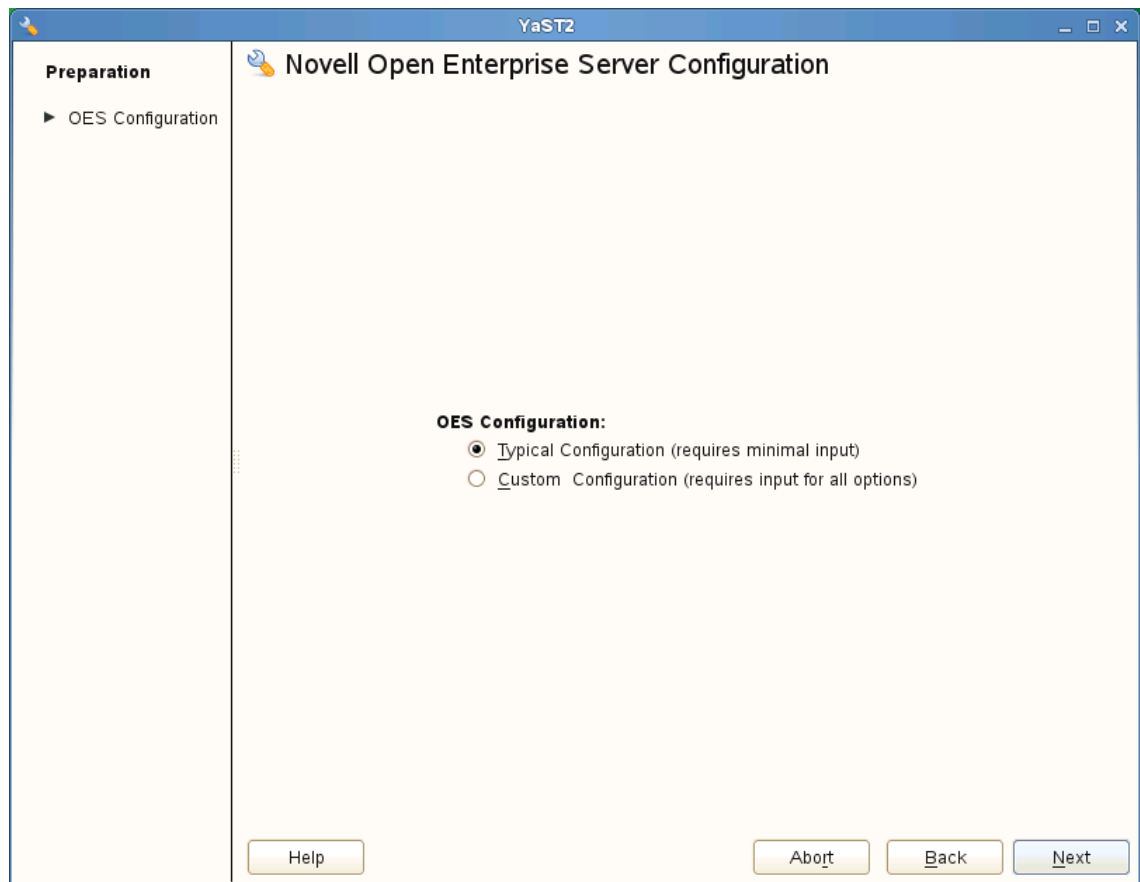
4 On the Novell Open Enterprise Server Configuration window, click **Change** and then click **Novell CIFS Services**.
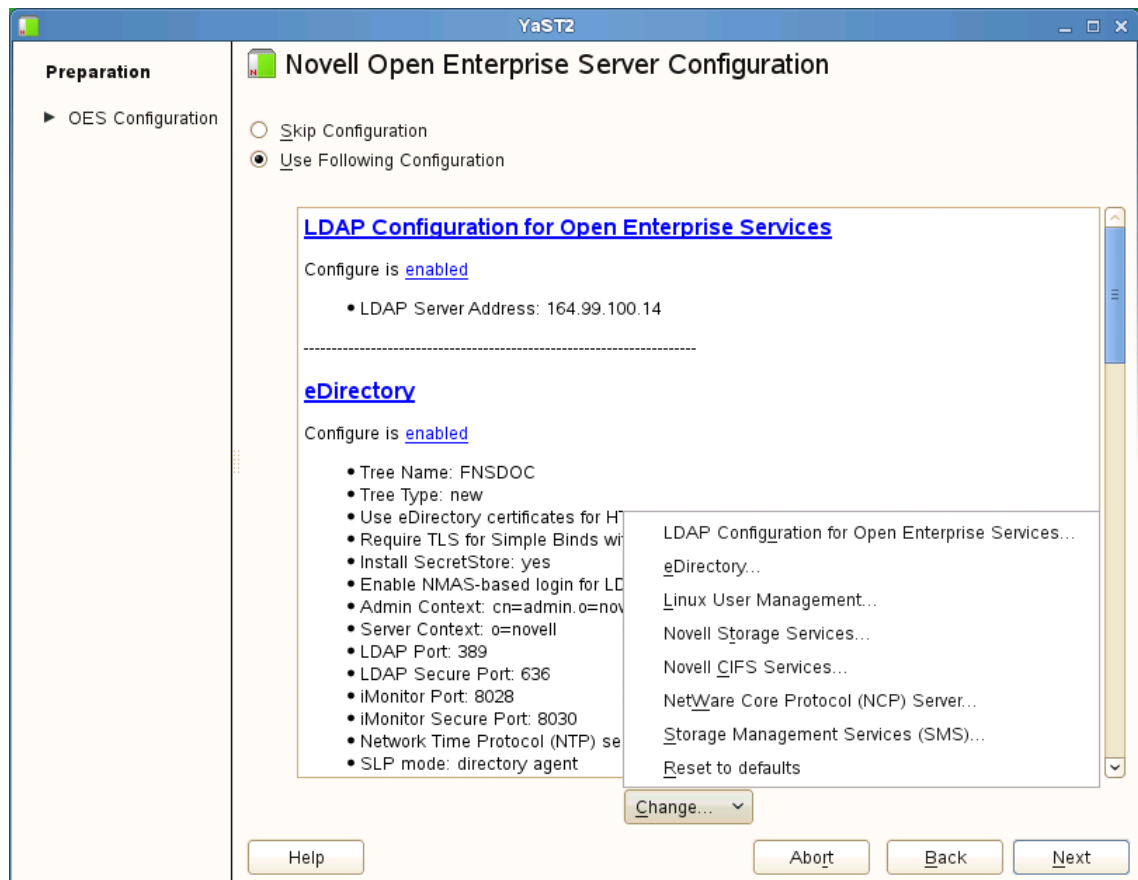
5 Select the IP address of the LDAP server from the **Directory Server Address** drop-down list. If you do not want to use the default, select a different LDAP server in the list.

6 Browse or specify a user (existing or created here) with rights to search the LDAP tree for CIFS objects.

If you selected the **Use Common Proxy User as default for OES Products** check box during eDirectory configuration, the Proxy user name and password fields are auto-populated. If a common proxy is not configured, the **CIFS Proxy User Name** field is populated with a system-generated proxy user name.

7 Specify a password (existing or created here) for the Proxy user.

This field is disabled if you selected the **Use Common Proxy User as default for OES Products** check box during eDirectory configuration. If a common proxy is not configured, the Proxy Password field is auto-populated with a system-generated proxy password.

8 Retype the same password in the **Verify Proxy User Password** field.

9 Click **Add**, then browse to search for an existing eDirectory context. Specify the list of contexts to search for CIFS users. They will be sequentially searched when CIFS users enter their credentials.
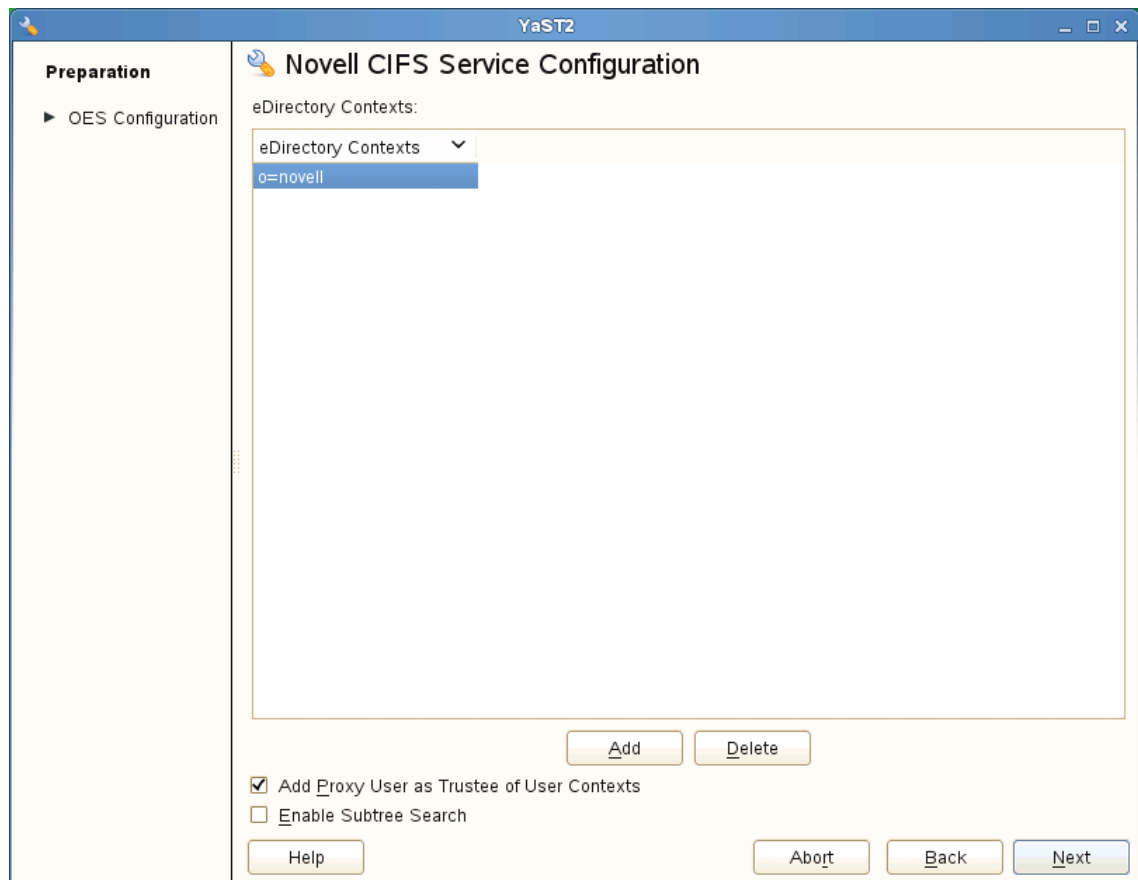
Add Proxy User as Trustee of User Contexts: This option is selected by default. Deselecting this option will not grant the CIFS proxy user the rights required over eDirectory contexts to search for a CIFS user in the subtree.

Enable Subtree Search: This option is not selected by default. Selecting this option enables CIFS to search for a user in the entire subtree of selected contexts.

The CIFS server searches through each context in the list until it finds the correct user object. For example, if users exist in ou=users, provide the context. If there are any users in ou=user1,ou=users, it is not resolved unless you have a subtree search enabled. The ou=user1,ou=users context must be added explicitly.

10 Click **Next**.

11 Click **Apply** to save the changes.

5.2 Installing CIFS after the OES 11 SP3 Installation

If you are installing CIFS after installing OES 11 SP3, ensure that you have the required eDirectory admin credentials before you proceed with the CIFS installation.

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: When "Novell CIFS" is selected, the CIFS dependency packages are also selected. These dependencies include: NetIQ eDirectory, Novell Linux User Management (LUM), NetWare Core Protocol Server (NCP), Novell Remote Manager (NRM), and Novell Storage Services (NSS). These packages are in addition to any other OES 11 SP3 service or dependency packages selected by default

---

4 Click **Accept**.

5 Select an appropriate install option.

The subsequent pages allow you to configure CIFS on OES 11 SP3.

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

NOTE: If you are installing CIFS after installing OES 11 SP3, you are prompted to enter the eDirectory admin password. Enter the password, then click **OK** to proceed.

---

7 Fill in the following fields, then 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.

Parameter	Description
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 11 SP3 server is attached to an existing tree, you 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. During eDirectory configuration, if you have selected the **Use Common Proxy User as default for OES Products** check box, then the proxy user and password fields are populated with common proxy user name and password. You cannot change this password in the CIFS configuration screen.
CIFS Proxy User Password	The password specified here is set in CASA or the local file.
Verify CIFS Proxy User Password	Re-enter the password for verification. It should be identical to the CIFS proxy user password.
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.

8 Select **eDirectory Contexts** that have CIFS users. CIFS server searches these contexts for CIFS users during authentication.

If you want to add a CIFS user context, click **Add**.

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.`

Add Proxy User as Trustee of User Contexts: This option is selected by default. Deselecting this option will not grant the CIFS proxy user the rights required over eDirectory contexts to search for a CIFS user in the subtree.

Enable Subtree Search: This option is not selected by default. Selecting this option enables CIFS to search for a user in the entire subtree of selected contexts.
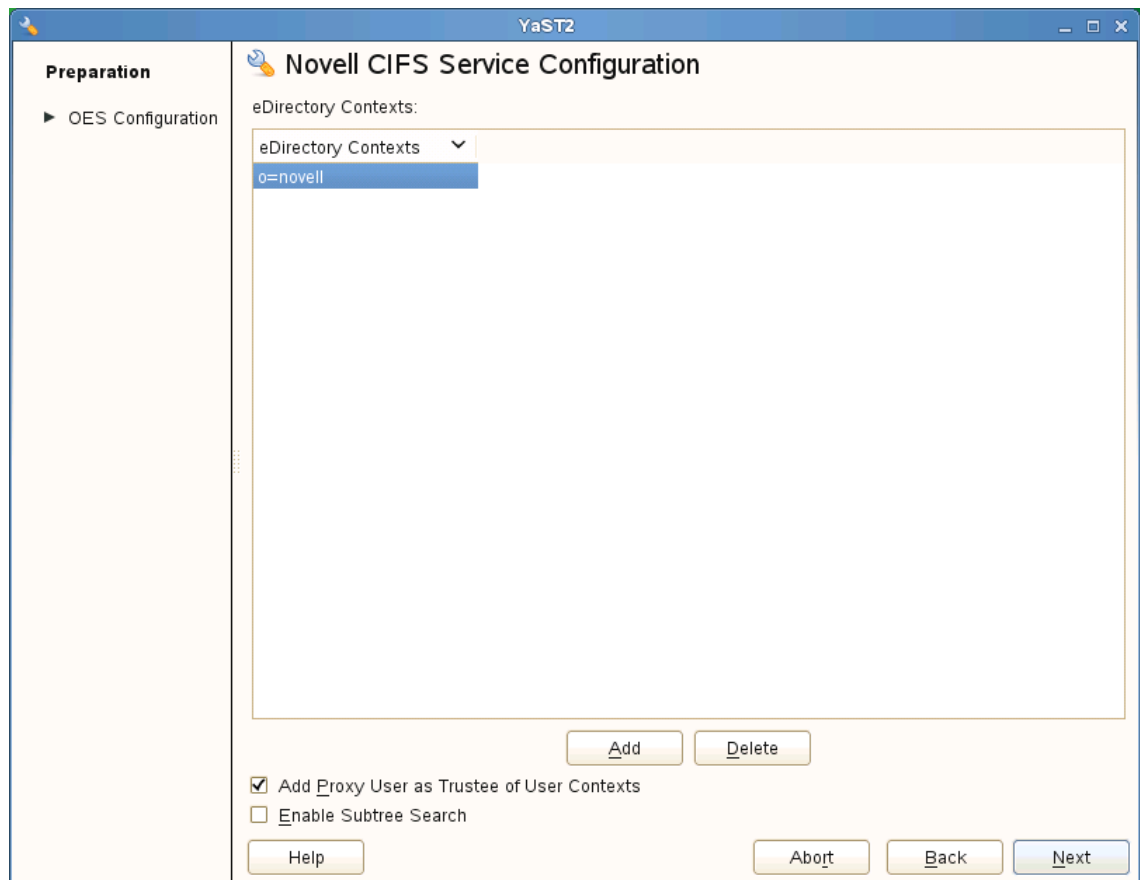
9 The CIFS configuration settings that you specified are saved successfully on your OES 11 SP3 server.

5.3 Installing NMAS

Use one of the following methods to install NMAS:

- **Fresh/Media Install:** LSM is installed with CIFS by default. NMAS can be installed only once for the entire tree.

- **Patches:** Patches for CIFS NMAS methods are packed with `novell-cifs-nmas-methods.rpm`. After the rpm is installed, run the following command to update the method version:

  ```
  nmasinst -addmethod <adminDN> <treeName> <configFile> [-h hostname[:port]] [-w pwd] [-checkversion]
  ```

  ```
  nmasinst -addmethod cn=admin.o=novell CIFS-TREE /opt/novell/cifs/share/nmasmthd/ntlm/config.txt -checkversion
  ```

  When prompted, type the admin password.

  For more information on nmasinst, see Using the nmasinst Utility to Install a Login Method in the Novell Modular Authentication Services 3.3.4 Administration Guide.

  After installation or upgrade of NMAS method, ensure that NMAS method is synchronized in eDirectory as described in section "Synchronizing NMAS Login Methods Is Required to Avoid Login Failures" in the *OES 11 SP3: Planning and Implementation Guide*.

NOTE: During the installation of a newer version of CIFS, it might try to include some NMAS methods that might already be existing on your server. In this case, the following error occurs `Add Method: 694 - ERROR: -16024`. This occurs only when the patches are updated from the command line interface. This error can be ignored as it does not cause disruption to any service. The NMAS methods present in the server are retained and are not overwritten.

5.4 Verifying the Installation

Perform the following steps if you want to verify that the installation was successful. For troubleshooting your installation, see Section 11.2, "CIFS Installation and Configuration," on page 82.

- Section 5.4.1, "Verifying Files and Folders," on page 35
- Section 5.4.2, "Verifying the File Configuration Information," on page 36
- Section 5.4.3, "Verifying LSM Installation," on page 36

5.4.1 Verifying Files and Folders

Run the following commands on the OES 11 SP3 server console:

1. Run the `ls /opt/novell/cifs/` command and verify that the `bin`, `schema`, and `share` folders are present.

2. Run the following commands and verify the presence of the following files:

Commands	Files
`ls /opt/novell/cifs/bin`	- cifs-config.sh - cifs_create_proxy_user.sh - cifs-lcm.sh - cifs_proxy_rights_assign.sh - cifs_retrieve_proxy_cred.sh - cifs_update_proxy_cred.sh - encrypt_password - getpwpolicies.sh - novcifs - retrive_proxy_cred - verify-user.sh
`ls /opt/novell/migration/sbin`	`migcifs.sh` `migcifs.pl` `migCifsS` `migCifsC` `readCasaC`

3. Run the `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 that 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 -a /etc/opt/novell/cifs`.

6 Check for `libcifslcm.so` library under `/usr/lib64`.

5.4.2 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.

5.4.3 Verifying LSM Installation

LSM installation can be verified either through iManager or Local File System.

Verifying through iManager

1 In iManager, click **NMAS**.

2 Under **NMAS Login Methods and NMAS Login Sequences**, verify that the `cifslinlsm` method is present.

Verifying through Local File System

1 Verify that CIFSLINLSM_X64 is present at `/var/opt/novell/eDirectory/data/nmas-methods` on a 64-bit system.

5.5 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 more information, see the *NetIQ® iManager Administration Guide*.

2 Click **Configure**, then go to **Plug-In Installation > Available Novell Plug-In Modules**.

For more information, see the *NetIQ® iManager Administration Guide*.

3 Select the **CIFS Management** plug-in from the list, then click **Install**.

4 Exit iManager.

5 From the OES 11 SP3 server console, run the following commands to complete the plug-in installation:

```
rcnovell-tomcat6 restart
```

5.6 What's Next

When the installation is complete, you can get started with CIFS administration activities. For details, see Chapter 6, "Administering the CIFS Server," on page 39.

6 Administering the CIFS Server

CIFS on an Open Enterprise Server (OES) 11 SP3 server can be managed and administered either through iManager 2.7.7 or from the command line.

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

CIFS maintains a configuration file and context search information that is set up during installation. An eDirectory search context is created by default during the OES 11 SP3 installation for all users who require access to the network. These contexts are saved in the context search file. When users specify a user name, the CIFS component running on the server searches each context in the list until it finds the correct user object.

For details on how to install the CIFS iManager plug-in, see Section 5.5, "Installing the CIFS iManager Plug-In," on page 36.

For basic information on command line administration, see Section 6.2, "Using the Command Line to Manage CIFS," on page 52 or for complete details, see Appendix A, "Command Line Utility for CIFS," on page 99.

6.1 Using iManager to Manage CIFS

You can manage CIFS services from iManager 2.7.7 and further versions. The recommended method to configure, manage, and modify CIFS properties and parameters is by using iManager.

NOTE: Admin equivalent/container admin users should be LUM-enabled in order to manage the CIFS server through the CIFS iManager plug-in. For more information, see "Using Novell iManager for Linux User Management" in the OES 11 SP2: Novell Linux User Management Administration Guide.

6.1.1 Prerequisites

* Install the CIFS iManager plug-in. For details, see Section 5.5, "Installing the CIFS iManager Plug-In," on page 36.
* Install CIFS on at least one OES 11 SP3 server. For details, see Chapter 5, "Installing and Setting Up CIFS," on page 27.
* Ensure that `ndsd` is running. Use `/etc/init.d/ndsd status` on the server console to check.

6.1.2 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`

where server_IP_address is the IP address of the server on which iManager is running.

For example:

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

2 At the login prompt, specify the server administrator user name, password, and tree name or IP address of the tree, then click **Login**.

For more information on iManager administration, see the *NetIQ® iManager Administration Guide*.

3 In the left pane of the iManager application, 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 11 SP3 server name.

or

Browse and select the server using the object selector.

or

Select the server from the object history list.

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

The information displayed changes to reflect the current state and properties of the selected server.

If a Samba server is running on the same server, CIFS will not start. See Section 11.1.1, "CIFS Does Not Start If Samba is Running," on page 81 to resolve the problem.

6 Continue with other administrative actions as necessary:

- Section 6.1.3, "Setting the CIFS Server and Authentication Properties," on page 42
- Section 6.1.4, "Managing CIFS Shares," on page 47
- Section 6.1.5, "Configuring a CIFS User Context," on page 50

6.1.3 Setting the CIFS Server and Authentication Properties

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

For information on starting iManager and accessing the CIFS server, see Section 6.1.2, "Selecting a Server to Manage," on page 40.

To change these parameters from command line, see Section 6.2.5, "Modifying the CIFS Configuration," on page 53.

- "Setting CIFS General Server Parameters" on page 42
- "Enabling and Disabling SMB Signing" on page 44
- "Setting CIFS General Authentication Parameters" on page 44

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 6-1   CIFS General Server Parameters

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

Table 6-1   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 11 SP3 server name.
WINS IP Address	The address of the WINS server.
Comment	The text in the Comment field is displayed when viewing details of the server. This can be useful if you want to provide a more detailed description of the server. 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 enabled by default.
Distributed File Services (DFS) Support	This option enables Distributed File Services support in CIFS. The option is disabled by default.
SMB Signature	This option is **Disabled by default**. Select **Mandatory** or **Optional** or **Disabled**. For details, see "Enabling and Disabling SMB Signing" on page 44.

Enabling and Disabling SMB Signing

SMB signing is a security mechanism designed to improve the security of the CIFS protocol. With SMB signing, an authenticating signature is added by placing a digital signature into each SMB packet. The digital signature is then verified by both the client and the server. It can be set to mandatory or optional mode. For more information, see Microsoft Knowledge Base article.

SMB signing should be turned off when domain authentication is configured.

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. When third party domain authentication is selected, SMB signing is disabled.

The functionality of CIFS third party domain authentication in OES is as same as in NetWare.

Figure 6-2 *CIFS Authentication Page Parameters*

Table 6-2 *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 (user name and password) on an OES 11 SP3 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 user name and password on the domain controller must match the user name 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.

Parameters	Description
Work Group / Domain Name	The workgroup or Windows domain to which the CIFS users belong.
	The domain name should be a valid DNS entry or the NetBIOS name of the domain. For more information, see Microsoft Knowledge Base article.
LMCompatibilityLevel	NTLMv2 is an authentication protocol that is cryptographically stronger than NTLMv1. NTLMv2 is not negotiated between the client and the server. The protocol does not determine the challenge or response algorithms, so it must be configured on both the client and the server.
	On a Windows client set the LMCompatibilityLevel by modifying the Windows registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA.
	On the server ser the LMCompatibilityLevel by running the `novcifs [-L 0│4│5] --lm=0│4│5` command.
	Novell CIFS currently supports 0, 4, and 5 compatibility levels for NTLMv2.
	Select the appropriate LMCompatibilityLevel from the drop-down list.
	◆ **Accept LM and NTLM responses (Default setting) - Level 0:** The server or domain controller compares the client's responses against LM, NTLM, LMv2, and NTLMv2 responses. Any valid response is accepted.
	◆ **Accept NTLM response/refuse LM response (NTLM authentication) - Level 4:** The server or domain controller accepts a valid LM, NTLM, LMv2, or NTLMv2 response.
	◆ **Accept NTLMv2 response /refuse LM and NTLM response (NTLMv2 required) - Level 5:** The server or domain controller compares the client's responses, using only LMv2 and NTLMv2.
	NOTE: When the **Accept NTLMv2 responses** only option is selected and you are attempting to map a share from a Windows 7 or Windows 8 workstation, make sure you specify the domain name along with the user name for the mapping to be successful.
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 the PDC reboots and the address changes.

6.1.4 Managing CIFS Shares

The **Share** 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 6.1.2, "Selecting a Server to Manage," on page 40.

To manage CIFS Shares from command line, see Section 6.2.7, "Working with CIFS Shares," on page 54.

Figure 6-3 *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 47
- ◆ "Editing a CIFS Share" on page 48
- ◆ "Removing a CIFS Share" on page 50
- ◆ "CIFS Share Parameters" on page 50

Adding a New CIFS Share

Before adding a new share, ensure that your CIFS server is running. For details on how to start the server, see Section 6.1.2, "Selecting a Server to Manage," on page 40.

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 **Add**.

For information on starting iManager and accessing the CIFS server, see Section 6.1.2, "Selecting a Server to Manage," on page 40.

New Share   ?

required = *

Share names can have up to 80 characters and contain characters
A to Z, 0 to 9, _, !, @, #, $, %, &, (,). Names cannot begin or end
with the "_" (underscore) character or contain "__" (multiple underscores).

Share Name*: [   ]

Volume*:   [   ] 🔍
Path*:   [   ]

              (vol: or vol:\directorypath)

Comment: [   ]

        [OK   ]   [Cancel]

2 Specify the **Share Name, Volume, Path**, and **Comment** for the new share. For details, see Table 6-3 on page 50.

3 Click **OK** to save your changes.

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

☑ **Complete: Success**

The share, CIFSShare, was successfully created.

        [OK   ]   [Repeat Task]

Editing a CIFS Share

Before editing a share, ensure that your CIFS server is running. For details on how to start the server, see Section 6.1.2, "Selecting a Server to Manage," on page 40.

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.

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 6.1.2, "Selecting a Server to Manage," on page 40.

Edit Share: VOL1   ?

required = *

Share names can have up to 80 characters and contain characters
A to Z, 0 to 9, _, !, @, #, $, %, &, (,). Names cannot begin or end
with the "_" (underscore) character or contain "__" (multiple underscores).

Share Name*:

VOL1

Path*:

VOL1   Modify

Comment:

NSS Volume1

OK   Cancel

2 Modify the **Share Name** or **Path** or **Comment** for the share. For details, see Table 6-3 on page 50.

3 Click the **Modify** button to modify the **Volume** and **Path** on the pop-up screen. For details, see Table 6-3 on page 50.

Modify Share Path   ✕

Volume*:   🔍

Path*:

(vol: or vol:\directorypath)

OK   Cancel

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 6.1.2, "Selecting a Server to Manage," on page 40.

1 On the default CIFS server page in iManager, click the **Share** tab, 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 the information in the following table to create and edit CIFS shares.

Table 6-3 *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 11 SP3 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 can contain only single-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 can contain only single-byte characters.

6.1.5   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 6.2.8, "Configuring the CIFS Context Search File," on page 55.

The recommended method is to use iManager to configure the search context.

Figure 6-4 *CIFS Context Page*

CIFS

To manage a CIFS server, select a server where CIFS is installed.

Server: oesbox.novell

| General | Share | **Context** |

Add... | Remove

☐ **Context**

☐ o=novell
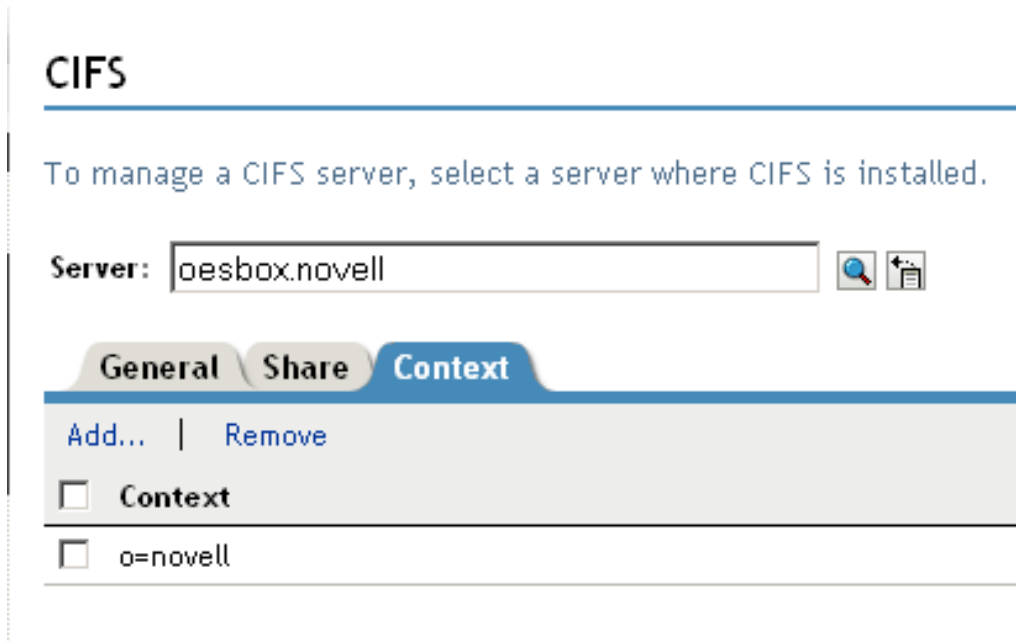
- ◆ "Adding a New Context" on page 51
- ◆ "Removing a Context" on page 51

Adding a New Context

Before adding a new context, ensure that your CIFS server is started and running. For details on how to start the server, see Section 6.1.2, "Selecting a Server to Manage," on page 40.

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

Figure 6-5 *Add New Context*

Context   ?

New

OK   Cancel

2 Use the object selector to select a context to add, then click **OK** to save.

Removing a Context

Before removing a context, ensure that your CIFS server is started and running. Select one or more contexts, then click **Remove**.

6.1.6 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.

6.2 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, "Command Line Utility for CIFS," on page 99 or enter `man novcifs` at the command prompt.

- Section 6.2.1, "Starting CIFS," on page 52
- Section 6.2.2, "Stopping CIFS," on page 52
- Section 6.2.3, "Restarting CIFS," on page 52
- Section 6.2.4, "Monitoring CIFS," on page 53
- Section 6.2.5, "Modifying the CIFS Configuration," on page 53
- Section 6.2.6, "Anonymous Login for CIFS," on page 53
- Section 6.2.7, "Working with CIFS Shares," on page 54
- Section 6.2.8, "Configuring the CIFS Context Search File," on page 55

6.2.1 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 Section 11.1.1, "CIFS Does Not Start If Samba is Running," on page 81.

6.2.2 Stopping CIFS

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

6.2.3 Restarting CIFS

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

6.2.4 Monitoring CIFS

Use the `rcnovell-cifs monitor` command to monitor the status of the CIFS server.

If the CIFS server is not running, the monitor script starts the CIFS server and returns the status.

6.2.5 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 6.1, "Using iManager to Manage CIFS," on page 39.

To edit the CIFS configuration from command line:

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

IMPORTANT: We recommend that you do not change the default settings in this file.

---

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 server.
- In the DOMAIN / WORKGROUP section, specify the Windows domain name for third-party domains and workgroup for the local option.
- 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 in order for the configuration changes to take effect.

6.2.6 Anonymous Login for CIFS

Anonymous login for CIFS can be used to map to the CIFS share without a user name and password.

If a user attempts to log in to a CIFS server with a user name that does not exist in eDirectory, he or she will be logged in as a guest user. The guest user will be granted rights applicable for a Public Trustee.

The anonymous configuration is set at the server level, so the anonymous login settings affect all CIFS shares on the server.

- "Setting Anonymous Login" on page 54
- "Anonymous Login in a Cluster" on page 54

Setting Anonymous Login

To set anonymous login, use the following command:

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

The CIFS connections logged in as an anonymous user have privileges on the NSS volumes assigned to the Public trustee. The Public trustee rights can be set on any folder in an NSS volume by using the Novell Client. For more information, see the Novell Client for Linux documentation.

If you don't have the Novell Client installed, you can use iManager to add Public trustee rights. For more information, see "Viewing, Adding, or Removing File System Trustees" in the OES 11 SP3: File Systems Management Guide.

Anonymous Login in a Cluster

In a cluster setup, anonymous login must be configured on every node and must be set to the same configuration level for consistent behavior across all shares.

This needs to be done for all CIFS server parameters except for server name, server comment, and shares.

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

6.2.7 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 a virtual server object using the command line (novcifs). If the shares are added on a cluster resource using the command line, then all the shares are lost if the resource leaves that node.

NOTE: Whenever a CIFS service is restarted on a node (node A) that hosts a cluster resource, the resource must be moved offline. It must then be available online or migrated to another node (node B) and brought back to the original node (node A) so 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 6.1.4, "Managing CIFS Shares," on page 47.

To manage CIFS shares using the console, see the following sections:

- "Adding a New Share Point on a Non-Clustered Volume (Login to the node as root)" on page 101
- "Removing a Share Point on a Non-Clustered Volume (Login to the node as root)" on page 102
- "Displaying the List of Share Points" on page 101

- "Displaying Details of a Share Point" on page 101
- "Enabling or Disabling SMB Signing" on page 103.

6.2.8 Configuring the CIFS Context Search File

Do not modify the CIFS Context Search file directly in a text editor. You should use iManager to configure the search context. For information, see Section 6.1.5, "Configuring a CIFS User Context," on page 50.

To edit the CIFS Context Search File:

1 Open the `/etc/opt/novell/cifs/cifsctxs.conf` file in a text editor.

2 Specify the context to be added, in dot format, for example, ou=fa-testing.o=novell

3 Save the file.

6.3 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.
- **Opportunistic Locking:** Opportunistic Locking, or Oplocks, improves file access performance and is enabled by default. Oplocks must be enabled on the server for Offline files to function correctly on Windows XP, Windows Vista, and Windows 7.

  IMPORTANT: If a file is opened with multiple protocols when the migration or failover begins, the file should be closed and reopened after the migration or failover, to acquire cross-protocol locks on the new node.

For more information, see "Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks" in the *OES 11 SP3: NCP Server for Linux Administration Guide*.

6.4 Third-Party Domain Authentication

For third-party domain authentication, the clients are members of a third-party domain such as Windows. A Windows domain controller performs the user authentication. The user name and password on the domain controller must match the user name and password used to log in to the Windows workstation.

Ensure that you understand and meet the following prerequisites before setting up third-party authentication:

6.4.1 Prerequisites

Prerequisites for the Windows Primary Domain Controller

- Ensure that the Primary Domain Controller (PDC) is up and reachable by using the NETBIOS name of the PDC from the CIFS server. For example, WINPDC_W.

- Disable the autodisconnect feature in the PDC to avoid resetting connection from the PDC to the CIFS server. You can do this by configuring the timeout value (in minutes) for idle sessions through the autodisconnect parameter.

  The valid value range is -1 to 65535. Setting the timeout period value to -1 completely disables the auto-disconnect of the idle sessions feature.

  ```
  net config server /autodisconnect:-1
  ```

  For more information about how to configure the timeout period (autodisconnect parameter), see "How Autodisconnect Works in Windows NT and Windows 2000" (http://support.microsoft.com/kb/138365).

- Disable SMB signing

  Modify the values of registry keys **EnableSecuritySignature** and **RequireSecuritySignature** to 0.

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters

  ```
  Value Name: EnableSecuritySignature
  Data Type: REG_DWORD
  Data: 0 (disable), 1 (enable)

  Value Name: RequireSecuritySignature
  Data Type: REG_DWORD
  Data: 0 (disable), 1 (enable)
  ```

  For more information, see "Overview of Server Message Block Signing" (https://support.microsoft.com/kb/887429?wa=wsignin1.0).

- Set Lmcompatibilitylevel on Windows 7 and Windows 8 Clients.

  1. Click **Start**, type **secpol.msc** in the **Start Search** box, and then press **ENTER**.
  2. On the left pane, select **Local Policies** > **Security Options**.

3. On the right pane, scroll down and double-click **Network Security: LAN Manager authentication level**.

4. Change the setting from **Send NTLMv2 Response only** to **Send LM & NTLM - use NTLMv2 session security if negotiated**.

For more information, see "How do I check the NTLM authentication Settings? (http://www.nbtnet.newboundary.com/support/docs/ppm/pm_chm.htm#ppm/troubleshooting/tasks/ppm0114.htm)"

◆ Restrict NTLM authentication.

1. Click **Start**, type **gpedit.msc** in the **Start Search** box, and then press **ENTER**.

2. On the left pane, select **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

To enable NTLM Pass-through Authentication,

1. On the right pane, modify the following policies:

Network security: Restrict NTLM: Incoming NTLM traffic. Set this to Allow all

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers. Set this to Allow all.

Network security: Restrict NTLM: Audit NTLM authentication in this domain. Set this to Enable all.

Network security: Restrict NTLM: Audit Incoming NTLM Traffic. Set this to Enable auditing for all accounts.

2. Close the Policy Editor.

3. At the command prompt, run `gpupdate /force`.

To disable restrictions on NTLM authentication,

1. Network security: Restrict NTLM: Incoming NTLM traffic. Set this to Allow all.

2. Close the Policy Editor.

3. At the command prompt, run `gpupdate /force`.

For more information, see "NTLM and Pass-through Authentication" (https://support.software.dell.com/kb/119536).

◆ The desktop user or the user that has joined the domain must be the same as the CIFS user.

◆ For Windows 2008 Server and later versions, apply the changes as indicated in the Microsoft Knowledge Base article.

NOTE: To access the CIFS shares when you are using third-party authentication, the Windows client might be required to log in as the same user with the same password.

Prerequisites for the CIFS Server

◆ Ensure that SMB signing is disabled on the CIFS server. For details, see "Enabling and Disabling SMB Signing" on page 44.

6.4.2 Using iManager to Enable Third-Party Authentication

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 user name, password, tree name, or IP address of the tree, then click **Login**.

Login

Username:

admin

(Ex: admin or admin.novell)

Password:

●●●●●●

Tree:

192.168.0.1

(192.168.14.199, mytree, myserver.company.com)

Login

® Copyright 1999-2008 Novell, Inc. All rights reserved.

For more information on iManager administration, see the *NetIQ® iManager 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 Select the CIFS server you want to manage.

5 Select **General > Authentication**.

6 Select **Third party Domain** as the mode of authentication.

7 Specify the **Work Group/Domain Name** of the Windows environment.

8 Specify the **LMCompatibility level**. For details, see Table 6-2, "CIFS Authentication Page Parameters," on page 45.

9 Specify the name of the Primary Domain Controller. Ensure that the name does not exceed 15 characters.

10 Specify the IP address of the Primary Domain Controller.

11 Click **OK** to save the changes in the CIFS properties.

6.5 Dynamic Storage Technology for CIFS Server

Dynamic Storage Technology (DST) for Novell Open Enterprise Server (OES) 11 SP3 is an information life-cycle management technology that uses a policy-based approach for relocating data between two Novell Storage Services (NSS) volumes located on different devices, and transparently provides a unified view of the file tree to users. You specify policies that classify data to be moved by its frequency of use, filename, file type, and file size. Policy enforcement is automated with scheduled and on-demand runs of the policies. DST allows you to seamlessly tier storage between high-performance and lower-performance devices.

For example, you can establish policies that keep frequently used mission-critical data on high-performance devices, and move rarely accessed less-essential data to lower-performance devices. Backup can be performed separately on the two volumes, which allows for different backup schedules. Dynamic Storage Technology enables you to manage data more efficiently for the enterprise and in doing so, the enterprise can potentially realize significant cost savings in storage management.

CIFS server for Linux provides the CIFS services for NSS volumes on Linux. Dynamic Storage Technology is a component of NCP Server.

Enabling DST: DST is automatically enabled when the shadow volume is added to the primary volume.

CIFS DST supports only NSS volumes being used as shadow volumes. If you plan to use DST, you need to install NSS when you install CIFS server and Dynamic Storage Technology. The NSS volumes must meet the "Storage Requirements for DST Volume Pairs" in the *OES 11 SP3: Dynamic Storage Technology Administration Guide*.

DST for CIFS server allows you to specify a shadow relationship between two volumes, which forms a shadow volume pair. The secondary directory tree structure, or shadow file tree, shadows the primary file tree. For more information, see "Planning for DST Shadow Volume Pairs and Policies" in the *OES 11 SP3: Dynamic Storage Technology Administration Guide*.

DST presents a unified view to users of the subdirectory trees on each volume. The primary file tree and secondary file tree have the same directory structure so that each subdirectory appears in both locations as data is moved between the two volumes. The primary tree and the secondary tree are overlaid to create one virtual volume tree that is transparently presented to the users. The CIFS users are not aware of the actual physical location of the files. For more information, see "Data Access Requirements for a DST Shadow Volume Pair" in the *OES 11 SP3: Dynamic Storage Technology Administration Guide*.

For more information about "Configuring DST Global Policies" see the *OES 11 SP3: Dynamic Storage Technology Administration Guide*.

6.6 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 both source (the server that hosts the junction) and target (the server that is pointed to by the junction) servers in order for the junctions to work. The junctions that point to subdirectories are also supported with CIFS Linux. For more information, see "Managing DFS Junctions" in the *OES 11 SP3: Novell Distributed File Services Administration Guide for Linux*.

6.6.1 Prerequisites

- Unicode must be enabled.
- DFS must be enabled for CIFS on all host and target servers.
- Both host and target CIFS servers must be running.
- The VLDB server must be running.
- CIFS clients should be able to resolve NetBIOS name of CIFS server on the target server. Without this, the clients will not be able to connect to the DFS Target.
- CIFS users should have required rights on both DFS source and target volumes. Without this, the clients will not be able to perform required operations.

IMPORTANT: The CIFS clients accessing DFS junctions must be DFS aware. From Linux SMB clients, junctions on OES cannot be traversed through Novell CIFS.

6.6.2 Enabling DFS Support

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 6-6 *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**.

NOTE: You can also enable DFS support for the CIFS server with the novcifs command line utility `--dfs-support=yes|no`.

6.6.3 Limitations

- Junctions from Linux to a NetWare system work only when the junction target is the root of the volume. However if both the source and target is on a Linux system, then junctions to subdirectories also work.

  Junctions in NetWare cannot point to volumes in Linux.

- DFS is available only if Unicode (UTF8 format) is enabled.
- Only CIFS shares are enabled with DFS support.

6.7 Subtree Search

A subtree search login enables CIFS to search for a user in the entire base context of a tree. The subtree search setting that is saved in the `cifs.conf` file stays persistent even if the system or service is restarted.

- Section 6.7.1, "Prerequisites," on page 63
- Section 6.7.2, "Enabling a Subtree Search," on page 63
- Section 6.7.3, "Subtree Search in a Cluster Setup," on page 63

6.7.1 Prerequisites

To use the subtree search feature, the CIFS proxy user should have read rights for the base context. These rights are assigned automatically from iManager when the context is added.

6.7.2 Enabling a Subtree Search

After you have finished installing CIFS, start the CIFS server and enable the subtree search by using the following command:

```
novcifs -y yes
```

To disable the subtree search, use the `novcifs -y no` command.

You can choose to enable or disable the subtree search before the user starts connecting to the CIFS server.

6.7.3 Subtree Search in a Cluster Setup

A subtree search can be configured only at a physical server or node level. In a cluster setup, each node should be configured with the same configuration level for consistent behavior.

NOTE: The time taken for the LDAP search to be completed depends on the WAN link and on the number of user replicas in the tree.

6.8 Enabling Offline Files Support

Offline Files helps you be more productive. You can use this feature on a portable computer, or on a desktop computer that occasionally connects to your workplace network. For example, this feature is useful if you are working at home on a desktop computer, and need to automatically get files off the network whenever you connect.

The files that you select are automatically downloaded from shared folders on the network and stored on your computer. When you disconnect, the files are available to use. When you reconnect to the network, your changes are added to the files on the network in a process called synchronization. If someone else on the network made changes to the same file, you can save your version, keep the other version, or save both.

You can enable client-side caching by using the following command:

```
novcifs [--csc= 0|1|2|3]
```

This feature configures the client-side caching feature that can be used to store frequently used information on the client's machine.

0 Enables Windows clients to cache files for offline use. Does not permit automatic file-by-file re-integration. (Default)

1 Enables Windows clients to cache files for offline use. Permits automatic file-by-file reintegration.

2 Enables Windows clients to cache files for offline use. Clients are permitted to work from their local cache even while online.

3 Does not permit Windows client to cache files for offline use.

For information on configuring workstations to use offline files, see Microsoft Knowledge Base article.

6.9 Directory Cache Management for CIFS Server

Table 6-4 *Server Parameter Information for Directory Cache Management*

Parameter Name and Description	Default Value	Value Options
MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY Controls the maximum number of file entries that can be cached by the system for a given folder in the directory cache.	10240	Minimum is 512 files.
MAXIMUM_CACHED_FILES_PER_VOLUME Controls the maximum number of file entries that can be cached by the system for a given volume in the directory cache.	256000	Minimum is 2048 files.
MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME Controls the maximum number of folder entries that can be cached by the system for a volume in the directory cache.	102400	4096

6.10 What's Next

To learn how to use CIFS services as an end user, see Chapter 10, "Working with Client Computers," on page 77.

7 Migrating CIFS to OES 11 SP3

The Open Enterprise Server (OES) 11 SP3 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 11 SP3 server either by using the GUI Migration Tool or from the command line. For more information on NetWare CIFS, see the *NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide*.

To get started with migration, see the *OES 11 SP3: Migration Tool Administration Guide*.

For more information on migrating CIFS, see "Migrating CIFS to OES 11 SP3" in the *OES 11 SP3: 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 11 SP3: Migration Tool Administration Guide*.

8 Running CIFS in a Virtualized Environment

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) 11 SP3, and requires no special configuration or other changes.

To get started with Xen virtualization, see the SLES 11 Virtualisation with Xen Aministration Guide.

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

For information on setting up virtualized OES 11 SP3, see "Installing, Upgrading, or Updating OES on a VM" in the *OES 11 SP3: Installation Guide*.

8.1 What's Next

To learn more about what you can do with CIFS on OES 11 SP3, continue with Chapter 6, "Administering the CIFS Server," on page 39.

9 Configuring CIFS with Novell Cluster Services for an NSS File System

Novell Cluster Services for Open Enterprise Server (OES) 11 SP3 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.

9.1 Benefits of Configuring CIFS for High Availability

With the OES 11 SP3 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 11 SP3, 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.
- 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.

9.2 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 Resource 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 active.

- **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.

- **Monitor script:** A file that contains the cluster resource commands that allows Novell Cluster Services to detect when an individual resource on a node has failed independently of its ability to detect node failures. The script is generated by default, but monitoring for a resource is not enabled by default. For information about how to enable and configure monitoring for a resource, see "Enabling Monitoring and Configuring the Monitor Script" in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*.

- **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.

9.3   CIFS and Cluster Services

Novell Cluster Services can be configured either during or after OES 11 SP3 installation. In a cluster, Novell CIFS for OES 11 SP3 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 9.3.1, "Prerequisites," on page 70
- Section 9.3.2, "Using CIFS in a Cluster Environment," on page 71
- Section 9.3.3, "Example for CIFS Cluster Rights," on page 72

9.3.1   Prerequisites

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

☐ Novell Cluster Services installed on OES 11 SP3 servers

For information on installing Novell Cluster Services, see "Installing, Configuring, and Repairing Novell Cluster Services" in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*.

For information on managing Novell Cluster Services, see " Managing Clusters" in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*.

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

Follow the instructions in Section 5.1, "Installing CIFS during the OES 11 SP3 Installation," on page 27 and Section 5.2, "Installing CIFS after the OES 11 SP3 Installation," on page 31.

9.3.2 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, the iManager tool, or the Novell Linux Volume Manager utility.

   For requirements and details about configuring shared NSS pools and volumes on Linux, see "Configuring and Managing Cluster Resources for Shared NSS Pools and Volumes" in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*.

   For details on creating a pool using Novell Linux Manager using the `nlvm create pool` command, see "NLVM Commands" in the *OES 11 SP3: NLVM Reference*.

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. **Configuring Monitor Script:** Configure resource monitoring to let the cluster resource failover to the next node in the preferred nodes list.

   When `rcnovell-cifs monitor` is invoked, it does the following:

   - ◆ Returns the status of CIFS, if CIFS is already running.
   - ◆ Starts a new instance of CIFS and returns status, if CIFS is not running (dead/etc.).

   Each time the monitor script detects that the CIFS service is down and starts the service, a message in the following format is logged in the `/var/log/messages` file:

   ```
   CIFS: Monitor routine, in novell-cifs init script, detected CIFS not
   running,starting CIFS
   ```

   For more information, see "Configuring a Monitor Script for the Shared NSS Pool" in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*

   IMPORTANT: Set the number of **Maximum Local Failures** permitted to 0. This ensures that if the CIFS server crashes, cluster services will trigger an immediate failover of the resource.

---

5. **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
```

For example, `novcifs --add '--vserver=".cn=CL-POOL-SERVER.o=novell.t=VALTREE."'`
`--ip-addr=10.10.10.10`

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.

6. **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
```

For example, `novcifs --remove '--vserver=".cn=CL-POOL-`
`SERVER.o=novell.t=VALTREE."' --ip-addr=10.10.10.10`

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.

7. **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)

   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.

9.3.3 Example for CIFS Cluster Rights

This section describes the rights management in cluster. It explains the rights required in CIFS and
explains with an example.

In a cluster, each cluster node can have an assigned CIFS Proxy User identity that is used to
communicate with eDirectory. As a best practice, the CIFS Proxy User is in the same eDirectory
context as the NCP Server object. Typically, this context is the OU where you create the cluster and
its cluster resources. If Common Proxy User is selected, the proxy user is always created in the same
context as cluster node.

When you add CIFS as an advertising protocol for a cluster pool resource (enabling CIFS on shared
NSS pool), the NCS:NCP Server object for the cluster resource will be treated as a CIFS virtual
Server object. Following CIFS specific attributes are added to the CIFS virtual server object:

- *nfapCIFSServerName* (read access)
- *nfapCIFSAttach* (read access)
- *nfapCIFSShares* (read access)
- *nfapCIFSComment* (read access)

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

You can grant these rights plus the inherit right at the OU level of the context that contains the cluster. This allows the rights to be inherited automatically for each CIFS Virtual Server object that gets created in the cluster when the CIFS Proxy User is in the same eDirectory context. If the CIFS Proxy Users are not in the same context as the CIFS Virtual Server object, you can set the rights at a higher OU level that includes the contexts for proxy users and the contexts for the CIFS Virtual Server objects. You can alternatively grant the rights for each CIFS Proxy User on the CIFS attributes on every CIFS Virtual Server object. To simplify the rights configuration, you can create an eDirectory group with members being the CIFS Proxy Users of the nodes in the cluster, and then grant the rights for the group.

The following sample use case explains the rights management in clusters.
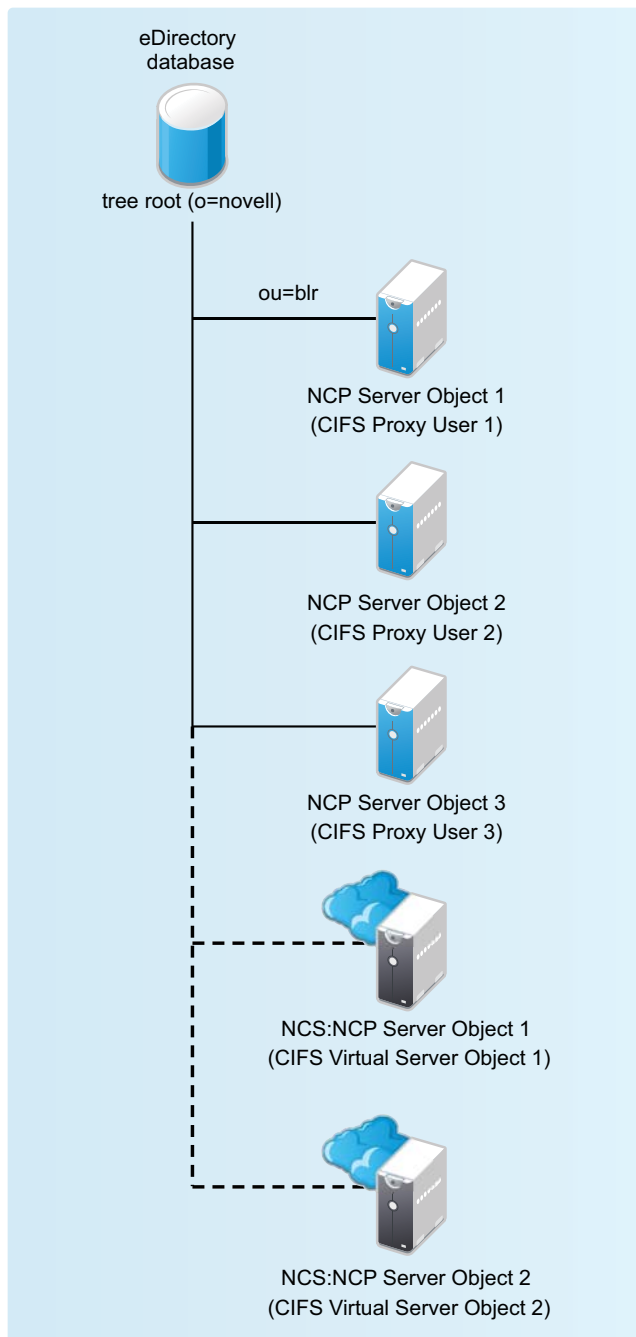
The CIFS proxy user 1, CIFS proxy user 2, and CIFS proxy user 3 have rights to read the eDirectory CIFS attributes under ou=blr (CIFS Virtual Server Object 1 and CIFS Virtual Server Object 2). Hence if these virtual servers are hosted in any of these three nodes, the configuration is read by the CIFS service in the corresponding node.

Granting Rights to CIFS Proxy Users Over Cluster Resources

1 Set up the cluster and add nodes to it.

2 Install Novell CIFS on each node.

3 Configure a *clustername_CIFS_PROXY_USER_GROUP* in eDirectory and add the CIFS Proxy user of each node in the cluster as a member.

4 Grant the group the eDir read, write, compare, and inherit rights for the CIFS attributes at the cluster OU level.

5 Configure a pool cluster resource and enable CIFS to create the CIFS Virtual Server object for the resource.

6 Verify that the CIFS Proxy User on each node is able to read the CIFS attributes and CIFS works as intended.

9.4 Configuring CIFS in a Cluster

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

9.4.1 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 disk you want to use for the pool is configured through the iSCSI or SAN software. It is marked as **Shareable for Clustering** by using NSSMU, the Storage plug-in to iManager, or the `nlvm share` command.

9.4.2 Creating Shared Pools and Accessing Sharepoints

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

Creating Pools Using iManager

For details on creating pools by using iManager, see "Creating a Pool" in the *OES 11 SP3: NSS File System Administration Guide for Linux*.

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

Creating Pools Using NSSMU

For details on creating pools by using NSSMU, see "NSS Management Utility (NSSMU) Quick Reference" in the *OES 11 SP3: NSS File System Administration Guide for Linux*.

Creating Pools Using NLVM

For details on creating pools by using NLVM, see "NLVM Commands" in the *OES 11 SP3: NLVM Reference*

You can add Novell CIFS as an advertising protocol when you create a cluster-enabled NSS pool. For information, see "Creating Cluster-Enabled Pools and Volumes."

You can add Novell CIFS as an advertising protocol when you cluster-enable an existing NSS pool. For information, see"Cluster-Enabling an Existing NSS Pool and Its Volumes."

You can add or remove Novell CIFS as an advertising protocol for an existing cluster-enabled NSS pool. For information, see "Adding Advertising Protocols for NSS Pool Cluster Resources."

9.5 What's Next

For information about managing the CIFS services by using iManager or the command line interface, see Chapter 6, "Administering the CIFS Server," on page 39.

For an explanation of how end users access network files from different workstations by using CIFS, see Chapter 10, "Working with Client Computers," on page 77.

10 Working with Client Computers

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

- Section 10.1, "Accessing Files from a Client Computer," on page 77
- Section 10.2, "Mapping Drives and Mounting Volumes," on page 78

10.1 Accessing Files from a Client Computer

You can access files and folders hosted on a CIFS server from Windows (XP, Vista, Win7) or Linux clients. Use one of the following methods to access the CIFS server from your clients:

- Section 10.1.1, "Accessing Files from a Windows Client," on page 77
- Section 10.1.2, "Accessing Files from a Linux Desktop," on page 78

10.1.1 Accessing Files from a Windows Client

- "Prerequisite" on page 77
- "Procedure to Access Files" on page 77

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 will not 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 is waiting for the server's response.

Procedure to Access Files

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

   In Windows 2000 and XP, click **My Network Places**. In Vista and Win 7, 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) 11 SP3 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.

10.1.2   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) desktop, you can also use `nautilus` to access the files.

Using an IP Address to Access Files

1 Run this command from the terminal:

```
smbclient://<SERVER_IP_ADDRESS>/<VOLUME_NAME or SHARE_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 terminal:

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

2 Enter the password when prompted.

Using nautilus to Access Files

1 Run this command from the nautilus address bar:

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

2 Enter the user name and password when prompted.

10.2   Mapping Drives and Mounting Volumes

You can map drives for accessing the CIFS share names from a Windows, Windows Vista, or Windows 7 client and mount the volumes from a Linux client.

10.2.1 Mapping Drives from a Windows Client

From a Windows (7, 8.1, or 10) 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 11 SP3 server name. For more information, contact your network administrator.

5 Specify the user name and password.

6 Click **OK** to proceed.

10.2.2 Mounting Volumes from a Linux Client

1 Log in as a `root` administrator.

2 From your console, enter the following command:

`mount -t cifs`

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

11 Troubleshooting CIFS

11.1 Known issues

11.1.1 CIFS Does Not Start If Samba is Running

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

Cause: Novell CIFS cannot coexist with Samba daemons as they both use the same port.

Action: Log in to the OES server as `root`. Use the following commands to stop the Samba daemons and restart the CIFS server:

- `rcsmb stop`
- `rcnmb stop`
- `rcnovell-cifs start`

11.1.2 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 11 SP3: Migration Tool Administration Guide*.

2 Reconfigure CIFS by using YaST on the target server.

For detailed YaST configuration steps, see Section 5.1, "Installing CIFS during the OES 11 SP3 Installation," on page 27 and Section 5.2, "Installing CIFS after the OES 11 SP3 Installation," on page 31.

11.1.3 File Level Trustees Are Deleted When a File is Modified

File level trustees might be deleted when a file is modified, depending on how the application works with files it opens for writing. Some third-party applications record changes in a temporary file in order to save internal memory or as a safety net to prevent data loss due to a power failure, system crash, or human error. When a user saves the changes, the application deletes the original file, and saves the temporary file with same name as the original file. In response to the deletion instruction, the file system deletes the original file as well as any file level trustees set on the file. The file system is not application aware; that is, it does not track the ultimate intent of the applications that you might use.

For more information, see "File-Level Trustees" in the *OES 11 SP3: File Systems Management Guide*.

11.2 CIFS Installation and Configuration

11.2.1 CIFS Does Not Start After Installation

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

Cause: CIFS might be installed as standalone after installing Open Enterprise Server (OES) 11 SP3.

Action: Restart the OES 11 SP3 server in order for the installation and configuration settings to take effect.

11.2.2 CIFS Terminates With Schema Not Extended Error After Installation

Cause: Proxy user credentials in the credential store (file/CASA) are not stored correctly.

Action: Reconfigure the CIFS proxy user.

11.3 Authentication

11.3.1 CIFS User Authentication Fails On an NTLMv2 enabled Windows XP Client in the First Attempt

Description: CIFS user authentication from a Windows XP client fails on the first attempt. The second time the user attempts to log in, authentication occurs as expected if NTLMv2 is enabled on Windows XP clients.

Cause: Windows XP sends the client machine name as a domain name. For the second attempt sends the actual domain name.

Action: Pass the user name in domainname\username format.

For example, if you are using net use command to map a CIFS share following is the command you can use.

```
net use <device name> \\<computer name or IP address>\<share> /user:<DOMAIN>\<USER>
<password>
```

```
net use * \\192.168.100.1\CIFS_VOL /user:BLR\cifsuser1 <password>
```

In this example, net use command is used to connect to the share named CIFS_VOL on a computer with IP address 192.168.100.1. The CIFS_VOL share will be mapped to the highest free drive letter [*].

```
net use e: \\192.168.100.1\CIFS_VOL /user:BLR\cifsuser1 <password>
```

In this example, net use command is used to connect to the share named CIFS_VOL on a computer with IP address 192.168.100.1. The CIFS_VOL share will be mapped to e: drive.

NOTE: NTLMv2 authentication is enabled by default on Windows 7 workstations.

11.3.2 Password Has Expired

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.

11.3.3 User Can Only See Folders Assigned With Public Trustee Rights

Error: Only folders to which the Public trustee has rights are visible.

Cause: If you have logged into a Windows workstation and see folders assigned only with Public Trustee rights, it is either because you have logged in with an incorrect user name or have logged in as a guest user.

Action: Log in with correct credentials.

11.3.4 Authentication Failed Due to Password Mismatch

Cause: The password is incorrect.

Action: Provide the correct password.

OR

Cause: Universal password is not set for the user.

Action: Set the universal password for the user.

OR

Cause: The client and the server have incompatible LMCompatibility level settings.

Action: Check for the LMComaptibility settings. For more information, refer "Setting LMCompatibilityLevel" on page 103.

11.4 Startup

- Section 11.4.1, "CIFS Is Not Starting," on page 84

11.4.1 CIFS Is Not Starting

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

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

1 Open YaST.

2 Click **Open Enterprise Server > OES Install and Configuration.**

3 On the Software Selection Page, click **Accept**.

   The status of the eDirectory service is displayed as **Reconfigure is disabled.**

4 To reconfigure, click **disabled** to change the status to **enabled.**

5 Click **Novell CIFS Service** to access the configuration dialog box.

6 Change the password in the **CIFS Proxy User Password** field.

   Specify a password that adheres to the password policy restrictions.

7 Retype the password in the **Verify CIFS Proxy User Password** field.

8 Click **Next** and continue with the remaining configuration steps in Section 5.2, "Installing CIFS after the OES 11 SP3 Installation," on page 31.

11.5 Migration

- Section 11.5.1, "CIFS Does Not Start After Migration Is Completed On The Target server," on page 84
- Section 11.5.2, "After Migration, the CIFS Server Does Not Come up on the Target Server by Default," on page 85

11.5.1 CIFS Does Not Start After Migration Is Completed On The Target server

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

Cause: CIFS configuration settings are not replicated to all the eDirectory servers containing the NCP server object for the target system.

Action: Ensure that all the eDirectory replicas containing target system NCP server object are in sync.

11.5.2 After Migration, the CIFS Server Does Not Come up on the Target Server by Default

Cause: CIFS configuration points to the proxy user used before the transfer ID migration and the old proxy user does not have rights on the new NCP server object after migration.

Action : CIFS server needs to be started manually, so that it reads the latest Proxy user which has proper rights on the NCP server object.

11.6 Mac Client

11.6.1 Unable to See the Contents of the Target That a Novell DFS Junction Points To

Cause: The Mac client sends the wrong password to the target server when attempting to set up a connection.

Action: Store the password of the user in the Mac keychain by selecting the "Remember this password in my keychain" check box in the login dialog that pops up when mapping to the CIFS share.

11.6.2 The Mac Client does not Display a Complete List of Available Shares

Cause: The CIFS server allows the Mac clients to map shares that have sharenames exceeding 12 chars, however, the CIFS server does not respond to the `NetShareEnum` request if the client uses a older version of `NetShareEnum` verb to get the list of all available shares.

Though the LANMAN protocol authenticates the trustees of the share, it will not list the share if the sharename exceeds 12 characters.

Action: It is recommended to specify the share name less than or equal to 12 characters.

11.6.3 Copying Multiple Large Files using Finder from a Mac OS X Client to an OES CIFS Share Fails

Error: Copying multiple large files using Finder from a Mac OS X client to an OES CIFS share fails with a "The operation could not be completed because <filename> is in use" message.

Cause: The pass-through information levels capability is not enabled on the Novell CIFS server, which causes an issue with the way Finder handles the Apple double files it creates during the copy operation.

Action: Enable the pass-through information levels capability for the Novell CIFS Server. The Novell CIFS server must be restarted after this option is modified.

11.7 DFS

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

Cause: Junction target has changed, but the Windows client is still pointing to the old target as it caches junction target information.

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

1 Restart the Windows client.

   or

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 Remap the drive.

11.7.2 Unable To Access DFS Junctions On A Novell CIFS Share From The Windows Client

Cause: The Windows client is not able to resolve the target OES server's IP address through NetBIOS.

Action: Add an entry with the CIFS server IP address and the NetBIOS name in the `HOSTS` and `LMHOSTS` files on the Windows client.

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

Windows does not prompt the server to resolve the junction every time it is accessed. It prompts the server only the first time and then caches it. When the junction is accessed the next time, Windows does not prompt the CIFS server to resolve the junction; instead it uses the target location that it received previously.

On a restart of the Windows machine, if the same mapping is used, it points to the 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 retrieves the latest value from the CIFS server.

11.8 Miscellaneous

11.8.1 Offline Files Synchronization Fails

Offline file synchronization fails to complete on a computer that is running Windows 7. Additionally logging the error message, "The specified network name is no longer available" in the Sync Center.

To fix this issue, apply the hotfix available on the Microsoft Support web site.

11.8.2 Synchronization of Offline Files Caching fails with the error "The process cannot access the file because it is being used by another process."

Cause: This error occurs on a computer that is running Windows 7, when Oplocks is disabled on the CIFS server or folders are taken offline on the client machine.

Action:

1. Enable Oplocks on the CIFS Server (Oplocks are enabled by default).
2. Delete the offline copy of the folder on the Windows client system.

For more information, see Section 6.8, "Enabling Offline Files Support," on page 63 and Section 13.3.6, "Oplocks," on page 97 in the OES 11 SP2: Novell CIFS for Linux Administration Guide.

11.8.3 Windows or Mac Unable to Resolve the NetBIOS Name of the CIFS Server

CIFS client on Windows 2000 Service Pack 4, Windows XP Service Pack 2, Windows Vista, Windows 7 or later releases, Mac 10.7 or later releases might have problems following DFS junctions over CIFS because of a defect in Windows and Mac client versions. (This problem exhibits itself in a pure Windows environment.) When using DFS with CIFS, this issue will be seen if the CIFS server and Windows / Mac 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 properly. This is a Microsoft / Mac CIFS client requirement, not a CIFS Linux server 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:

+ 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.

+ **Windows 2000:** `c:\WINNT\system32\drivers\etc\hosts`
+ **Windows XP/Vista/7 or later:** `c:\windows\system32\drivers\etc\hosts`

   If you do not have a hosts file, create the file.

+ **Mac 10.7 or later:** `/etc/hosts`

2 A line at the end of the file that identifies the IP address and NetBIOS name of the data server, such as.

```
192.168.1.1       servername_W
```

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

IMPORTANT: It is not possible to modify the CIFS server name of the virtual server with iManager. 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, use the *<Cluster IP address>* or *<Cluster Resource IP address>* in place of the server IP.
+ Server name: USERSVR
+ NetBIOS server name: USERSVR_W

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

The line you add to the hosts file is:

```
10.10.1.1 USERSVR_W
```

The string length of the NetBIOS name should not exceed 15 characters. The host name or the last 13 characters from the host name (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 (Optional) Select **Reconnect at Logon**.

5d Click **Finish**.

11.8.4 Temporary Files Created On The OES Server By MS Office 2010 Are Not Deleted

Cause: The **Enable for Editing** option is enabled in MS Office 2010.

Action: To ensure the temporary files are not stored in the server, disable the Enable for Editing option in MS Office 2010.

11.8.5 Users Created Using UID Qualifier Cannot Access CIFS Shares

Cause: The users are by default created with the `cn` qualifier. If you create a user with the `uid` qualifier, the user cannot access the CIFS shares.

Action: Ensure you create a user with the default `cn` qualifier.

12 Security Guidelines for CIFS

You can use several protection mechanisms to counteract potential security vulnerabilities for CIFS on Open Enterprise Server (OES) 11 SP3.

- Section 12.1, "Using Credentials," on page 91
- Section 12.2, "Using CASA," on page 91
- Section 12.3, "Using VPN Connections," on page 91
- Section 12.4, "Using SMB Signing," on page 91
- Section 12.5, "Other Security Considerations," on page 91

12.1 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 a combination of alphanumeric characters, uppercase letters, lowercase letters, and adheres to the password policy restrictions.

12.2 Using CASA

We recommend that you select CASA as the Credential Storage Location during YaST configuration of CIFS.

12.3 Using VPN Connections

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

12.4 Using SMB Signing

For a secure connection, set the SMB signing option to **optional** in iManager. For details, see "Enabling and Disabling SMB Signing" on page 44.

12.5 Other Security Considerations

OES 11 SP3 provides Universal Password security. For details, see Security Considerations in the *Novell Password Management Administration Guide*.

13 Tuning the Parameters and Settings for a File Server Stack

Following are the settings or parameters that can have an impact on the performance of the file server while accessing the data hosted on NSS volumes.

13.1 eDirectory

13.1.1 FLAIM Database

eDirectory uses FLAIM (Flexible Adaptable Information Manager) as its database. It is used for traditional, volatile, and complex information. It is a highly scalable database engine that supports multiple readers and a single-writer concurrency model.

Physically, FLAIM organizes data in blocks. Some of the blocks are typically held in memory and they represent the block cache. The entry cache, at times called a record cache, caches logical entries from the database. Entries are constructed from the items in the block cache. FLAIM maintains hash tables for both caches. The hash bucket size is periodically adjusted based on the number of items.

By default, eDirectory uses a block of 4 KB. The block cache size for caching the complete DIB is equal to the DIB size, and the size required for the entry cache is about two to four times the DIB size.

13.1.2 Thread Pool

eDirectory is multithreaded for performance reasons. In multithreading, when the system is busy, more threads are created to handle the load, and some threads are terminated to avoid extra overhead. Not every module uses the thread pool. The actual number of threads for the process is more than the number that exists in the thread pool. For example, FLAIM manages its background threads separately.

Use the `ndstrace -c threads` command to get the thread pool statistics.

Here's an example of a sample thread pool.

```
Summary      : Spawned 71, Died 24
Pool Workers : Idle 14, Total 47, Peak 52
Ready Work   : Current 1, Peak 12, maxWait 592363 us
Sched delay  : Min 23 us, Max 1004764 us, Avg: 5994 us
Waiting Work : Current 15, Peak 20
```

Here are some thread pool parameters:

- `n4u.server.max-threads`: Maximum number of threads that can be available in the pool.
- `n4u.server.idle-threads`: Maximum number of idle threads that can be available in the pool.
- `n4u.server.start-threads`: Number of threads started.

Run the `ndsconfig get` and `ndsconfig set` commands to get and set the thread pool size respectively.

Usually the default settings work for around 3000 to 4000 user connections unless eDirectory is busy with some other background processing of maintenance events, like creating external references for a user object that is in a remote eDirectory replica. As a best practice, the servers that hold the eDirectory replicas should be reachable over fast links from the servers that host the CIFS server.

In eDirectory 8.8 SP7, the max threads has been increased from 128 to 256.

We recommend that you monitor the output of `ndstrace -c` to see how many threads are being used. If the total threads to `max-threads` value is constantly being reached, consider changing the max value to a higher number. The recommended limit is 512, but in some OES environments, we have it set to more than that as well.

For information on how to tune the FLAIM database and Thread pool for optimum eDirectory performance, see FLAIM Database and Thread Pool in the NetIQ eDirectory 8.8 SP8 Tuning Guide for UNIX* Platforms.

13.2 NSS

- Section 13.2.1, "IDCacheSize," on page 94
- Section 13.2.2, "Minimum Buffer Cache," on page 95
- Section 13.2.3, "Setting the Name Cache Size," on page 95

Execute the following commands at the nsscon console prompt. To start the nsscon console, do the following:

1 As a `root` user, open a terminal console.

2 At the console prompt, enter `nsscon`.

13.2.1 IDCacheSize

`nss /IDCacheSize=value`

This sets the maximum number of entries for NSS GUID to ID, and ID to GUID cache.

For example, `nss /IDCacheSize = 256000`

Default: 16384

Range: 16384 to 524288

Recommendation: The recommendation is to set the IDCacheSize to the corresponding number of users accessing the file system. For example, if the user home directories are around 4000, then the recommended IDCacheSize is 4000.

13.2.2 Minimum Buffer Cache

To set the Minimum Number of Cache Buffers to use for the kernel memory:

```
nss /MinBufferCacheSize=value
```

where value is the number of 4 KB buffers.

The default value is 30000. The maximum setting is the amount of memory in KB divided by 4 KB. For a 32-bit machine, the maximum setting is 250000 buffers.

13.2.3 Setting the Name Cache Size

The NSS Name Cache is responsible for caching the Name Tree information. This is the information that is read when you perform any kind of search by file or directory name. The Name Cache maps a name to a ZID (a unique file object ID). Directory listings do not do this as much as normal file opens that must resolve each name in the file path.

Use the **NameCacheSize** parameter to specify the amount of recently used Name Tree entries for files and directories that NSS caches. Each entry uses about 150 bytes of memory. Increasing the maximum number of Name Cache entries does not necessarily improve the performance for getting directory listing information. This happens because NSS looks up information about the file from a tree or structure outside of the name tree.

If you want to see how your name cache is performing, use the `nsscon /NameCacheStats` command in the shell prompt.

```
nsscon /NameCacheSize=<value>
```

If you are already inside the NSSCON console prompt, use `/NameCacheSize=<value>` or `nss /NameCacheSize=<value>`.

Specify the maximum number of recently used Name Tree entries for files and directories to cache. Name cache grows up to the specified limit. Unlike the file system cache, it does not take the maximum amount of memory allocated from the start.

Default: 100000

Range: 17 to 1000000

For more information on tuning NSS performance on Linux, see Tuning Cache Buffers for NSS and Configuring or Tuning Group I/O in the OES 11 SP2: NSS File System Administration Guide for Linux.

13.3 CIFS

13.3.1 Maximum Cached Subdirectories Per Volume

This controls the maximum number of folder entries that can be cached by the CIFS server for a volume in the directory cache. The default value is 102400.

Use the following command to the set the Maximum Cached Subdirectories Per Volume:

```
novcifs –k SDIRCACHE = <value for the Maximum Cached Subdirectories Per Volume>
```

13.3.2 Maximum Cached Files Per Subdirectory

This controls the maximum number of file entries that can be cached by the CIFS server for a given folder in the directory cache. The default value is 10240.

Use the following command to the set the Maximum Cached Files Per Subdirectory:

```
novcifs –k DIRCACHE = <value for the Maximum Cached Files Per Subdirectory>
```

13.3.3 Maximum Cached Files Per Volume

This controls the maximum number of file entries that can be cached by the CIFS server for a given volume in the directory cache. The default value is 256000.

Use the following command to the set the Maximum Cached Files Per Volume:

```
novcifs –k FILECACHE = <value for the Maximum Cached Files Per Volume>
```

NOTE: The filecache size determines how many files or folders can be opened at a time. However, the total number of files and folders residing in a volume might be substantially lager than this number. This setting caches only the file name and related information; it does not cache the whole file.

Recommendation: Set this value close to the number of files and folders available in a volume.

13.3.4 Subtree Search

A subtree search or contextless login enables CIFS to search for a user in the entire base context of a tree. The subtree search setting that is saved in the `cifs.conf` file stays persistent even if the system or service is restarted.

To use the subtree search feature, the CIFS proxy user should have read rights for the base context. These rights are assigned automatically from iManager when the context is added. A subtree search can be configured only at a physical server or at node level. In a cluster setup, each node should be configured with the same configuration level for consistent behavior.

Use the following command to enable or disable subtree search:

```
novcifs -y yes|no
```

Subtree search performance depends on the distribution of eDirectory replicas in the tree, rather than on the actual hierarchy of eDirectory contexts.

13.3.5 Information and Debug Logs

Please keep the CIFS information and debug logs in a disabled state unless you specifically require the detailed log information.

To enable or disable the Debug Log for Developers, use the following command: `novcifs [-b yes|no | --enable-debug=yes|no]`

To enable or disable the Info Log, use the following command: `novcifs [-f yes|no |--enable-info=yes|no]`

13.3.6 Oplocks

The Oplocks or opportunistic locking improves file access performance by caching files at the client side. This option is enabled by default.

Recommendation: For better performance, oplocks should be enabled (use iManager).

13.3.7 Cross Protocol Locks

The CrossProtocol locks help in using the files in the right way from different clients depending on the type of file accessed. This option is enabled by default.

Recommendation: Option should be enabled for data integrity purposes.

13.3.8 SMB Signing

SMB signing ensures data integrity. This option is disabled by default in the latest CIFS release. This is because both the client and server are in a trusted corporate network and because the disabled state provides optimal file server performance. SMB signing should be turned off when domain authentication is configured.

Recommendation: Option is disabled by default.

`novcifs –g yes / no / optional / force`

For more information on CIFS parameters that affect the file system performance, see Locks Management for CIFS, Enabling Offline Files Support and Directory Cache Management for CIFS Server in the OES 11 SP2: Novell CIFS for Linux Administration Guide.

13.4 NCP

13.4.1 Thread Pools

To manage the thread pools in NCP, see Managing NCP Threads in the OES 11 SP2: NCP Server for Linux Administration Guide.

Tuning the number of asynchronous threads in NCP will help to route the NCP requests to eDirectory.

13.4.2 Cache Settings

To set the directory cache values in NCP, see Directory Cache Management for NCP Server in the OES 11 SP2: NCP Server for Linux Administration Guide.

A Command Line Utility for CIFS

This section describes the command line utilities for running CIFS services on an Open Enterprise Server (OES) 11 SP3 server.

To access a man page with the command information, enter `man novcifs` at the command prompt. To run this command, log in as root.

novcifs(8)

Name

novcifs - A command line utility that communicates with the `cifsd` daemon. You must be logged in as `root` to use novcifs.

Syntax

```
novcifs [options]
```

```
[-sl, --share --list]
```

```
[-sln SHARENAME, --share --list --name=SHARENAME]
```

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

```
[-srn SHARENAME, --share --remove --name=SHARENAME]
```

```
[-sap PATH -n SHARENAME -m CONNECTION-LIMIT -c COMMENT -v VIRTUALSERVERFDN, --share
--add --path=PATH --name=SHARENAME --conn-limit=CONNECTION-LIMIT --comment=COMMENT
--vserver=VIRTUALSERVERFDN]
```

```
[-srn SHARENAME -v VIRTUALSERVERFDN, --share --remove --name=SHARENAME --
vserver=VIRTUALSERVERFDN]
```

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

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

```
[-e yes|no, --guest-login=yes|no]
```

```
[-a -D DNSNAME -I IPADDR, --add --dns-name=DNSNAME --ip-addr=IPADDR]
```

```
[-r -D DNSNAME -I IPADDR, --remove --dns-name=DNSNAME --ip-addr=IPADDR]
```

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

```
[-e yes|no, --add --dns-name=DNS_NAME --ip-addr=IP_ADDR]
```

```
[-C | --Conn]
```

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

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

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

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

```
[-L 0|4|5, --lm=0|4|5]
```

```
[-y [yes|no]]
```

```
[-k [SDIRCACHE | DIRCACHE | FILECACHE] = value, --set-cache SDIRCACHE | DIRCACHE |
FILECACHE = value]]
```

```
[-t [yes|no]]
```

```
[-S yes|no]

[--enable-range-lock-mask=yes|no]

[--csc= 0|1|2|3]

[-UT TIMEOUT-PERIOD, --block-invalid-users --timeout-period=TIMEOUT-PERIOD]

[-Uan USER-NAME, --block-invalid-users --add --name=USER-NAME]

[-Urn USER-NAME, --block-invalid-users --remove --name=USER-NAME]

[-Ul, --block-invalid-users --list]

[--dynamic-fid-pool=yes|no]

[-d fh, --dump-statistics=fh]

[-d fp, --dump-statistics=fp]

[-d dc, --dump-statistics=dc]

[-Rp FILE-PATH, --rights --path=FILE-PATH]

[--resync=VOLUME-NAME]

[--vol-stats=VOLUME-NAME]

[--info-level-passthru=yes|no]

[--list-servers]

[--share-vols-default=SERVER_NAME --value=yes|no]

[--oplock-break-ack-timeout=<time in seconds>]

[--dfs-support=yes|no]
```

Options

Displaying the List of Share Points

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

Lists all the available share points.

Displaying Details of a Share Point

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

Displays details of a specific share point.

Adding a New Share Point on a Non-Clustered Volume (Login to the node as root)

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

Adds a new share point.

Example:

```
novcifs -sap CIFSV:/home/user1 -n user1home -m 0 -c "User1 home directory"
```

```
novcifs -sap CIFSV: -n volumeshare -m 0 -c "Volume share"
```

Removing a Share Point on a Non-Clustered Volume (Login to the node as root)

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

Removes an existing share point.

Example:

```
novcifs -srn user1home
```

Adding a New Share Point on a Clustered Volume (Login to the node hosting resource as root)

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

Adds a new share point on a clustered volume.

Example:

Assuming the resource name of the clustered volume SHAREDV is
.cn=PROJECT.ou=CL1.ou=Service.o=CT.t=NOVELL

```
novcifs -sap SHAREDV:/home/user1 -n user1home -m 0 -c User1 home directory -v
PROJECTS.CL1.Service.CT.NOVELL
```

Removing a Share Point on a Clustered Volume

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

Removes an existing share point.

Example:

```
novcifs -srn user1home -v PROJECT.CL1.Service.CT.NOVELL
```

Enabling or Disabling the Debug Log

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

Enables or disables the debug log.

Enabling or Disabling the Info Log

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

Enable this option to log all informative messages from the CIFS server.

Enabling or Disabling Anonymous (guest) Login

```
novcifs [-e yes|no | --guest-login=yes|no]
```

Enables or disables guest user login.

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

```
novcifs [-a -D DNSNAME -I IPADDR | --add --dns-name=DNSNAME --ip-addr=IPADDR]
novcifs [-r -D DNSNAME -I IPADDR | --remove --dns-name=DNSNAME --ip-addr=IPADDR]
```

This option associates DNS names with cluster resource IP address in the CIFS server. You can assign more than one DNS name to the same cluster resource and access it using the CIFS client.

Displaying Active Connection Count

```
novcifs [-C | --Conn]
```

Displays the number of active connections.

Adding a Virtual Server

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

Adds a virtual server to CIFS.

Removing a Virtual Server

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

Removes a virtual server from CIFS.

Displaying Operational Parameters

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

This option displays the current settings of the CIFS server.

Enabling or Disabling SMB Signing

```
novcifs [-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.

Setting LMCompatibilityLevel

```
novcifs [-L 0|4|5| --lm=0|4|5]
```

This option sets the LAN Manager authentication level.

0 for Accept LM and NTLM responses.
4 for Accept NTLM response/refuse LM response.
5 for Accept NTLMv2 response/refuse LM and NTLM responses.

Enabling or Disabling Subtree Search Capability

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

Enables CIFS to search for the user in the entire base context.

Changing the Cache Settings

```
novcifs -k [SDIRCACHE | DIRCACHE | FILECACHE] = value | --set-cache SDIRCACHE |
DIRCACHE | FILECACHE = value]
```

Changes the cache value. The following are the default cache values:

Maximum cached subdirectories per volume (SDIRCACHE)=102400
Maximum cached files per subdirectory (DIRCACHE)=10240
Maximum cached files per volume (FILECACHE)=256000

Enabling or Disabling Auditing

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

Enables or disables auditing.

IMPORTANT: Ensure that the `novell-vigil` service is running before you enable this option.

Enabling or Disabling File Synchronization

```
novcifs [-S yes|no | --sync=yes|no]
```

Enables or disables file synchronization. This parameter ensures that all the data previously written to a CIFS share has been written to the disk.

Enabling or Disabling Mask Behavior for Range Locks

```
novcifs [--enable-range-lock-mask=yes|no]
```

Enables or disables range lock masking behavior.

IMPORTANT: If you enable or disable this parameter, make sure you restart the CIFS server using the `rcnovell-cifs restart` command in order for the changes to take effect.

By default, range lock masking is enabled.

Enabling or Disabling Client-side Caching

```
novcifs [--csc= 0|1|2|3]
```

Enables or disables client-side caching feature, which can be used to store frequently used information on the client's machine.

0 Caches files for offline use. Does not permit automatic file-by-file reintegration.
1 Caches files for offline use. Permits automatic file-by-file reintegration.
2 Caches files for offline use. Clients are permitted to work from their local cache even while online.
3 Disables offline caching.

By default, client-side caching is disabled.

Enabling Invalid User Caching

CIFS is now able to cache the invalid user logins for a specific timeout period. Further authentication requests from the same user name will be ignored based on the configured timeout period.

```
novcifs [-UT TIMEOUT-PERIOD | --block-invalid-users --timeout-period=TIMEOUT-
PERIOD]
```

Specifies the amount of time a user should be considered as invalid to ignore authentication requests. Specify the timeout period in minutes. The range should be between 0 and 525600.

```
novcifs [-Uan USER-NAME | --block-invalid-users --add --name=USER-NAME]
```

Adds the specified user to the list of default invalid users whose authentication requests need to be ignored permanently.

```
novcifs [-Urn USER-NAME | --block-invalid-users --remove --name=USER-NAME]
```

Removes the specified user from the list of cached invalid users to start considering authentication requests.

```
novcifs [-Ul | --block-invalid-users --list]
```

Lists all the cached invalid users whose authentication requests are currently ignored.

Enabling CIFS File Id Pool

Enables CIFS to increase the file id pool from 65k to 600k. By default, this option is disabled.

```
novcifs [--dynamic-fid-pool=yes|no]
```

Dumping File Handle Statistics

Dumps statistics of Linux file handles opened.

```
novcifs [-d fh | --dump-statistics=fh]
```

Dumps statistics of Linux file handles and CIFS protocol file Ids opened.

```
novcifs [-d fp | --dump-statistics=fp]
```

Dumping Directory Cache Statistics

Dumps cache statistics used to store file and directory names.

```
novcifs [-d dc | --dump-statistics=dc]
```

Viewing the Trustees Associated with a File or Folder

Displays the list of trustees associated with the specified file or folder as per the CIFS cache record.

```
novcifs [-Rp FILE-PATH | --rights --path=FILE-PATH]
```

Synchronizing the Trustee List for a Volume

Imports the trustee information from the `trustee_database.xml` file associated with the specified volume into the CIFS cache.

```
novcifs [--resync=VOLUME-NAME]
```

Viewing Statistics of Trustees for a Volume

Displays the count of new, modified, and removed trustees for the specified volume. Run this command after synchronizing the trustee list.

```
novcifs [--vol-stats=VOLUME-NAME]
```

CIFS Monitoring and Management

With the file monitoring options you can view details of open files and close open files within a volume, by connection and file handles associated with a file. For more information, see Chapter 3, "CIFS Monitoring and Management," on page 17.

Enabling or Disabling the Pass-through Information Levels Capability

Enables or disables the pass-through information levels capability on the server.

The option is disabled by default. Enabling this option can cause differences in client behavior. Restart the CIFS server any time you modify this option.

```
novcifs [--info-level-passthru=yes|no]
```

How does enabling this option impact the client behavior?

The pass-through information levels capability exposes additional information levels as part of the CIFS protocol.

When the capability is enabled, Windows 7 starts using the new information levels - sends different verbs. No visible end user impact.

When should you enable it?

You want to do a multi-select and copy of large files from Finder on Mac clients to OES servers. The sequence of calls Finder performs for this operation causes problems if the pass through capability is not enabled.

Enabling this option also improves Web download experience to a CIFS Share on Mac Clients.

How do the users see their current quota on the client?

Passthru Info Levels Capability disabled: The Total, Used, and Free spaces displayed by the client will be the total Volume quota. It does not consider User and Directory quotas set.

For example, set 1 TB as Volume quota, 1 GB as User quota, and 100 GB as Directory quota. The disk usage (Total space, Used space, and Free space) visible to the user is 1 TB (Volume quota).

Passthru Info Levels Capability enabled: The Total, Used, and Free spaces displayed by the client is limited to Volume quota and User quota. It does not consider Directory quota set.

For example, set 1 TB as Volume quota, 1 GB as User quota, and 100 GB as Directory quota. The Free space and Total space visible to the user is limited to 1 GB [minimum of User and Volume quotas], and the Used space displayed will be the effective used space, which is less than or equal to 1 GB.

Passthru Info Levels Capability enabled (Mac clients): The Total, Used, and Free spaces displayed by the client will be the total Volume quota. It does not consider User and Directory quotas set.

For example, set 1 TB as Volume quota, 1 GB as User quota, and 100 GB as Directory quota. The disk usage (Total space, Used space, and Free space) visible to the user is 1 TB (Volume Quota).

Viewing the NetBIOS Names of Servers and Changing the Behavior of Exporting Volumes by Default

In releases earlier than OES 11 SP2, all mounted NSS volumes are exported as shares by default when the CIFS service is started. The name of the share is the same as the corresponding volume name. If a user removes a default share using the `novcifs` command or iManager, it will once again be exported as a share if the CIFS service is restarted.

In OES 11 SP2 and later, this behavior can be modified by setting the value of the nfapCIFSShareVolsByDefault attribute of the NCP server object to false. This prevents any default shares that were removed from being shared again if the server is restarted or if the resource is migrated. This setting can be modified using the `novcifs` command.

The setting to control whether volumes are shared by default is specific to each physical and virtual CIFS server. Different physical and virtual servers running on an OES host can behave differently in terms of how they share volumes by default, depending on the value of the setting for each server.

With the new command option introduced in `novcifs`, the administrator can choose to export all mounted volumes as shares, or export only the specified volumes as shares.

```
novcifs [--list-servers]
```

Lists the NetBIOS name and whether all NSS volumes are exported as shares by default for each CIFS server on this system. Returns an entry for each physical and virtual server running on this system.

```
novcifs [--share-vols-default=SERVER_NAME --value=yes|no]
```

Enables or disables all volumes being exported as shares by default.

SERVER_NAME: The NetBIOS name of one of the CIFS servers returned by the `--list-servers` command.

yes: Exports all the volumes belonging to <SERVER_NAME> as CIFS shares.

no: Exports only those shares specified by the CIFS administrator.

This option is enabled by default. When this option is disabled, no new volumes mounted will be shared; however, volumes that are already exported as shares will remain as shares until they are manually removed by the administrator. When this option is enabled, any new volume mounted will be exported, and after the CIFS service is restarted all mounted volumes will be exported as shares.

Limitation: This feature does not work for virtual servers in a cluster environment where nodes earlier than OES 11 SP2 exist.

Examples:

Viewing the list of physical and virtual CIFS servers and the "Share volumes by default" option for each server.

```
novcifs --list-servers
List of CIFS servers:
--------------------
LINUX-100-1_W   -  "Share volumes by default" attribute is enabled
R1-CLUSPOOL1-W  -  "Share volumes by default" attribute is disabled
```

Disabling the "Share volumes by default" option.

```
novcifs --share-vols-default=LINUX-100-1_W --value=no
Updating the Share Volumes By Default setting of the server completed successfully.
```

Enabling the "Share volumes by default" option.

```
novcifs --share-vols-default=R1-CLUSPOOL1-W --value=yes
Updating the Share Volumes By Default setting of the server completed successfully.
```

Setting Oplock Break Acknowledgment Timeout Period

Specifies the amount of time in seconds the CIFS server waits for the client's response after sending a request to the client to release oplock on a file.

Default: 30 seconds. Minimum: 5 seconds. Maximum: 30 seconds.

```
--oplock-break-ack-timeout=<time in seconds>
```

Enabling or Disabling DFS Support

Enables or disables DFS support for the CIFS server. By default, this option is disabled.

```
--dfs-support=yes|no
```

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/log/cifs/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.

B Comparing Novell CIFS and Novell Samba

This section compares features and capabilities of Novell CIFS and Novell Samba on Open Enterprise Server 11 SP3 servers.

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

Parameter	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.
Client-side Caching	Yes. Configurable at server-level.	Configurable at share-level.
DST	Yes	No
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 or the NSSMU utility to create an NSS volume on an OES11 SP3 server. For instructions on how to setup an NSS volume, see the *OES 11 SP3: File Systems Management Guide*.
LUM and Samba enablement	LUM enablement is not required.	Users must be enabled for LUM and Samba and assigned to a Samba group.
NetBIOS support	Yes. SMB over NetBIOS (139).	SMB over Netbios (139) and SMB over TCP/IP (445).
Novell Trustee Rights	Yes	No
Scalability	Higher when compared with Samba.	Lower when compared with CIFS.
Subtree Search	Yes	No

C Comparing CIFS on NetWare and CIFS on OES 11 SP3

This section compares features and capabilities of Novell CIFS on NetWare and Novell Open Enterprise Server 11 SP3 servers.

Table C-1 *CIFS services on NetWare and OES 11 SP3*

Service	NetWare	OES 11 SP3
64-Bit Support	No	Yes
NSS Support	Yes	Yes
Distributed File Services	Yes	Yes
OpLocks	Yes	Yes
Cross Protocol Locking	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	Yes
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	No	Yes
Dynamic Storage Technology Support	No	Yes
LDAP User (Subtree) Search	No	Yes

D Configuration and Log Files

Table D-1 *CIFS Configuration Files*

Path	Description
/etc/opt/novell/cifs/cifs.conf	CIFS server
/etc/opt/novell/cifs/cifsctxs.conf	List of eDirectory contexts having CIFS users
/etc/opt/novell/cifs/cifslogrotate	Initiates the rotation using the `cifslogrotate.conf` file
/etc/opt/novell/cifs/cifslogrotate.conf	Hourly rotation of CIFS log file
/etc/opt/novell/cifs/logrotate.d/novell-cifs-hourly	Customized hourly rotation of CIFS log file
/opt/novell/cifs/share/nmasmthd/ntlm/config.txt	Used by installation of CIFS NMAS method into eDirectory tree

Table D-2 *CIFS Log Files*

Path	Description
/var/log/cifs/cifs.log	CIFS server run-time
/var/opt/novell/log/cifs.log	Soft link to /var/log/cifs/cifs.log

With the CIFS logrotate function, you can now administer your log files on an hourly basis. The cron job checks the size of the log file on a hourly basis to see if it exceeds the predefined quota. If the quota is crossed, the existing file is rotated and logging information is written to a new file.

This operation continues until there are 10 cifslog files. When the last cifslog file reaches the predefined quota, the first log file is rotated.

To implement this feature, copy the `cifslogrotate` file to `/etc/cron.hourly/` and remove the `/etc/logrotate.d/` `novell-cifs` configuration file.

E   Documentation Updates

This section contains information about documentation content changes made to the *Novell CIFS Administration Guide* since the initial release of Novell Open Enterprise Server 11 SP1.

This document was updated on the following dates:

E.1   July 2016

Update was made to the following section. The changes are explained below.

Location	Change
Section 2.1, "What's New (OES11 SP3)," on page 13	This section is new.

E.2   May 2016

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

Location	Change
Section 2.2, "What's New (OES11 SP2 May 2016 Patches)," on page 13	This section is new.

E.3   May 2014

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

Location	Change
Section 2.3, "What's New (OES11 SP2 May 2014 Patches)," on page 13	This section is new.

E.4 January 2014

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

Location	Change
Section 2.4, "What's New (OES 11 SP1 January 2014 Patches)," on page 13	This section is new.
Section 2.5, "What's New (OES 11 SP2)," on page 14	This section is new.
"Enabling or Disabling the Pass-through Information Levels Capability" on page 106	This section is new.
"Viewing the NetBIOS Names of Servers and Changing the Behavior of Exporting Volumes by Default" on page 107	This section is new.
Chapter 3, "CIFS Monitoring and Management," on page 17	This chapter is new.
Section 4.2.2, "Required eDirectory Rights and Permissions," on page 22	This section is new.
Chapter 11, "Troubleshooting CIFS," on page 81	Reworded and reorganized this chapter.
Section 9.3.3, "Example for CIFS Cluster Rights," on page 72	Reworked and moved this section from Chapter 4, "Planning and Implementing CIFS," on page 21.
Section 11.8.1, "Offline Files Synchronization Fails," on page 87	This section is new.
Section 11.8.2, "Synchronization of Offline Files Caching fails with the error "The process cannot access the file because it is being used by another process."," on page 87	This section is new.
Section 11.1.3, "File Level Trustees Are Deleted When a File is Modified," on page 82	This section is new.
Section 5.1, "Installing CIFS during the OES 11 SP3 Installation," on page 27	This section is new.

E.5 April 2013 (OES 11 SP1)

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

Location	Change
"Viewing the Trustees Associated with a File or Folder" on page 105	This section is new.
"Synchronizing the Trustee List for a Volume" on page 105	This section is new.
"Viewing Statistics of Trustees for a Volume" on page 106	This section is new.

E.6 November 2012 (OES 11 SP1)

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

Location	Change
"Enabling CIFS File Id Pool" on page 105	This section is new.
"Dumping File Handle Statistics" on page 105	This section is new.
"Dumping Directory Cache Statistics" on page 105	This section is new.

E.7 September 2012 (OES 11 SP1)

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

Location	Change
"Enabling Invalid User Caching" on page 105	This section is new.

E.8 April 2012 (OES 11 SP1)

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

Location	Change
Chapter 2, "What's New or Changed in Novell CIFS," on page 13	This section is new.