opentext™

Open Enterprise Server 24.4

OES CIFS Administration Guide

January 2025

Legal Notices

Copyright 2022 - 2025 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 9

1 Overview of CIFS 11

1.1 Understanding CIFS . . . 11
1.2 CIFS and Universal Password . . . 12
1.3 CIFS Features and Capabilities . . . 12
1.4 Limitations . . . 14
1.5 What's Next . . . 14

2 What's New or Changed in CIFS 15

2.1 What's New or Changed in OES CIFS (OES 25.1) . . . 15
2.2 What's New or Changed in OES CIFS (OES 24.4) . . . 15
2.2.1 OES MFA on CIFS service . . . 15

3 Planning and Implementing CIFS 17

3.1 Planning for CIFS . . . 17
3.2 Preparing for CIFS Installation . . . 17
3.2.1 Prerequisites . . . 17
3.2.2 Required eDirectory Rights and Permissions . . . 18
3.3 CIFS System Prerequisites . . . 20
3.3.1 Server Hardware Requirements . . . 20
3.3.2 Client Operating System Requirements . . . 20
3.3.3 CIFS Prerequisite Checklist . . . 20
3.4 Co-existence Issues . . . 21
3.5 Planning for SMB Changes in OES 2018 and later . . . 21
3.6 What's Next . . . 23

4 Installing and Setting Up CIFS 25

4.1 Installing CIFS during the OES Installation . . . 25
4.2 Installing CIFS after the OES Installation . . . 27
4.3 Installing NMAS . . . 28
4.4 Verifying the Installation . . . 29
4.4.1 Verifying Files and Folders . . . 29
4.4.2 Verifying the File Configuration Information . . . 31
4.4.3 Verifying LSM Installation . . . 31
4.5 Installing the CIFS iManager Plug-In . . . 31
4.6 Installing Avahi After OES Installation . . . 31
4.7 What's Next . . . 32

5 Administering the CIFS Server 33

5.1 Using iManager to Manage CIFS . . . 33

5.1.1 Prerequisites . . . 34
5.1.2 Selecting a Server to Manage . . . 34
5.1.3 Setting the CIFS Server and Authentication Properties . . . 35
5.1.4 Managing CIFS Shares . . . 39
5.1.5 Configuring a CIFS User Context . . . 41
5.1.6 Stopping CIFS . . . 41
5.2 Using the Command Line to Manage CIFS . . . 41
5.2.1 Starting CIFS . . . 42
5.2.2 Stopping CIFS . . . 42
5.2.3 Restarting CIFS . . . 42
5.2.4 Monitoring CIFS . . . 42
5.2.5 Modifying the CIFS Configuration . . . 42
5.2.6 Anonymous Login for CIFS . . . 43
5.2.7 Working with CIFS Shares . . . 44
5.2.8 Configuring the CIFS Context Search File . . . 44
5.3 Apple Time Machine Backups to NSS Volumes . . . 44
5.4 Multi-Factor Authentication for CIFS Service . . . 45
5.4.1 Configure CIFS to Enforce MFA for Drive Mapping . . . 45
5.5 Locks Management for CIFS . . . 46
5.6 Third-Party Domain Authentication . . . 47
5.6.1 Prerequisites . . . 47
5.6.2 Using iManager to Enable Third-Party Authentication . . . 49
5.7 Roaming User Profile . . . 49
5.7.1 Configuration Required on OES Server for Roaming Profiles . . . 50
5.8 Dynamic Storage Technology for CIFS Server . . . 51
5.9 DFS Junction Support in CIFS Linux . . . 52
5.9.1 Prerequisites . . . 52
5.9.2 Enabling DFS Support . . . 52
5.9.3 Limitations . . . 53
5.10 Subtree Search . . . 53
5.10.1 Prerequisites . . . 53
5.10.2 Enabling a Subtree Search . . . 53
5.10.3 Subtree Search in a Cluster Setup . . . 53
5.11 Enabling Offline Files Support . . . 54
5.12 Enabling Folder Redirection Support . . . 54
5.13 Directory Cache Management for CIFS Server . . . 55
5.14 Server-side Copy Feature . . . 56
5.15 What's Next . . . 56

6 CIFS Monitoring and Management 57

6.1 Overview of CIFS Monitoring and Management . . . 57
6.2 Using CIFS Monitoring and Management . . . 57
6.3 Monitoring Connections . . . 57
6.3.1 Access Modes . . . 58
6.4 Monitoring Files . . . 58

7 Migrating CIFS to OES 61

8 Running CIFS in a Virtualized Environment 63

8.1 What's Next . . . 63

9 Configuring CIFS with Cluster Services for an NSS File System 65

9.1 Benefits of Configuring CIFS for High Availability . . . 65
9.2 Cluster Terminology . . . 65
9.3 CIFS and Cluster Services . . . 66
9.3.1 Prerequisites . . . 66
9.3.2 Using CIFS in a Cluster Environment . . . 67
9.3.3 Example for CIFS Cluster Rights . . . 69
9.4 Configuring CIFS in a Cluster . . . 71
9.4.1 Prerequisites . . . 71
9.4.2 Creating Shared Pools and Accessing Sharepoints . . . 71
9.5 What's Next . . . 72

10 Working with Client Computers 73

10.1 Accessing Files from a Client Computer . . . 73
10.1.1 Accessing Files from a Windows Client . . . 73
10.1.2 Accessing Files from a Linux Desktop . . . 74
10.2 Mapping Drives and Mounting Volumes . . . 75
10.2.1 Mapping Drives from a Windows Client . . . 75
10.2.2 Mounting Volumes from a Linux Client . . . 75
10.3 Using OES File Access Rights Management (NFARM) . . . 75
10.3.1 Salvage and Purge on Windows . . . 76
10.3.2 Salvage and Purge on Mac . . . 80
10.3.3 Password Expiry Notification on Windows . . . 82
10.3.4 Managing Access Rights and Quotas for AD Entities . . . 84

11 Troubleshooting CIFS 85

11.1 Known issues . . . 85
11.1.1 Deleting a Directory Having a Large Number of Files is Taking Too Long On a Windows 10 Client . . . 86
11.1.2 CIFS Does Not Come Up After Upgrading to OES 2018 or Later if Service Proxy is Configured . . . 86
11.1.3 Interruption in access to the CIFS shares from Windows clients upon change of server dialect from SMB2 or later to SMB or upon cluster resource migration . . . 86
11.1.4 Windows Explorer Hangs On Accessing the CIFS Share Path . . . 87
11.1.5 Salvaged Files are not Displayed in Windows 7 Enterprise Client . . . 87
11.1.6 Automatic Synchronization of Offline Files . . . 87
11.1.7 Members Of The Default ad-supervisor-group "Domain Admins" Can Map AD-enabled NSS Volumes Although Their Effective Rights on Those Volumes Is Displayed As NULL . . . 87
11.1.8 Users Are Not Able to Map NSS Resources . . . 88
11.1.9 CIFS Fails to Write Core Dumps . . . 89
11.1.10 CIFS Users Unable to Authenticate to OES Server if the Tree has Netware server as the eDirectory Replica Holding Server . . . 90
11.1.11 Windows Clients Do Not Reflect The Latest File/Folder Operations . . . 90
11.1.12 Different Tree Migration Is Not Available in the Migration Tool . . . 90
11.1.13 File Level Trustees Are Deleted When a File is Modified . . . 90
11.2 CIFS Installation and Configuration . . . 91
11.2.1 CIFS Does Not Start After Installation . . . 91
11.2.2 CIFS Terminates With Schema Not Extended Error After Installation . . . 91
11.3 Authentication . . . 91

11.3.1 Configuring AD Server to Support Kerberos Authentication for External Forest Users Using CIFS Client . . . 91
11.3.2 Disabling Kerberos Authentication While the OES Server is being Upgraded to OES 2018 or Later . . . 92
11.3.3 CIFS User Authentication Fails On an NTLMv2 enabled Windows XP Client in the First Attempt . . . 94
11.3.4 Password Has Expired . . . 94
11.3.5 User Can Only See Folders Assigned With Public Trustee Rights . . . 95
11.3.6 Authentication Failed Due to Password Mismatch . . . 95
11.4 Startup . . . 95
11.4.1 CIFS Is Not Starting . . . 95
11.5 Migration . . . 96
11.5.1 CIFS Does Not Start After Migration Is Completed On The Target server . . . 96
11.5.2 After Migration, the CIFS Server Does Not Come up on the Target Server by Default . . . 96
11.6 Mac Client . . . 96
11.6.1 Unable to See the Contents of the Target That a DFS Junction Points To . . . 96
11.6.2 The Mac Client does not Display a Complete List of Available Shares . . . 97
11.6.3 Copying Multiple Large Files using Finder from a Mac OS X Client to an OES CIFS Share Fails . . . 97
11.7 DFS . . . 97
11.7.1 Unable to Resolve DFS junctions from Windows Clients . . . 97
11.7.2 Junction Target Changes Require DFSUTIL Command Execution to Clear the Cache . . . 98
11.7.3 Unable To Access DFS Junctions On a CIFS Share From the Windows Client . . . 98
11.7.4 After Modifying the Junction Target, Accessing the Junction Still Leads to the Old Target . . . 98
11.8 Miscellaneous . . . 98
11.8.1 Files Deleted from Redirected Folder are Not Available in NFARM Salvage Purge List on Windows Clients . . . 99
11.8.2 After Successful Folder Redirection, Multiple Login or Logout Requests Observed in Log File . . . 99
11.8.3 Executing --join or --leave-domain in novell-ad-util Fails with an Error “Insufficient rights to do the operation, perform kinit.” . . . 99
11.8.4 Not Able to Change Authentication Mode in iManager . . . 100
11.8.5 Offline Files Synchronization Fails . . . 100
11.8.6 Synchronization of Offline Files Caching Fails with an Error “The process cannot access the file because it is being used by another process.” . . . 100
11.8.7 Windows or Mac Unable to Resolve the NetBIOS Name of the CIFS Server . . . 100
11.8.8 Temporary Files Created On the OES Server By MS Office 2010 Are Not Deleted . . . 102
11.8.9 Users Created Using UID Qualifier Cannot Access CIFS Shares . . . 102
11.8.10 Troubleshooting NIT . . . 102

12 Security Guidelines for CIFS 105

12.1 Using Credentials . . . 105
12.2 Using OES Credential Store . . . 105
12.3 Using VPN Connections . . . 105
12.4 Using SMB Signing . . . 105
12.5 Other Security Considerations . . . 105

13 Tuning the Parameters and Settings for a File Server Stack 107

13.1 eDirectory . . . 107
13.1.1 FLAIM Database . . . 107
13.1.2 Thread Pool . . . 107

13.2 NSS 108
13.2.1 IDCacheSize 108
13.2.2 Minimum Buffer Cache 109
13.2.3 Setting the Name Cache Size 109
13.3 CIFS 110
13.3.1 Maximum Cached Subdirectories Per Volume 110
13.3.2 Maximum Cached Files Per Volume 110
13.3.3 Subtree Search 111
13.3.4 Information and Debug Logs 111
13.3.5 Oplocks 111
13.3.6 Leasing 111
13.3.7 Cross Protocol Locks 112
13.3.8 SMB Signing 112
13.3.9 Dynamic FID Pool 112
13.4 NCP 112
13.4.1 Thread Pools 112
13.4.2 Cache Settings 113

A Command Line Utility for CIFS 115

novcifs 116

B Comparing CIFS on NetWare and CIFS on OES 2018 or Later 133

C Configuration and Log Files 135

About This Guide

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

- Chapter 1, “Overview of CIFS,” on page 11
- Chapter 2, “What’s New or Changed in CIFS,” on page 15
- Chapter 3, “Planning and Implementing CIFS,” on page 17
- Chapter 4, “Installing and Setting Up CIFS,” on page 25
- Chapter 5, “Administering the CIFS Server,” on page 33
- Chapter 6, “CIFS Monitoring and Management,” on page 57
- Chapter 7, “Migrating CIFS to OES,” on page 61
- Chapter 8, “Running CIFS in a Virtualized Environment,” on page 63
- Chapter 9, “Configuring CIFS with Cluster Services for an NSS File System,” on page 65
- Chapter 10, “Working with Client Computers,” on page 73
- Chapter 11, “Troubleshooting CIFS,” on page 85
- Chapter 12, “Security Guidelines for CIFS,” on page 105
- Chapter 13, “Tuning the Parameters and Settings for a File Server Stack,” on page 107
- Appendix A, “Command Line Utility for CIFS,” on page 115
- Appendix B, “Comparing CIFS on NetWare and CIFS on OES 2018 or Later,” on page 133
- Appendix C, “Configuration and Log Files,” on page 135

Audience

This guide is intended for OES 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 `comment on this topic` 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 24.4 Documentation Web site.

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.

- Section 1.1, “Understanding CIFS,” on page 11
- Section 1.2, “CIFS and Universal Password,” on page 12
- Section 1.3, “CIFS Features and Capabilities,” on page 12
- Section 1.4, “Limitations,” on page 14
- Section 1.5, “What's Next,” on page 14

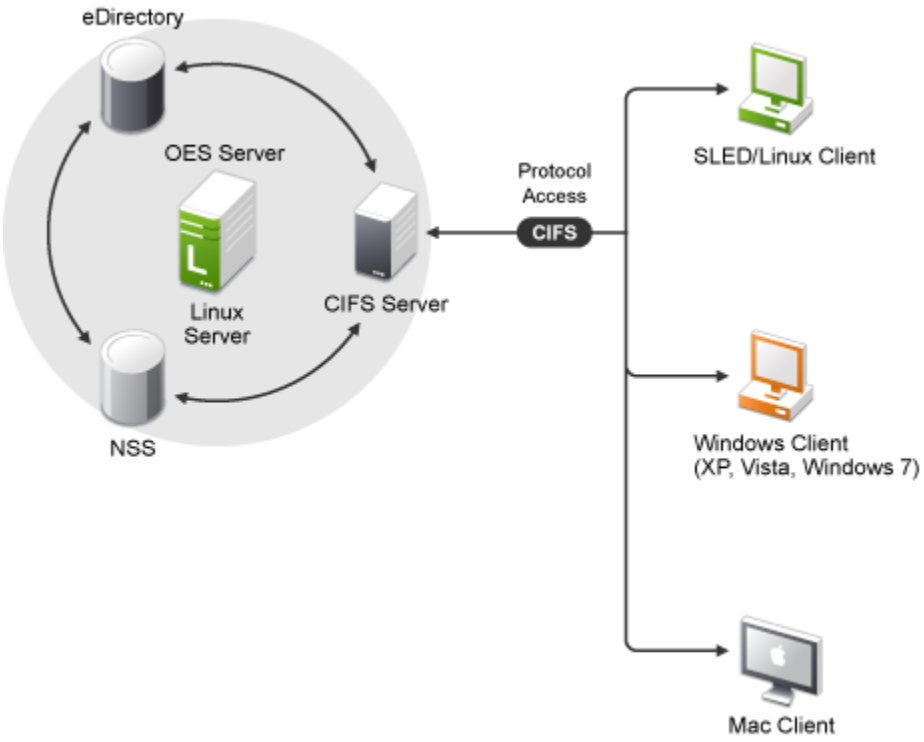
1.1 Understanding CIFS

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 either relies on NetBIOS over TCP (NBT) via 139 port or bypasses NetBIOS and directly use TCP via 445 port 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.

CIFS runs on the Open Enterprise Server (OES), uses NetIQ eDirectory services for eDirectory user authentication and kerberoes for AD user authentication. It 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 *CIFS Conceptual Overview*



CIFS enables any SMB clients like Windows, Linux, and Mac client work stations and not limited to these desktop clients only to create, copy, delete, move, save, and open files on an OES 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 eDirectory user in native and domain mode 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:

Table 1-1 *CIFS Feature List*

Feature	Description
Client Support	SUSE Linux Enterprise Server 12 SP5
	SUSE Linux Enterprise Server 15 SP4
	Windows 10
	Windows 11
	Windows Server 2019
	Windows Server 2022
	Macintosh OS X 11 (Big Sur)
	Macintosh OS X 12 (Monterey)
	Macintosh OS X 13 (Ventura)
	Macintosh OS X 14 (Sonoma)
	Macintosh OS X 15 (Sequoia)
Integration and Support for OpenText Technologies	Integration with NetIQ eDirectory.
	Integration with the Storage Services (NSS) file system.
	Support for DST shadow volume pair access. For more information, see Section 5.8, “Dynamic Storage Technology for CIFS Server,” on page 51.
	Support for DFS junctions. For more information, see Section 5.9, “DFS Junction Support in CIFS Linux,” on page 52.
Subtree Search (eDirectory users only)	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 5.10, “Subtree Search,” on page 53.
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 and NCP).
	This option ensures that a file is updated correctly before another user, application, or process can access it.
	For more information, see Section 5.5, “Locks Management for CIFS,” on page 46.
Universal Password (eDirectory users only)	Support for Universal Password. For more information, see Password Management Security Consideration.

Feature	Description
Authentication Modes	CIFS supports NMAS authentication method. Support for NTLMv1 and NTLMv2 authentication mode. For more information, see Table 5-2 on page 37. Support for Third-Party Authentication. Kerberos authentication for Active Directory users. Extended Security Support (NTLMSSP) for eDirectory Users.
File Access	Supports the OES Trustee Model for eDirectory and Active Directory users. For more information, see "OES Trustee Model" in the Storage Services File System (NSS) Administration Guide for Linux..
Client-side caching (Offline Files support)	Stores frequently used information on the client's machine. For more information, see Section 5.11, "Enabling Offline Files Support," on page 54.
High Availability	Supported by Cluster Services for high availability. For more information, see Chapter 9, "Configuring CIFS with Cluster Services for an NSS File System," on page 65.
Administration and Configuration	Performed through iManager (by eDirectory users only) and novcifs. For more information, see Section 5.1, "Using iManager to Manage CIFS," on page 33 and Appendix A, "Command Line Utility for CIFS," on page 115.
User Management	CIFS does not require Linux User Management (LUM) enabling.

1.4 Limitations

- Recursive Change notification is not supported.

1.5 What's Next

If you are planning to implement CIFS on your enterprise server, continue with Chapter 3, "Planning and Implementing CIFS," on page 17.

2 What's New or Changed in CIFS

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

- Section 2.1, "What's New or Changed in OES CIFS (OES 25.1)," on page 15
- Section 2.2, "What's New or Changed in OES CIFS (OES 24.4)," on page 15

2.1 What's New or Changed in OES CIFS (OES 25.1)

OES 25.1 is an update that includes features updates, enhancements, improves usability, and defect fixes.

2.2 What's New or Changed in OES CIFS (OES 24.4)

2.2.1 OES MFA on CIFS service

OES CIFS can be configured to use an OES MFA service to enforce multi-factor authentication when users access the CIFS share. MFA server service is supported on OES 24.4 or later versions.

3 Planning and Implementing CIFS

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

- Section 3.1, “Planning for CIFS,” on page 17
- Section 3.2, “Preparing for CIFS Installation,” on page 17
- Section 3.3, “CIFS System Prerequisites,” on page 20
- Section 3.4, “Co-existence Issues,” on page 21
- Section 3.5, “Planning for SMB Changes in OES 2018 and later,” on page 21
- Section 3.6, “What's Next,” on page 23

3.1 Planning for CIFS

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

- Upgrading from OES 2 SP3 Linux to OES 2018 or later on your enterprise servers. For details, see “Upgrading OES” in the *Installation Guide*.
- Migrating from NetWare to an OES 2018 or later setup. For details see, Chapter 7, “Migrating CIFS to OES,” on page 61.

3.2 Preparing for CIFS Installation

- Section 3.2.1, “Prerequisites,” on page 17
- Section 3.2.2, “Required eDirectory Rights and Permissions,” on page 18

3.2.1 Prerequisites

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

- ❒ CIFS users that exist in eDirectory 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.

- ❒ If you plan to set the dialect as SMB2, apply the hotfix as mentioned in Section 11.1.11, “Windows Clients Do Not Reflect The Latest File/Folder Operations,” on page 90.

  For more information about toggling between SMB versions, see “Toggling between SMB Versions” on page 125.

- ❒ Enable “Kerberos Forest Search Order (KFSO)” for SMB client connection in the Windows client where the user login. For more information, see Section 11.3.1, “Configuring AD Server to Support Kerberos Authentication for External Forest Users Using CIFS Client,” on page 91.
- ❒ Provide the complete DNS name of the OES CIFS server.

3.2.2 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.

3.3 CIFS System Prerequisites

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

- Section 3.3.1, “Server Hardware Requirements,” on page 20
- Section 3.3.2, “Client Operating System Requirements,” on page 20
- Section 3.3.3, “CIFS Prerequisite Checklist,” on page 20

3.3.1 Server Hardware Requirements

For details, see “Meeting All Server Software and Hardware Requirements” in the *Installation Guide*.

3.3.2 Client Operating System Requirements

- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 15 SP4
- Windows 10
- Windows 11
- Windows Server 2019
- Windows Server 2022
- Macintosh OS X 11 (Big Sur)
- Macintosh OS X 12 (Monterey)
- Macintosh OS X 13 (Ventura)
- Macintosh OS X 14 (Sonoma)
- Macintosh OS X 15 (Sequoia)

3.3.3 CIFS Prerequisite Checklist

Use the following checklist to verify CIFS dependencies before proceeding:

- ❒ CIFS supports only Storage Services (NSS) volumes.
- ❒ NCP should be up and running in order for CIFS to function properly.

3.4 Co-existence Issues

Do not install any of the following service combinations on the same server as OES CIFS. Although not all of the combinations cause pattern conflict warnings, the following SLES and OES patterns are not supported:

- ❒ SLES File Server Pattern
- ❒ OES patterns Domain Services for Windows (DSfW)
- ❒ Any other SMB implementation
- ❒ Xen Virtualization Host pattern

3.5 Planning for SMB Changes in OES 2018 and later

OES 2018 (and later) server and the SMB clients negotiate to determine the SMB dialect with the highest level of functionality that both the client and server support. However, SMB v3 (SMB 3.0) is the default protocol in OES 2018 and later.

If you set the protocol dialect SMB v2, the following configuration options will become invalid:

- LM Compatibility Level
- Unicode Support
- Info Level Pass-through capability

If you set the protocol dialect to SMB v1, CIFS server will not enforce File System change notification.

IMPORTANT: Domain pass-through authentication is supported for backward compatibility only. When authentication mode is changed/set to Third party authentication, Clients can connect only with NT LM 0.12 (CIFS/SMB v1) protocol version/dialect.

Table 3-1 *Client/SMB compatibility matrix*

Client Operating Systems	**OES 2018 SP3 Server**			
	NT LM 0.12 (SMB v1) over TCP 445	**SMB 2.002 (SMB v2) over TCP 445**	**NT LM 0.12 (SMB v1) over TCP 139**	**SMB 2.002 (SMB v2) over TCP 139**
Microsoft Windows 8.1	SMB v1	SMB v2	SMB v1	SMB v2
Microsoft Windows 10	SMB v1	SMB v2	SMB v1	SMB v2
Windows Server 2008	SMB v1	SMB v2	SMB v1	SMB v2
Windows Server 2012	SMB v1	SMB v2	SMB v1	SMB v2
Windows Server 2016	SMB v1	SMB v2	SMB v1	SMB v2
Macintosh OS X 10.12.x (Intel, 64-bit)	SMB v1	SMB v2	SMB v1	SMB v2

Client Operating Systems		OES 2018 SP3 Server			
		NT LM 0.12 (SMB v1) over TCP 445	**SMB 2.002 (SMB v2) over TCP 445**	**NT LM 0.12 (SMB v1) over TCP 139**	**SMB 2.002 (SMB v2) over TCP 139**
Macintosh OS X 10.13.x (Intel, 64-bit)		SMB v1	SMB v2	SMB v1	SMB v2
Macintosh OS X 10.14.x (Intel, 64-bit)		SMB v1	SMB v2	SMB v1	SMB v2
SUSE Linux Enterprise Desktop 11 SP3	`mount` Command	SMB v1	SMB v2	SMB v1	SMB v2
	File Browser	SMB v1	SMB v1 Through File browser, the client always negotiates over SMB v1 even when SMB v2 dialect is selected on the server side.	SMB v1	SMB v1 Through File browser, the client always negotiates over SMB v1 even when SMB v2 dialect is selected on the server side.
SUSE Linux Enterprise Desktop 12	`mount` Command	SMB v1	SMB v2	SMB v1	SMB v2
	File Browser	SMB v1	SMB v1 Through File browser, the client always negotiates over SMB v1 even when SMB v2 dialect is selected on the server side.	SMB v1	SMB v1 Through File browser, the client always negotiates over SMB v1 even when SMB v2 dialect is selected on the server side.

NOTE: Accessing OES shares through SMB V2 (SMB 2.002) from SLED clients might fail for Active Directory users. OpenText plans to fix this in a future release.

Table 3-2 *Client/Port support matrix*

	Connect		Reconnect		
Client Versions	**Default Port**	**Fall Back Port**	**Default Port**	**Fall Back Port**	**Remarks**
Windows 8	445	139	445	139	This is the standard/expected behavior on client side. Changes can be done on the client side to switch protocol and/or disable/enable certain port to use another port. For example Windows 8.1/10, if the client is modified to use SMB V1 then 139 port will work as well.
Windows 8.1	445	139	445	X	
Windows 10	445	139	445	X	
Windows Server 2008	445	139	445	X	
Windows Server 2012	445	139	445	X	
Windows Server 2016	445	139	445	X	
MAC 10.X	445	139	445	139	
SLED 12	445	139	445	139	

3.6 What's Next

To proceed with CIFS installation on an OES server, continue with Chapter 4, “Installing and Setting Up CIFS,” on page 25.

4 Installing and Setting Up CIFS

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

- Section 4.1, “Installing CIFS during the OES Installation,” on page 25
- Section 4.2, “Installing CIFS after the OES Installation,” on page 27
- Section 4.3, “Installing NMAS,” on page 28
- Section 4.4, “Verifying the Installation,” on page 29
- Section 4.5, “Installing the CIFS iManager Plug-In,” on page 31
- Section 4.6, “Installing Avahi After OES Installation,” on page 31
- Section 4.7, “What's Next,” on page 32

4.1 Installing CIFS during the OES Installation

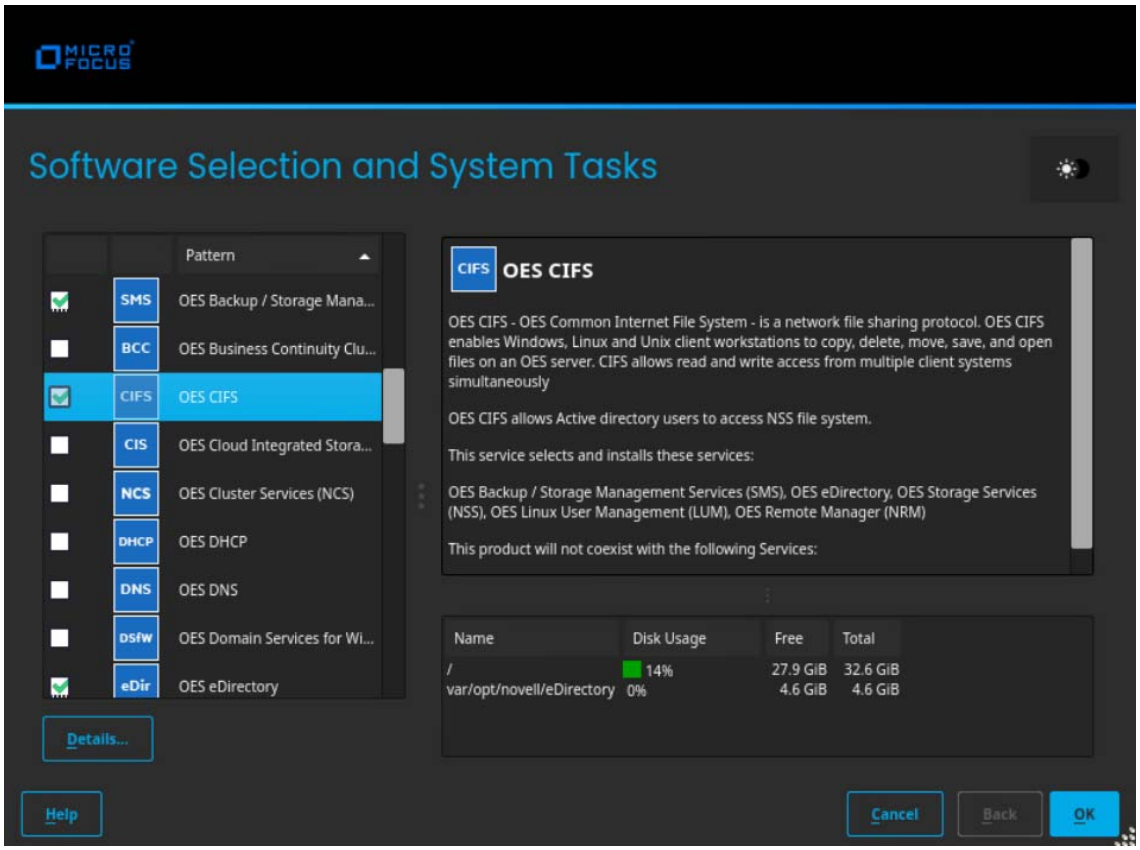
1. In the YaST install for OES, on the **Installation Settings** page, click **Software** to go to the **Software Selections** page.

   For information about the OES installation process, see the Installation Guide.

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

   The following additional services are automatically selected:

   - OES Backup / Storage Management Services (SMS)
   - NetIQ eDirectory
   - OES Linux User Management (LUM)
   - OES NCP Server / Dynamic Storage Technology
   - OES Remote Manager (NRM)
   - OES 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 Open Enterprise Server Configuration window, click **Change** and then click **OES 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.

4.2 Installing CIFS after the OES Installation

If you are installing CIFS after installing OES, 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 **OES CIFS** from the software patterns listed.

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

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

NOTE: If you are installing CIFS after installing OES, 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.
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 server is attached to an existing tree, you can change this to another LDAP port.
Local NCP Server context	Displays the NCP Server context.
Credential Storage Location	By default, the credential is stored in OES Credential Store. 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 server.

4.3 Installing NMAS

Use one of the following methods to install NMAS:

- **Fresh/Media Install:** LSM is installed with CIFS by default. NMAS method needs to be installed only once for the entire tree.
- **Upgrade and 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.

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.

4.4 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 91.

- Section 4.4.1, “Verifying Files and Folders,” on page 29
- Section 4.4.2, “Verifying the File Configuration Information,” on page 31
- Section 4.4.3, “Verifying LSM Installation,” on page 31

4.4.1 Verifying Files and Folders

Run the following commands on the OES server console:

1. Run the `ls /opt/novell/cifs/` command and verify that the `bin`, `locale`, `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_ncp_attribs.sh ◆ cifs_update_proxy_cred.sh ◆ encrypt_password ◆ getpwpolicies.sh ◆ novcifs ◆ retrive_proxy_cred ◆ migafp2cifs

Commands	Files
`ls /opt/novell/migration/sbin`	◆ maprights ◆ maptrustees ◆ migCifsC ◆ migCifsS ◆ migcifs.sh ◆ migcred ◆ migedir ◆ migfiles ◆ migftp.pl ◆ miggui ◆ migmatchup ◆ mignds ◆ migndscheck ◆ mignotify ◆ migrights ◆ migtime.pl ◆ migtrustees ◆ mls ◆ mpvguid ◆ getServerCert.rb ◆ libX11.so ◆ serveridswap ◆ volmount.rb ◆ 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 OES Credential Store for storing the CIFS proxy user credentials, run the `oescredstore -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`.

4.4.2 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.

4.4.3 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.

4.5 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 server console, run the following command to complete the plug-in installation:

   `rcnovell-tomcat restart` or `systemctl restart novell-tomcat.service`.

4.6 Installing Avahi After OES Installation

If you did not install Avahi Package Services during the OES installation, you can install it later by using **YaST > Open Enterprise Server**.

1. Open the YaST Control Center. In the left panel under **Groups** section, click **Software**, then click **Software Management** to open the **Software Search** page.

2. Search **Avahi** in the search bar.
3. Select **Avahi** from the **Package** search result list, then click **Accept**.
4. Restart CIF server to view the CIFS server detected on the Mac Client

---

NOTE: User need permission to

4.7 What's Next

When the installation is complete, you can get started with CIFS administration activities. For details, see Chapter 5, “Administering the CIFS Server,” on page 33.

5 Administering the CIFS Server

CIFS on an Open Enterprise Server (OES) server can be managed and administered either through iManager 3.2.6 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 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 4.5, “Installing the CIFS iManager Plug-In,” on page 31.

For basic information on command line administration, see Section 5.2, “Using the Command Line to Manage CIFS,” on page 41 or for complete details, see Appendix A, “Command Line Utility for CIFS,” on page 115.

- Section 5.1, “Using iManager to Manage CIFS,” on page 33
- Section 5.2, “Using the Command Line to Manage CIFS,” on page 41
- Section 5.3, “Apple Time Machine Backups to NSS Volumes,” on page 44
- Section 5.4, “Multi-Factor Authentication for CIFS Service,” on page 45
- Section 5.5, “Locks Management for CIFS,” on page 46
- Section 5.6, “Third-Party Domain Authentication,” on page 47
- Section 5.7, “Roaming User Profile,” on page 49
- Section 5.8, “Dynamic Storage Technology for CIFS Server,” on page 51
- Section 5.9, “DFS Junction Support in CIFS Linux,” on page 52
- Section 5.10, “Subtree Search,” on page 53
- Section 5.11, “Enabling Offline Files Support,” on page 54
- Section 5.12, “Enabling Folder Redirection Support,” on page 54
- Section 5.13, “Directory Cache Management for CIFS Server,” on page 55
- Section 5.14, “Server-side Copy Feature,” on page 56
- Section 5.15, “What’s Next,” on page 56

5.1 Using iManager to Manage CIFS

You can manage CIFS services from iManager. 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 iManager for Linux User Management" in the Linux User Management Administration Guide.

- Section 5.1.1, "Prerequisites," on page 34
- Section 5.1.2, "Selecting a Server to Manage," on page 34
- Section 5.1.3, "Setting the CIFS Server and Authentication Properties," on page 35
- Section 5.1.4, "Managing CIFS Shares," on page 39
- Section 5.1.5, "Configuring a CIFS User Context," on page 41
- Section 5.1.6, "Stopping CIFS," on page 41

5.1.1 Prerequisites

- Install the CIFS iManager plug-in. For details, see Section 4.5, "Installing the CIFS iManager Plug-In," on page 31.
- Install CIFS on at least one OES server. For details, see Chapter 4, "Installing and Setting Up CIFS," on page 25.
- Ensure that ndsd is running. Use `systemctl status ndsd.service` on the server console to check.

5.1.2 Selecting a Server to Manage

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

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

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 **Next**.

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 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.

6 Continue with other administrative actions as necessary:

- Section 5.1.3, “Setting the CIFS Server and Authentication Properties,” on page 35
- Section 5.1.4, “Managing CIFS Shares,” on page 39
- Section 5.1.5, “Configuring a CIFS User Context,” on page 41

5.1.3 Setting the CIFS Server and Authentication Properties

The server and authentication parameters can be set 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 5.1.2, “Selecting a Server to Manage,” on page 34.

To change these parameters from command line, see Section 5.2.5, “Modifying the CIFS Configuration,” on page 42.

- “Setting CIFS General Server Parameters” on page 35
- “Enabling and Disabling SMB Signing” on page 36
- “Setting CIFS General Authentication Parameters” on page 36

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.

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 5-1 *CIFS Server Page Parameters*

Parameter	Description
CIFS Virtual Server Name	The name of the server running CIFS services. The length can be a maximum of 15 characters. The default server name is the OES server name. If OES host or a cluster resource is joined to domain and you need to rename this parameter, then follow the procedure provided at Renaming the Netbios Name of OES Host or Cluster Resource in the NSS AD Administration Guide.
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 36.

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.

Table 5-2 *CIFS Authentication Page Parameters*

Parameters	Description
Mode	Indicates the method of authentication used by CIFS. CIFS uses either eDirectory (local) or third-party Domain authentication mechanisms. ◆ **eDirectory (Local):** Clients are members of a workgroup. The server running CIFS services performs the user authentication. The login credentials (user name and password) on an OES 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. **NOTE:** Extended Security (NTLMSSP) and SMB2 are not supported for Third Party Domain mode authentication. For more information on enabling Third party domain authentication, see Section 5.6, “Third-Party Domain Authentication,” on page 47.
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.

Parameters	Description
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. 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 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.

5.1.4 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 5.1.2, “Selecting a Server to Manage,” on page 34.

To manage CIFS Shares from command line, see Section 5.2.7, “Working with CIFS Shares,” on page 44.

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 39
- “Editing a CIFS Share” on page 39
- “Removing a CIFS Share” on page 40
- “CIFS Share Parameters” on page 40

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 5.1.2, “Selecting a Server to Manage,” on page 34.

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 5.1.2, “Selecting a Server to Manage,” on page 34.
2. Specify the **Share Name, Volume, Path**, and **Comment** for the new share. For details, see Table 5-3 on page 40.
3. Click **OK** to save your changes.

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

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 5.1.2, “Selecting a Server to Manage,” on page 34.

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 5.1.2, “Selecting a Server to Manage,” on page 34.
2. Modify the **Share Name** or **Path** or **Comment** for the share. For details, see Table 5-3 on page 40.
3. Click the **Modify** button to modify the **Volume** and **Path** on the pop-up screen. For details, see Table 5-3 on page 40.
4. Click **OK** twice to save your changes.

Removing a CIFS Share

Before deleting a share, ensure that your CIFS server is started and running. For information on starting iManager and accessing the CIFS server, see Section 5.1.2, “Selecting a Server to Manage,” on page 34.

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, a 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 5-3 *Shares Page Parameters*

Parameter	Description
Name	The name that the CIFS share uses for all the CIFS services and for display on Windows computers. For example, if you specify `Company Photos` as the share name associated with `vol1\graphics`, then Windows workstations browsing the network see `Company Photos` instead of `vol1\graphics`. A Share name can be up to 80 characters long and can contain any single-byte characters, but should not begin or end with an underscore _ or contain multiple underscores _.
Volume	The OES 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.

5.1.5 Configuring a CIFS User Context

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

To configure a context search from the command line, see Section 5.2.8, "Configuring the CIFS Context Search File," on page 44.

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

- "Adding a New Context" on page 41
- "Removing a Context" on page 41

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 5.1.2, "Selecting a Server to Manage," on page 34.

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

5.1.6 Stopping CIFS

To stop a running CIFS server:

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

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

5.2 Using the Command Line to Manage CIFS

Command line utilities are available to control the CIFS services. The main activities for CIFS services are described in this section. For information about specific CIFS commands, see Appendix A, "Command Line Utility for CIFS," on page 115 or enter `man novcifs` at the command prompt.

- Section 5.2.1, "Starting CIFS," on page 42
- Section 5.2.2, "Stopping CIFS," on page 42
- Section 5.2.3, "Restarting CIFS," on page 42
- Section 5.2.4, "Monitoring CIFS," on page 42
- Section 5.2.5, "Modifying the CIFS Configuration," on page 42
- Section 5.2.6, "Anonymous Login for CIFS," on page 43
- Section 5.2.7, "Working with CIFS Shares," on page 44
- Section 5.2.8, "Configuring the CIFS Context Search File," on page 44

5.2.1 Starting CIFS

Use the `rcnovell-cifs start` or `systemctl start novell-cifs.service` command to start CIFS.

5.2.2 Stopping CIFS

Use the `rcnovell-cifs stop` or `systemctl stop novell-cifs.service` command to stop CIFS.

5.2.3 Restarting CIFS

Use the `rcnovell-cifs restart` or `systemctl restart novell-cifs.service` command to restart CIFS.

5.2.4 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.

5.2.5 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 5.1, “Using iManager to Manage CIFS,” on page 33.

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` or `systemctl restart novell-cifs.service` command in order for the configuration changes to take effect.

5.2.6 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 43
- "Anonymous Login in a Cluster" on page 43

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 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 2023: 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.

5.2.7 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 5.1.4, “Managing CIFS Shares,” on page 39.

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 118
- “Removing a Share Point on a Non-Clustered Volume (Login to the node as root)” on page 118
- “Displaying the List of Share Points” on page 118
- “Displaying Details of a Share Point” on page 118
- “Enabling or Disabling SMB Signing” on page 120.

5.2.8 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 5.1.5, “Configuring a CIFS User Context,” on page 41.

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.

5.3 Apple Time Machine Backups to NSS Volumes

The user/trustees should have read, write, create, erase, modify, and file scan permissions on NSS volumes to back up their data on the MAC clients.

Starting from Open Enterprise Server 2018 SP3, Mac clients auto-detect shares/volumes configured as ATM backup targets in the same subnet if Avahi service is up and running. If you have not installed Avahi Package Services during the OES installation, you can install it later by using **Yast>Open Enterprise Server**.

1. Open the YaST Control Center. In the left panel under **Groups** section, click **Software**, then click **Software Management** to open the **Software Search** page.
2. Search **Avahi** in the search bar.

3. Select **Avahi** from the **Package** search result list, then click **Accept**.
4. Restart CIFS server to view the CIFS server detected on the Mac Client.

novcifs Command

Apple Time Machine Backup: Enables or disables share to be Apple Time Machine (ATM) backup target. Enable this option to let ATM running on the Mac clients to backup their data to the specified share.

```
--atm-backup=yes|no  --name=SHARENAME
```

ATM backup feature works only when `--leasing` is enabled with SMB3 or later connections.

5.4 Multi-Factor Authentication for CIFS Service

OES CIFS can be configured to use an OES MFA service to enforce multi-factor authentication when users access the CIFS share. MFA server service is supported on OES 24.4 or later versions.

By default, MFA agent is installed and active on all the CIFS servers which is required for OES MFA service. MFA is enforced and triggered from the CIFS server and no configuration is needed on the CIFS client.

With MFA enabled, the first-factor authentication continues to be the existing password-based authentication using NTLMSSP for eDirectory users and Kerberos for Active Directory users. OES MFA service is used to perform the second factor authentication. For second-factor authentication, CIFS supports only the smart phone push method.

- Section 5.4.1, “Configure CIFS to Enforce MFA for Drive Mapping,” on page 45

5.4.1 Configure CIFS to Enforce MFA for Drive Mapping

MFA can be enabled at the server level or share level. When enabled at the server level, MFA is enforced for all the shares on the server. By default, MFA is disabled on the CIFS server.

- Server level

  ```
  novcifs--mfa=yes|no
  ```

- Share level

  ```
  novcifs -s --mfa=yes|no -n SHARENAME, --share --mfa=yes|no --name
  SHARENAME
  ```

5.5 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, and Windows Vista.

  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.

- **Leasing:** Leasing is an enhancement to conventional Oplocks and is available with SMB2.1 and above dialects. Leasing enables clients to do read, write and handle caching in an efficient way, which significantly improves the performance by reducing the network traffic. It provides better performance compared to Oplocks by increasing the amount of caching and by reducing the number of cache break. It is recommended to use leasing for increased file access performance.

  You can use the novcifs option `novcifs --leasing=yes|no` to enable or disable the file leasing. It is enabled by default. Leasing can be enabled only if Oplocks is enabled.

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

5.6 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:

- Section 5.6.1, “Prerequisites,” on page 47
- Section 5.6.2, “Using iManager to Enable Third-Party Authentication,” on page 49

IMPORTANT: Domain pass-through authentication is supported for backward compatibility only. When authentication mode is changed to Third party authentication, CIFS will support only the SMB1 protocol.

5.6.1 Prerequisites

- “Prerequisites for the Windows Primary Domain Controller” on page 47
- “Prerequisites for the CIFS Server” on page 49

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
  ```
- Set the value of registry key `AllowLegacySrvCall` to 1 to allow legacy service calls.
  1. Open Registry Editor. To do this, click **Start**, type `regedit` in the Start Search box, and then press ENTER.
  2. Locate and then right-click the following registry subkey:

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`
  3. On the **Edit** menu, point to **New**, and then click DWORD (32-bit) Value.
  4. Type `AllowLegacySrvCall`, and then press ENTER.
  5. Right-click `AllowLegacySrvCall`, and then click **Modify**.
  6. Type 1 in the **Value** data box, and then click **OK**.
  7. Exit Registry Editor.

  For more information, see Microsoft Knowledge Base (https://support.microsoft.com).
- 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 Microsoft documentation.

- Set Lmcompatibilitylevel on 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**.
- 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`.
- 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 36.
- Set the dialect to SMB v1 using the command `novcifs --dialect=SMB`.

5.6.2 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 **Next**.

   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 5-2, "CIFS Authentication Page Parameters," on page 37.
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.
12. For the changes to take effect, you must restart the CIFS service.

    ```
    systemctl restart novell-cifs.service
    ```

5.7 Roaming User Profile

Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers. When a user signs in to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user signs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile. Roaming User Profiles is typically enabled on domain accounts by a network administrator.

File share path where profile is stored: Configure the profile path in Windows user properties as `\\fs1.corp.contoso.com\User Profiles$\%username%\`

NOTE: Do not forget to add backslash at the end of the profile path.

For more information, see Folder Redirection, Offline Files, and Roaming User Profiles overview (https://technet.microsoft.com/en-us/library/hh848267.aspx).

Windows recommends to enable the use of separate profiles for each version of Windows. This means for each version of client a profile is stored on a different folder in the file share.

Operating System Version	Roaming User Profile Location
Windows XP and Windows Server 2003	`\\<servername>\<fileshare>\<username>`
Windows Vista and Windows Server 2008	`\\<servername>\<fileshare>\<username>\.V2`
Windows 7 and Windows Server 2008 R2	`\\<servername>\<fileshare>\<username>\.V2`
Windows 8 and Windows Server 2012	`\\<servername>\<fileshare>\<username>\.V3` (after the software update and registry key are applied `\\<servername>\<fileshare>\<username>\.V2` (before the software update and registry key are applied)

For more information, see Deploy Roaming User Profiles (https://technet.microsoft.com/en-us/library/jj649079.aspx#EnableProfileVersions).

5.7.1 Configuration Required on OES Server for Roaming Profiles

In a pure Windows to Windows world a Windows client would automatically create a username.V<n> folder on Windows file server and assign rights to this folder for the user. However, in Windows to OES server environment, the client cannot automatically assign user rights on the folder. Therefore, the Administrator has to create a folder on a file share and assign rights on that folder for the corresponding user. For example,

```
rights -a -f /media/nss/<volume>/<home>/<user> -r all trustee
<AD_domain>\\user
```

Recommendation:

Administrator creating and assigning rights to each version folder might be a repetitive task, this can be simplified by adding a backslash "\" to the profile path in user properties as follows:

```
\\fs1.corp.contoso.com\User Profiles$\%username%\
```

Add user rights as follows:

```
rights -a -f /media/nss/<volume>/<folder>/<user> -r all trustee
<AD_domain>\\user
```

This will in turn allow the Windows clients to create separate folder for each version of the client inside the file share like this

```
/media/nss/<volume>/<folder>/<user>/.V2
/media/nss/<volume>/<folder>/<user>/.V3
```

For more information about assigning rights, see rights in the Storage Services File System (NSS) Administration Guide for Linux.

5.8 Dynamic Storage Technology for CIFS Server

Dynamic Storage Technology (DST) for Open Enterprise Server (OES) is an information life-cycle management technology that uses a policy-based approach for relocating data between two 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 *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 *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 *Dynamic Storage Technology Administration Guide*.

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

5.9 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 *Distributed File Services Administration Guide for Linux*.

- Section 5.9.1, "Prerequisites," on page 52
- Section 5.9.2, "Enabling DFS Support," on page 52
- Section 5.9.3, "Limitations," on page 53

5.9.1 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.
- With Port 445 support, clients might not use NetBIOS for resolution of DFS target name. DNS should also be updated with entries for NetBIOS name of the CIFS target.

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

5.9.2 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.
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`.

5.9.3 Limitations

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

5.10 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.

You can only search eDirectory users that are in native and domain mode. You cannot search Active Directory users.

- Section 5.10.1, “Prerequisites,” on page 53
- Section 5.10.2, “Enabling a Subtree Search,” on page 53
- Section 5.10.3, “Subtree Search in a Cluster Setup,” on page 53

5.10.1 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.

5.10.2 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.

5.10.3 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.

5.11 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 Support website.

5.12 Enabling Folder Redirection Support

Folder redirection allows you to redirect the local path of a folder to a network file share. With this feature enabled, based on the trustee assignments, users can access and work with files on a server as if the files are on the local computer and they can also access the files from any other computer on the network. For example, you can redirect the local Documents folder and host it on a network share. The files in the folder are then available to the user from any computer on the network. OES CIFS shares can be used as a target for Folder Redirection.

NOTE: The support for this feature is available only for AD users.

To configure CIFS share as the target path for Folder Redirection:

1. Identify the users to whom Folder Redirection has to be enabled and create a group of those users.

   Based on your AD environment, add this group as a member of OESAccessGrp or DLOESAccessGrp. For more information on the NSS AD infrastructure requirements, see Meeting NSS AD Infrastructure Requirements in the NSS AD Administration Guide.

2. Create a share to host the redirected folders on the server.

Use the root of the share as the target path for Folder Redirection and not any directory under root. It is recommended to suffix the share name with $ to prevent the share from enumeration. For example, `test_share$`.

3 Enable Folder Redirection for the share created by using the command:

```
novcifs -s --folder-redirection=yes|no -n <share_name>
```

4 Add the user group as a trustee on the target path of the Folder Redirection enabled share and assign `rwcemf` rights.

IMPORTANT: Do not assign supervisor right.

5 Set the Inherited Rights Filter to **None** on the target path of the share that is created to host the redirected folders.

The CIFS share can now host the redirected folders.

NOTE: When a user log in to a workstation and redirects the local folder to the network share, a directory with the same user name used for login in created within the share. The user is added as a trustee on this directory with rwcemf rights and Inherited Rights Filter set to None. This implies that only the logged in user has access to all the redirected folders in this user specific directory within the share.

5.13 Directory Cache Management for CIFS Server

Table 5-4 *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

5.14 Server-side Copy Feature

The server-side copy feature is enabled by default and does not need any configuration change on the client or server.

Server side copy support on OpenText CIFS server enables Windows workstation clients to make use of server-side copy that can considerably improve the performance for file copy operations within the same share as the file data need not traverse the network.

Server-side copy is invoked automatically through SMB protocol for all eDirectory and Active Directory users when they copy files from one location to another location on the same share. When a file copy operation is initiated from CIFS client, the client issues FSCTL_SRV_COPYCHUNK request to the CIFS server. Upon receiving this request, the CIFS server reads the file date from the source location on the disk and writes it to the target location on the disk.

Server-side copy is invoked only when the source and target locations of file copy are in the same CIFS share. It is not invoked for file copy operation between two different CIFS shares on the same or different server.

For example, a file copy from `\Share1\Dir1` to `\Share1\Dir2` invokes server-side copy. Whereas a file copy from `\Share1\Dir1` to `\Share2\Dir2` does not.

Supported Clients:

- Windows Server 2019 and later: via Windows Explorer or Robocopy
- Windows 10 and later: via Windows Explorer or Robocopy

5.15 What's Next

To learn how to use CIFS services as an end user, see Chapter 10, "Working with Client Computers," on page 73.

6 CIFS Monitoring and Management

The commands introduced in the `novcifs` utility let you to manage open files and CIFS connections.

You can filter connections to see if the connections originate from eDirectory or Active Directory.

6.1 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.

6.2 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 115.

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.

6.3 Monitoring Connections

Table 6-1 *Connection Monitoring command options*

Option	Description
`-C, --Conn`	Displays the count of active connections.
`-Cl, --Conn --list`	Lists all CIFS connections.
`-ClA, --Conn --list --ad`	Lists all Active Directory connections.
`-ClE, --Conn --list --eDir`	Lists all eDirectory 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.

6.3.1 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 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.

DA: Indicates the right to delete 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.

6.4 Monitoring Files

Table 6-2 *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.
`-Flop FILE-PATH, --Files --list --oplock-lease-info --path=FILE-PATH`	Lists users who opened the file and the oplock or lease information of the file by the specified file path.
`-Flov VOLUME-NAME, --Files --list --oplock-lease-info --volume=VOLUME-NAME`	Lists users, files opened by them, and the oplock or lease information of the files on the specified volume.

Option	Description
`-Flon CONNECTION-NUMBER, --Files --list --oplock-lease-info --connection=CONNECTION-NUMBER`	Lists files opened by the user session and the oplock or lease information of the files by the specified connection number.
`-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
- Oplock or lease information of the 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.

Oplock or Lease Information: Specifies the oplock or lease acquired by the client on the file.

batch: Indicates the Batch Oplock.

excl: Indicates the Exclusive Oplock.

R: Indicates the Read Caching Lease.

RH: Indicates the Read Handle Caching Lease.

RW: Indicates the Read Write Caching Lease.

RWH: Indicates the Read Write Handle Caching Lease.

7 Migrating CIFS to OES

The Open Enterprise Server (OES) 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 an OES server to another OES server by using the GUI Migration Tool or from the command line.

To get started with migration, see the *Migration Tool Administration Guide*.

For more information on migrating CIFS, see "Migrating CIFS to OES 24.4" in the *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 *Migration Tool Administration Guide*.

8 Running CIFS in a Virtualized Environment

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

To get started with Xen virtualization, see the SLES 15 Virtualization 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, see "Installing OES on a VM" in the *Installation Guide*.

8.1 What's Next

To learn more about what you can do with CIFS on OES, continue with Chapter 5, "Administering the CIFS Server," on page 33.

9 Configuring CIFS with Cluster Services for an NSS File System

Cluster Services for Open Enterprise Server (OES) 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 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.

- Section 9.1, “Benefits of Configuring CIFS for High Availability,” on page 65
- Section 9.2, “Cluster Terminology,” on page 65
- Section 9.3, “CIFS and Cluster Services,” on page 66
- Section 9.4, “Configuring CIFS in a Cluster,” on page 71
- Section 9.5, “What's Next,” on page 72

9.1 Benefits of Configuring CIFS for High Availability

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

- Cluster Services and Storage Services (NSS), which are part of OES, combine with 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 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 and Linux clients.
- **CIFS virtual server:** A cluster-enabled pool and the 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 Cluster Services.
- **Monitor script:** A file that contains the cluster resource commands that allows 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 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 Cluster Services.

9.3 CIFS and Cluster Services

Cluster Services can be configured either during or after OES installation. In a cluster, CIFS for OES 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 CIFS in a cluster environment:

- Section 9.3.1, "Prerequisites," on page 66
- Section 9.3.2, "Using CIFS in a Cluster Environment," on page 67
- Section 9.3.3, "Example for CIFS Cluster Rights," on page 69

9.3.1 Prerequisites

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

❒ Cluster Services installed on OES 2018 or later servers

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

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

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

Follow the instructions in Section 4.1, “Installing CIFS during the OES Installation,” on page 25 and Section 4.2, “Installing CIFS after the OES Installation,” on page 27.

9.3.2 Using CIFS in a Cluster Environment

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

- CIFS is not cluster-aware and is not clustered by default. You must install and configure CIFS on every node in the cluster where you plan to give users CIFS access to the shared cluster resource.
- CIFS runs on all nodes in the cluster at any given time.
- 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 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 OES 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 Cluster Services for Linux Administration Guide*.

   For details on creating a pool using OES Linux Manager using the `nlvm create pool` command, see “NLVM Commands” in the *OES 23.4: 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 displayed on the terminal console:

   ```
   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 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 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 OES 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.

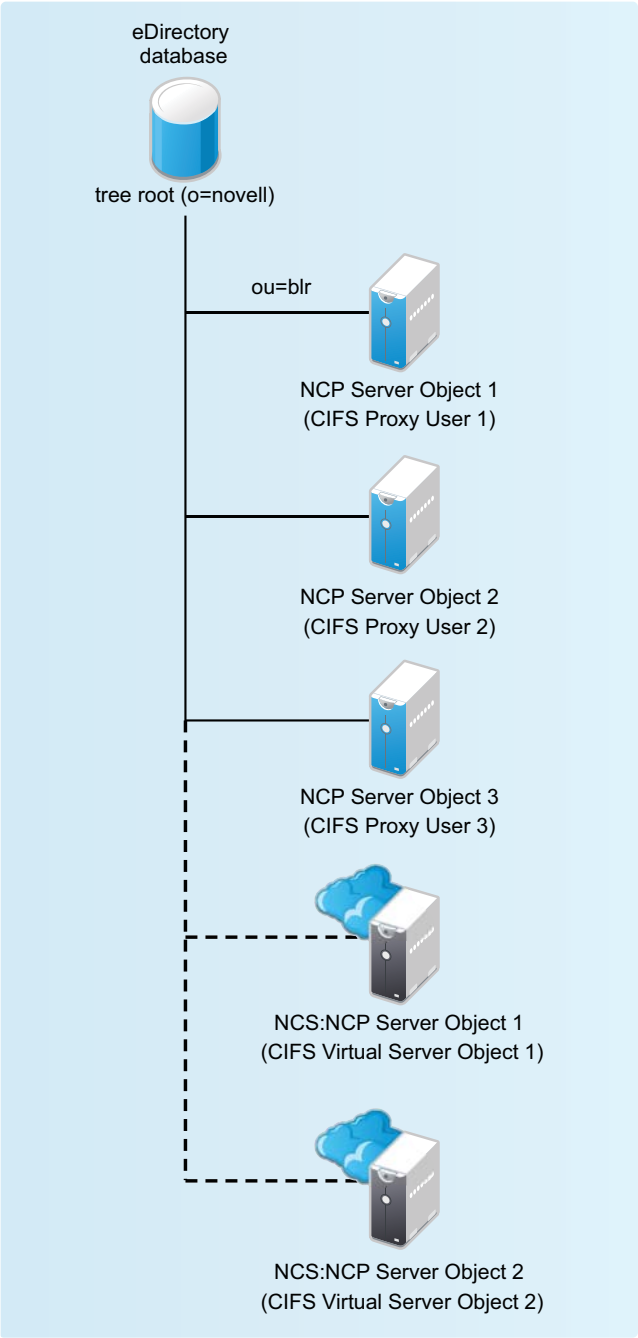
Apart from the above mentioned CIFS specific attributes, CIFS proxy user must have read access on following attributes of CIFS virtual server object:

- NCS:Netware Cluster
- NCS:Volume

If you want to do Active Directory integration for the cluster resource, CIFS proxy user must have read access on the "Resource" attribute of CIFS virtual server object and read access on the "Host server" attribute of cluster pool 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 OES 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:

- Section 9.4.1, “Prerequisites,” on page 71
- Section 9.4.2, “Creating Shared Pools and Accessing Sharepoints,” on page 71

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” on page 71
- “Creating Pools Using NSSMU” on page 72
- “Creating Pools Using NLVM” on page 72

Creating Pools Using iManager

For details on creating pools by using iManager, see “Creating a Pool” in the *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*.

Creating Pools Using NLVM

For details on creating pools by using NLVM, see "NLVM Commands" in the *OES 23.4: NLVM Reference*

You can add 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 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 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 5, "Administering the CIFS Server," on page 33.

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 73.

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 73
- Section 10.2, “Mapping Drives and Mounting Volumes,” on page 75
- Section 10.3, “Using OES File Access Rights Management (NFARM),” on page 75

10.1 Accessing Files from a Client Computer

You can access files and folders hosted on a CIFS server from Windows 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 73
- Section 10.1.2, “Accessing Files from a Linux Desktop,” on page 74

10.1.1 Accessing Files from a Windows Client

- “Prerequisite” on page 73
- “Procedure to Access Files” on page 73

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.

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, 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) 2018 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" on page 74
- "Using a NETBIOS Name to Access Files" on page 74
- "Using nautilus to Access Files" on page 74

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 Windows and Windows Vista clients and mount the volumes from a Linux client.

- Section 10.2.1, “Mapping Drives from a Windows Client,” on page 75
- Section 10.2.2, “Mounting Volumes from a Linux Client,” on page 75

10.2.1 Mapping Drives from a Windows Client

From a Windows (2000, XP, or Vista) 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 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>`

10.3 Using OES File Access Rights Management (NFARM)

NFARM is a shell extension that enables eDirectory or Active Directory users on Windows and Mac workstation to perform Salvage and Purge operations. In addition,

- Allows the eDirectory users on Windows workstation (without Client for Open Enterprise Server) to manage the password expiry.
- Enables Windows Active Directory administrators to manage the access rights and quotas of AD users or groups on OES Storage Services (NSS) resources.

NOTE: The Open Enterprise Server download page offers the NFARM management service only if the server has the CIFS pattern installed.

Accessing and Installing NFARM

Go to OES Welcome page (http://<OES server IP Address or the host name>/welcome/client-software.html) and download the matching version of NFARM.

- **Windows:** NFARM installer for Windows (64-bit)
- **Mac:** NFARM installer for Mac

For more information on support matrix, prerequisites and installing NFARM, see NFARM (OES File Access Rights Management) in the NSS AD Administration Guide.

By installing NFARM on a workstation, the following features are available:

- Section 10.3.1, “Salvage and Purge on Windows,” on page 76
- Section 10.3.2, “Salvage and Purge on Mac,” on page 80
- Section 10.3.3, “Password Expiry Notification on Windows,” on page 82
- Section 10.3.4, “Managing Access Rights and Quotas for AD Entities,” on page 84

10.3.1 Salvage and Purge on Windows

The Salvage and Purge utility for Windows lets you recover or delete the files and directories permanently from the NSS file system. The files that have been purged cannot be recovered.

This tool gets automatically installed when you install NFARM (NFARM installer for Windows).

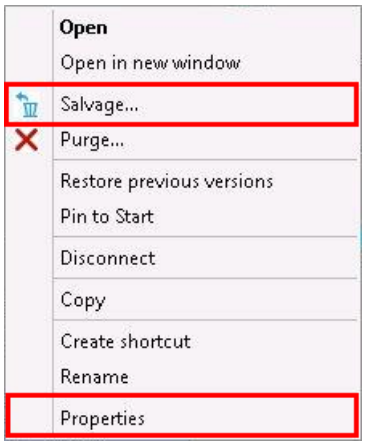
- “Salvaging Files” on page 76
- “Purging Files” on page 78

Salvaging Files

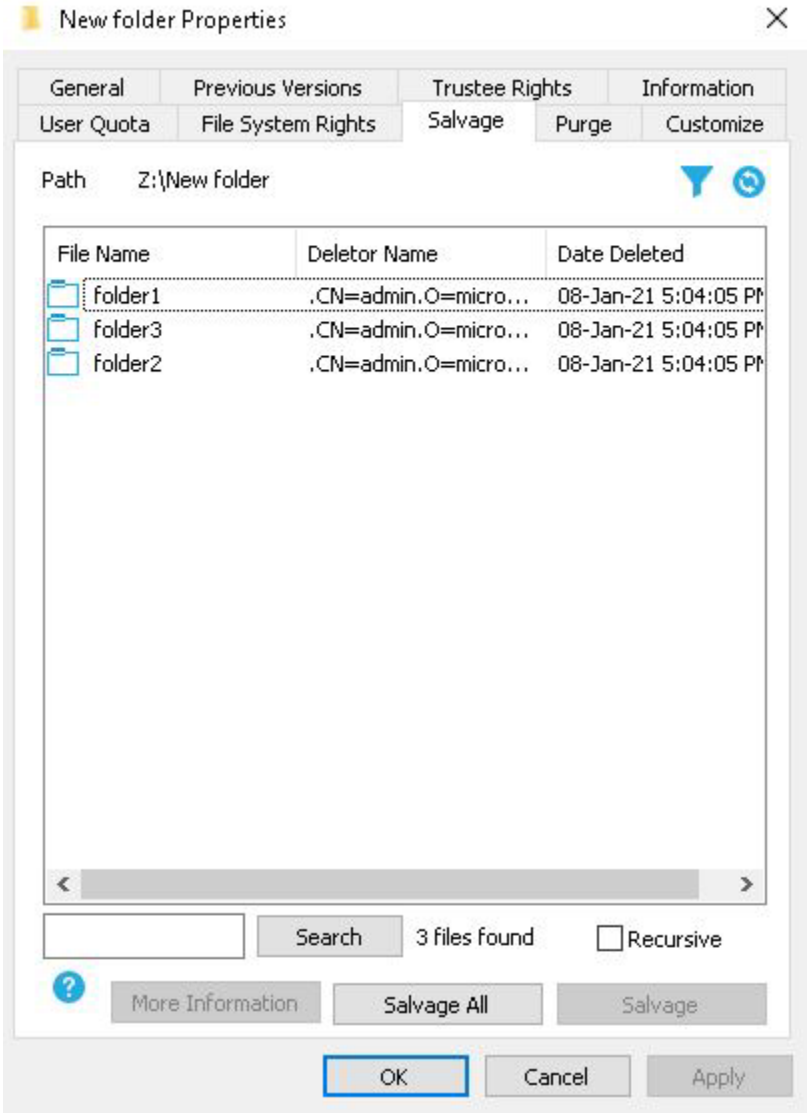
The salvage utility for Windows lets you recover the deleted files and directories from the NSS file system.

To salvage:

1 Right-click a Windows mapped network drive or folder, then click **Salvage** or **Properties > Salvage**.



- The following tabs are displayed:



- Filter : Set attributes to filter and display the data to be salvaged.

- Clear Filter : Clear filter and displays the data to be salvaged.
- Recursive: Salvage all data from the folder and subfolders.

2 Select the salvageable files, then click **Salvage**. The selected files are salvaged. To salvage all files, click **Salvage All**.

TIP: ◆**To select all files:** Select the first file, then press CTRL+SHIFT+END.

- **To select multiple files:** Press and hold the CTRL key, then click the files of your choice.
- **To select a series of files:** Press and hold the SHIFT key, then click the first file and the last files.
- **To refresh:** Click (refresh) to display the latest list of salvageable files and folders.
- **To sort:** Click the column heading to sort the files and folders. The ▼ icon indicates descending order and the ▲ icon indicates ascending order.

---

3 While salvaging, if a file already exists with the same name, you are prompted to rename it.

4 To see the attributes of the selected files, click **More Information**. The attributes include: File name, Deletor Name, Date Deleted, Creator Name, Date Created, Modifier Name, Date Modified, Archiver Name, Date Archived, Date Accessed, and File Size.

The **More Information** dialog box also includes **Salvage** and **Salvage All**. Follow the same procedure provided in Step 2 on page 78 to perform the salvage operation.

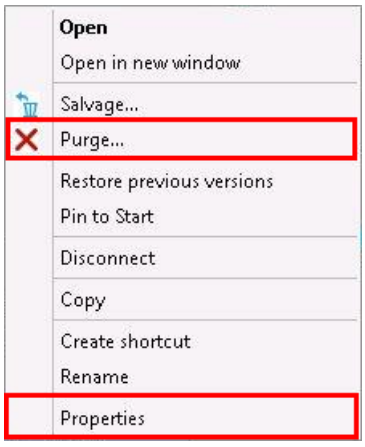
NOTE: To salvage the deleted files from a sub-directory, ensure to salvage the sub-directory and then salvage the files in the sub-directory.

Purging Files

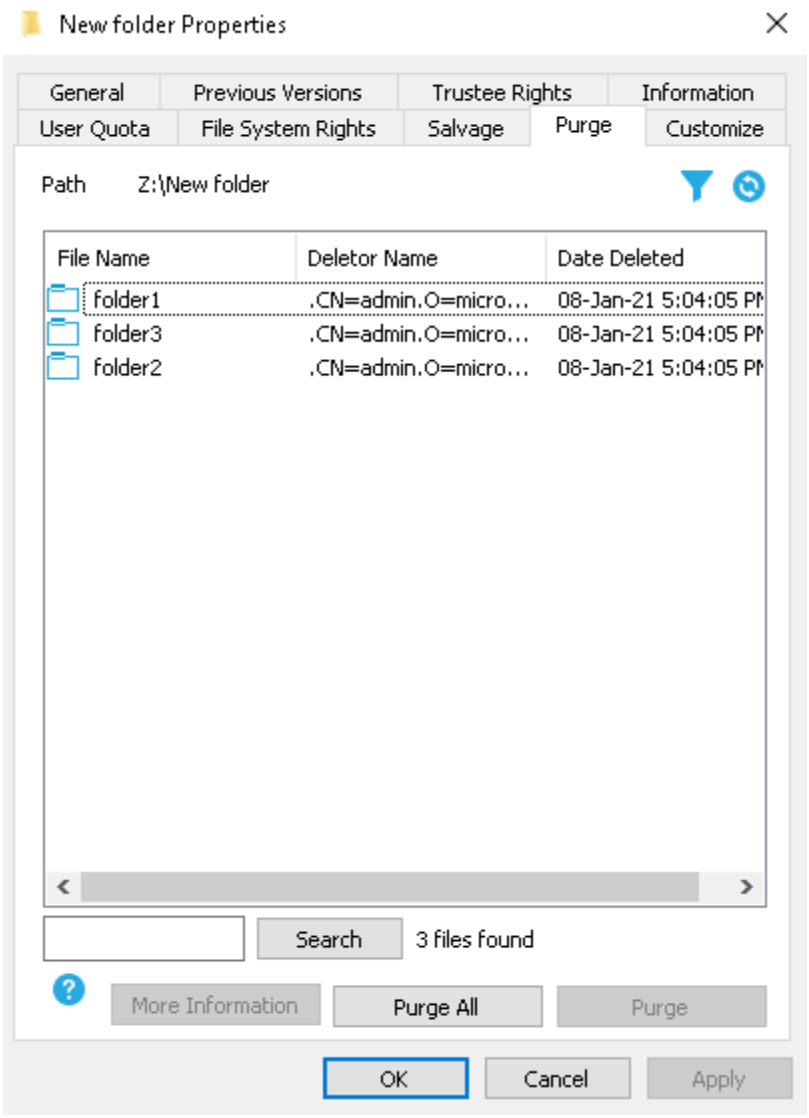
The purge utility for Windows lets you delete files and folders permanently from the NSS file system. Purging is an irreversible action. The files that have been purged cannot be recovered.

To purge:

1 Right-click a Windows mapped network drive or folder, then click **Purge** or **Properties > Purge**.



- The following tabs are displayed:



- Filter : Set attributes to filter and display the data to be salvaged.
- Clear Filter : Clear filter and displays the data to be salvaged.
- Recursive: Salvage all data from the folder and subfolders.

2 Select the files to be purged, then click **Purge**. The selected files are purged. To purge all files, click **Purge All**.

TIP: ◆**To select all files:** Select the first file, then press CTRL+SHIFT+END.

- **To select multiple files:** Press and hold the CTRL key, then click the files of your choice.
- **To select a series of files:** Press and hold the SHIFT key, then click the first file and the last files.
- **To refresh:** Click (refresh) to display the latest list of purgeable files and folders.
- **To sort:** Click the column heading to sort the files and folders. The ▼ icon indicates descending order and the ▲ icon indicates ascending order.

---

3 To see the attributes of the selected files, click **More Information**. The attributes include: File name, Deletor Name, Date Deleted, Creator Name, Date Created, Modifier Name, Date Modified, Archiver Name, Date Archived, Date Accessed, and File Size.

The **More Information** dialog box also includes **Purge** and **Purge All**. Follow the same procedure provided in Step 2 on page 79 to perform the purge operation.

NOTE: The Recursive option is not provided in the GUI. By default, the NSS file system purges the data recursively.

10.3.2 Salvage and Purge on Mac

The Salvage and Purge utility for Mac allows the eDirectory and Active Directory users to recover or permanently delete files and directories from the NSS file system. Purging is an irreversible action. The files that have been purged cannot be recovered.

This tool gets automatically installed when you install NFARM (NFARM installer for Mac).

1 Go to **Finder > Go > Connect to Server** to map an OES network drive.

IMPORTANT: For eDirectory users, ensure to select the **Remember this password in my keychain** check box before connecting to a server.

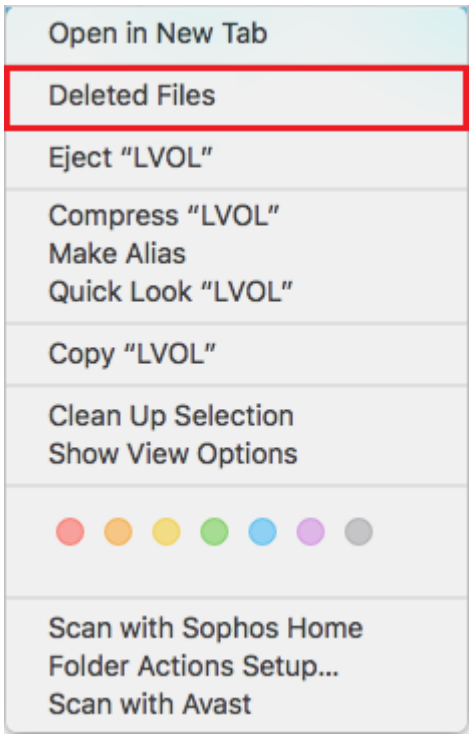
---

2 On Mac workstation, run the following command:

```
pluginkit -a /Applications/SalvagePurge.app/Contents/Plugins/
FinderSyncContextMenu.appex
```

This command registers the Salvage and Purge application with the Finder extension.

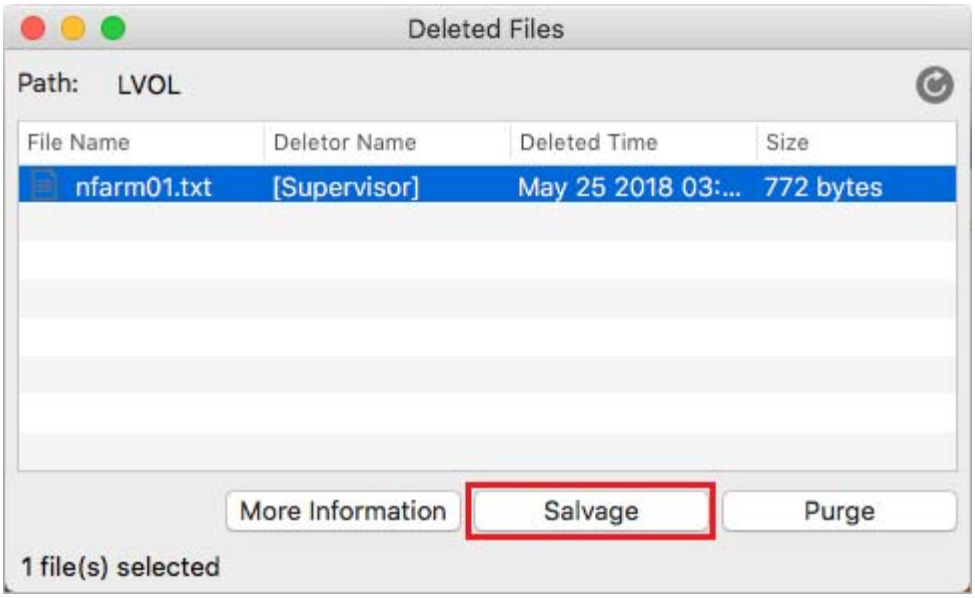
3 Right-click a OES mapped drive, then click **Deleted files**.



A new window is displayed with the list of deleted files. The deleted file attributes include: File Name, Deletor Name, Deleted Time, and Size.

4 Perform salvage or purge operation.

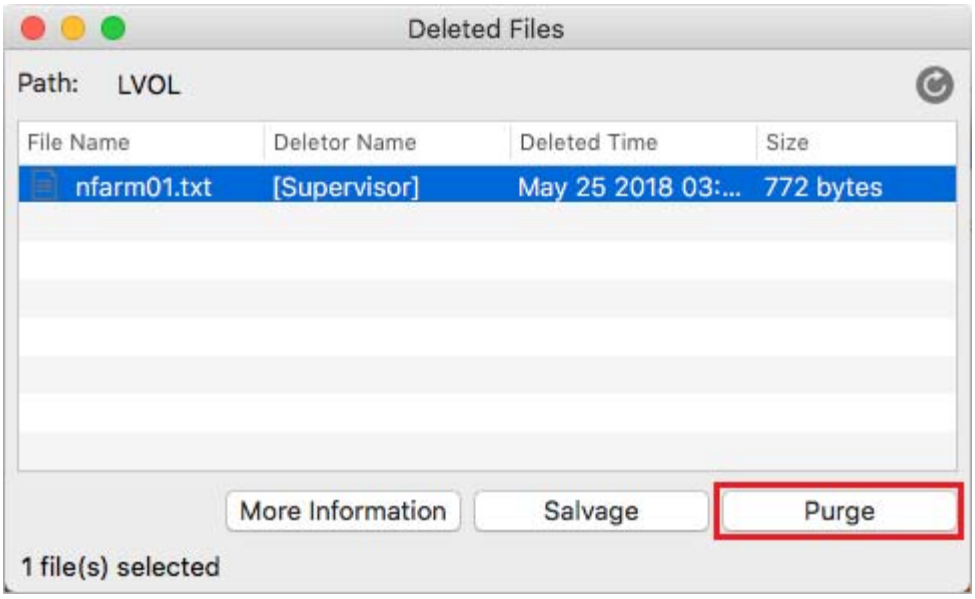
- To Salvage:
  1. Select the salvageable files, then click **Salvage**. The selected files are salvaged.



  2. While salvaging, if a file already exists with the same name, you are prompted to rename it.

NOTE: To salvage the deleted files from a sub-directory, ensure to salvage the sub-directory and then salvage the files in the sub-directory.

- To Purge:
  1. Select the files to be purged, then click **Purge**.



2. A confirmation dialog box is displayed, click **Yes**. The selected files are purged.

TIP: ◆**To select all files:** Select the first file, then press COMMAND+A.

- **To select multiple files:** Press and hold the ALT key, then click the files of your choice.
- **To select a series of files:** Select the first file, press and hold the SHIFT key, and then click the last file.
- **To refresh:** Click (refresh) to display the latest list of salvageable or purgeable files and folders.

---

5 Click **More Information** to view all the attributes of the selected files. It includes File Name, Deletor Name, Deleted Time, Creator Name, Created Time, Modifier Name, Modified Time, Archiver Name, Archived Time, Accessed Time, and Size.

The **More Information** dialog box also includes **Salvage** and **Purge**. Follow the same procedure provided in Step 4 on page 81 to perform the salvage or purge operation.

10.3.3 Password Expiry Notification on Windows

The password expiry notification feature allows the eDirectory users to change the password directly from their client device. If the eDirectory password is due to expire and the user maps to a network drive using their eDirectory credentials from the Windows computer (without Client for Open Enterprise Server), a password expiry notification is displayed.

NOTE: You must select the **Get Password Expiry Notification** check box to receive the notifications related to password expiry.

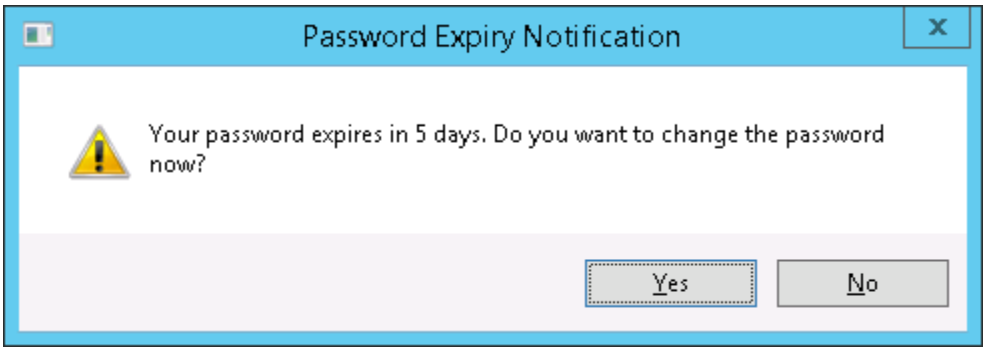
NFARM must be installed on the workstation for password expiry notification feature to be available.

The password expiry notification is configured by the registry entry `PCNotifyConf` in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Notifyees` key. This key is created by the installation of NFARM with the default value as 10 days and can be

modified based on the requirement. For example, if the value is configured as 20 days, the password expiry notification is displayed 20 days before the expiry time, 5 days before the expiry time, 3 days before the expiry time, 1 day before the expiry time, and last day of the password expiry time.

Notifying Users Before Password Expires

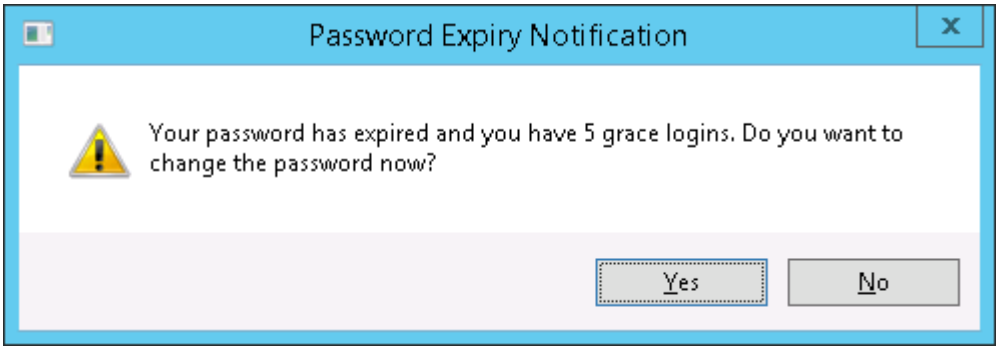
When the user maps a network drive using the eDirectory credentials, and the password of eDirectory user is due to expire (for example, the password expires in 5 days), the password expiry notification is displayed as follows:



If the user clicks **Yes**, a Change Password dialog box is displayed. Specify the old password and new password, then click Change Password.

Displaying Grace Logins After Password Expires

If the user maps a network drive after the password expires, they are provided with additional grace logins.



If the user clicks **Yes**, a Change Password dialog box is displayed. Specify the old password and new password, then click Change Password.

If the user fails to change the password within the provided grace logins they would not be able to map to a network drive.

10.3.4 Managing Access Rights and Quotas for AD Entities

The AD administrators or users with sufficient rights can mange the following:

- Trustees explicit rights, inherited rights filter, and view effective rights. You can also view trustees with rights from the selected path and child or parent directories.
- Owners, NSS attributes and directory quota
- User quotas
- All paths that a user is a trustee of

For more information, see NFARM (OES File Access Rights Management) in the NSS AD Administration Guide.

11 Troubleshooting CIFS

- Section 11.1, “Known issues,” on page 85
- Section 11.2, “CIFS Installation and Configuration,” on page 91
- Section 11.3, “Authentication,” on page 91
- Section 11.4, “Startup,” on page 95
- Section 11.5, “Migration,” on page 96
- Section 11.6, “Mac Client,” on page 96
- Section 11.7, “DFS,” on page 97
- Section 11.8, “Miscellaneous,” on page 98

11.1 Known issues

- Section 11.1.1, “Deleting a Directory Having a Large Number of Files is Taking Too Long On a Windows 10 Client,” on page 86
- Section 11.1.2, “CIFS Does Not Come Up After Upgrading to OES 2018 or Later if Service Proxy is Configured,” on page 86
- Section 11.1.3, “Interruption in access to the CIFS shares from Windows clients upon change of server dialect from SMB2 or later to SMB or upon cluster resource migration,” on page 86
- Section 11.1.4, “Windows Explorer Hangs On Accessing the CIFS Share Path,” on page 87
- Section 11.1.5, “Salvaged Files are not Displayed in Windows 7 Enterprise Client,” on page 87
- Section 11.1.6, “Automatic Synchronization of Offline Files,” on page 87
- Section 11.1.7, “Members Of The Default ad-supervisor-group "Domain Admins" Can Map AD-enabled NSS Volumes Although Their Effective Rights on Those Volumes Is Displayed As NULL,” on page 87
- Section 11.1.8, “Users Are Not Able to Map NSS Resources,” on page 88
- Section 11.1.9, “CIFS Fails to Write Core Dumps,” on page 89
- Section 11.1.10, “CIFS Users Unable to Authenticate to OES Server if the Tree has Netware server as the eDirectory Replica Holding Server,” on page 90
- Section 11.1.11, “Windows Clients Do Not Reflect The Latest File/Folder Operations,” on page 90
- Section 11.1.12, “Different Tree Migration Is Not Available in the Migration Tool,” on page 90
- Section 11.1.13, “File Level Trustees Are Deleted When a File is Modified,” on page 90

11.1.1 Deleting a Directory Having a Large Number of Files is Taking Too Long On a Windows 10 Client

Deleting a directory containing a large number of files is taking too long on a Windows 10 Client. To resolve this issue, update to the latest Windows Client.

11.1.2 CIFS Does Not Come Up After Upgrading to OES 2018 or Later if Service Proxy is Configured

Cause: CIFS service configured with service proxy fails to come up after upgrading to OES 2018 or later. This is because the service proxy users are not migrated to OES Credential Store (OCS).

Action: To resolve this issue, perform the following:

1. Login as root user.
2. Run `yast2 novell-cifs` and then enter eDirectory user password.
3. Specify the CIFS proxy user password.
4. Click **Next** and continue with CIFS configuration.
5. Verify the CIFS service is up and running by using the following command:

   ```
   systemctl status novell-cifs.service
   ```
6. Verify the service entry is present in OES Credential Store by using the following command:

   ```
   oescredstore -l
   ```

11.1.3 Interruption in access to the CIFS shares from Windows clients upon change of server dialect from SMB2 or later to SMB or upon cluster resource migration

Description: If you change the server dialect from SMB2 or later to SMB, the Windows client with the existing mapped share might not establish connection automatically.

Also, in a mixed-node cluster environment, if you migrate a cluster resource from OES 2015 or later node configured with SMB2 or later to earlier versions of OES or nodes configured with SMB, the existing connections accessing that resource might not establish automatically.

Cause: The client maintains a runtime cache for each server with which it communicates, whose cached entry indicates the dialect supported by the server.

When the share is on the server configured with SMB2 or later dialect, the client maps the share using that dialect. Even after the server dialect is changed to SMB, the client still attempts to reconnect using SMB2 or later, which the server rejects.

Similarly, when a cluster resource is on an OES 2015 or later node with SMB2 or later, the client maps the resource using that dialect. If the same resource is migrated to nodes with SMB, the client assumes that this server is also SMB2 or later dialect capable and without negotiating with the server attempts to reconnect using SMB2 or later, which the node rejects as it is not SMB2 or later dialect capable.

Action: To resolve this problem, the user must manually disconnect the share and map it again. When doing a fresh mapping, the client first enumerates and negotiates the capability of the server and then connects using the highest dialect that the server is capable of.

11.1.4 Windows Explorer Hangs On Accessing the CIFS Share Path

Cause:

- If the CIFS share path (path to the volume or root directory of the sharepoint) contains millions of objects and you are accessing the shared path using the Windows Explorer, it hangs.
- If a subdirectory inside the CIFS share path contains millions of objects and you are accessing the shared path using Windows Explorer, it hangs as you approach the subdirectory containing millions of objects.

Action: To resolve this issue, ensure that the CIFS share path or any subdirectory inside the CIFS share path does not contain millions of objects.

11.1.5 Salvaged Files are not Displayed in Windows 7 Enterprise Client

Cause: This is due to cache refresh issue in Windows CIFS client. For more information, see https://support.microsoft.com/en-in/kb/2646563.

Action: To view the salvaged files, do the following in Windows Explorer:

- Refresh or
- Perform any file I/O operation.

11.1.6 Automatic Synchronization of Offline Files

Even though manual synchronization is enabled, the offline files and folders on the Windows clients automatically synchronize with the OES server the next time the clients are connected to the network.

OpenText has no plans to fix this issue, because this issue pertains to the functionality of the Windows clients.

11.1.7 Members Of The Default ad-supervisor-group "Domain Admins" Can Map AD-enabled NSS Volumes Although Their Effective Rights on Those Volumes Is Displayed As NULL

Description: If the ad-supervisor-group in NIT is changed from the default group "Domain Admins" to a custom-created group, the effective rights of the members of the default group "Domain Admins" is displayed as NULL. However, those users are able to successfully map and perform administrative activities on those AD-enabled NSS volumes from a CIFS client.

Cause: Modification of ad-supervisor-group do not take effect across subsystems until SEV refresh is performed.

Action: Force the SEV update to occur immediately for all users in the NSS file system by running the `nss /ForceSecurityEquivalenceUpdate` command at the nsscon prompt.

IMPORTANT: You have to perform this action on all the servers where you have changed ad-supervisor-group using the `nitconfig set ad-supervisor-group=<group_name>` command.

Now, verify the Effective Rights of the members of the Domain Admins group. It must display as NULL and those users shouldn't be able to map AD-enabled NSS volumes and perform administrative activities.

11.1.8 Users Are Not Able to Map NSS Resources

Users are not able to map NSS resources shared with them from Windows Explorer.

Mapping might fail for the following reasons:

1. No DNS reverse lookup zone (IPv4 and IPv6) exists for the Active Directory server.
2. No DNS entry exists for the OES server.
   - Ping the OES server to see if it is reachable.
   - Do an `nslookup` for the OES server. An NXDOMAIN error might be returned.

   Create a Host(A) record in the applicable forward lookup zone for the OES server.

   Running the `nslookup` or `dig` commands must return successful results.
3. No DNS entry exists for the OES NSS pool cluster resource.
   - Ping the OES NSS pool cluster resource to see if it is reachable.
   - Do an `nslookup` for the OES NSS pool cluster resource. An NXDOMAIN error might be returned.

   Create a Host(A) record with the NetBIOS name of the cluster resource in the applicable forward lookup zone.

   Running the `nslookup` or `dig` commands must return successful results.
4. CIFS is not configured as the Advertising protocol while creating the cluster pool.

   Create a cluster pool with CIFS as the Advertising protocol.
5. Neither the password policy nor Universal Password is set for the eDirectory user.

   Using iManager, set the password policy (**iManager** > **Passwords** > **Password Policies**) and set the Universal Password (**iManager** > **Passwords** > **Set Universal Password**).

   Check the `/var/log/cifs/cifs.log` file for more details.
6. The NSS resource is not exposed as a CIFS share.

   Using iManager, expose the NSS resource as a CIFS share (**iManager** > **File Protocols** > **CIFS** > **Shares**).
7. Improper mapping of user rights.

   Using NURM, remap the user rights.

   From the server console, run any of the following commands to check the trustee rights for the volume or directory that you are trying to map.

   ```
   rights -f /media/nss/VOLNAME show
   rights -f /media/nss/VOLNAME/DIRNAME show
   ```
8. Wrong user name or password.

The client from which the user is trying to map the shared resource is joined to the Windows domain, and the user exists in both directory services.

For example, the Windows client “win7client” is joined to the domain “acme.com” and the user “susanne” exists in both of the directory services. Susanne can share the same password in both directory services or can have different passwords.

Susanne is assigned as a trustee to the directory “/media/nss/VOL1/mktg.” Using iManager, the directory “mktg” is exposed as a CIFS share with the share name “marketing.”

Using NURM, the Administrator has mapped eDirectory user susanne’s rights to the Active Directory user susanne.

When susanne tries to map the shared resource, the Windows client will first attempt to authenticate the domain user “Susanne,” that is, “acme\susanne.” The client will expect Susanne to provide her Active Directory password. If the passwords are the same in both the directory services, the client will authenticate Susanne using the Active Directory password.

If Susanne specifically wants to map the resource using her eDirectory user credentials, then she can use either of the formats: “\username” or “treename\username” and provide her eDirectory password.

Active Directory User: Map the NSS resource by specifying the host name of the OES server, for example, `\\eurus\marketing`.

eDirectory User: Map the NSS resource by specifying the host name or IP address of the OES server, for example, `\\eurus\marketing` or `\\192.168.100.10\marketing`.

How to check whether the logged-in user is from Active Directory or eDirectory?

From the server console, run the `novcifs -Cl` command to view the connection details.

You can also view the CIFS connection list using OES Remote Manager (NRM) (**Manage CIFS Services** > **Manage Connections**).

11.1.9 CIFS Fails to Write Core Dumps

Description: The CIFS service fails to write core dumps when it crashes.

Cause: Beginning with OES 2015, the setfsuid() system call is used to perform all file system operations with the user context.

The setfsuid() system call introduced in the CIFS daemon resets the process-specific dumpable setting to the system-wide setting `kernel.suid_dumpable` (default value is 0). Therefore, if `kernel.suid_dumpable` is not 2, it might affect the capability of the CIFS process in generating a core if it crashes.

Action: Enable the kernel to write core dumps by executing the command `sysctl -w kernel.suid_dumpable=2`.

For security reasons, core dumps in this mode are not overwritten. This mode is appropriate when administrators are attempting to debug problems.

To additionally make this configuration change persistent over reboots, add the line `kernel.suid_dumpable=2` to the `/etc/sysctl.conf` configuration file.

11.1.10 CIFS Users Unable to Authenticate to OES Server if the Tree has Netware server as the eDirectory Replica Holding Server

Description: OES server fails to authenticate CIFS users if it is joined to a tree wherein a NetWare server holds the master or read/write replicas of CIFS users.

Cause: The NMAS method in OES Linux has been updated; however, it is not updated in NetWare.

Action: Move the master or read/write replicas of CIFS users from the NetWare server to an OES Linux server (OES 2 SP3, OES 11, OES 11 SP1, OES 11 SP2) before you join an OES 2018 or later server to the tree.

11.1.11 Windows Clients Do Not Reflect The Latest File/Folder Operations

Description: Windows 7 and Windows 2008 R2 clients do not reflect the latest file or folder operations such as, create, rename, and salvage.

Cause: This issue is observed when the clients communicate with the server using SMB 2.002 or later protocol versions.

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

11.1.12 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 *Migration Tool Administration Guide*.

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

   For detailed YaST configuration steps, see Section 4.1, "Installing CIFS during the OES Installation," on page 25 and Section 4.2, "Installing CIFS after the OES Installation," on page 27.

11.1.13 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 2023: File Systems Management Guide*.

11.2 CIFS Installation and Configuration

- Section 11.2.1, “CIFS Does Not Start After Installation,” on page 91
- Section 11.2.2, “CIFS Terminates With Schema Not Extended Error After Installation,” on page 91

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).

Action: Restart the OES 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/OES Credential Store) are not stored correctly.

Action: Reconfigure the CIFS proxy user.

11.3 Authentication

- Section 11.3.1, “Configuring AD Server to Support Kerberos Authentication for External Forest Users Using CIFS Client,” on page 91
- Section 11.3.2, “Disabling Kerberos Authentication While the OES Server is being Upgraded to OES 2018 or Later,” on page 92
- Section 11.3.3, “CIFS User Authentication Fails On an NTLMv2 enabled Windows XP Client in the First Attempt,” on page 94
- Section 11.3.4, “Password Has Expired,” on page 94
- Section 11.3.5, “User Can Only See Folders Assigned With Public Trustee Rights,” on page 95
- Section 11.3.6, “Authentication Failed Due to Password Mismatch,” on page 95

11.3.1 Configuring AD Server to Support Kerberos Authentication for External Forest Users Using CIFS Client

Error: User authentication failed and not able to login.

Cause: “Kerberos Forest Search Order (KFSO)” is not configured for SMB client connection.

Action: Enable “Kerberos Forest Search Order (KFSO)” for SMB client connection in the Windows client where the user login and also provide the complete DNS name of the OES CIFS server.

For more information on how to configure KFSO, see the following links:

- https://technet.microsoft.com/en-us/library/dd560670(v=ws.10).aspx
- https://technet.microsoft.com/en-us/library/hh920181(v=ws.10).aspx

11.3.2 Disabling Kerberos Authentication While the OES Server is being Upgraded to OES 2018 or Later

The clients that are already joined to an AD domain and accessing shares on an OES server as eDirectory users will not be able to map the same shares once the OES server is upgraded to OES 2015 (or later) and joined to the AD domain.

This is because, once the OES server is upgraded to OES 2015 (or later) and joined to the AD domain, the clients would start authenticating to OES CIFS service with Kerberos. As Kerberos authentication is supported only for AD users, the CIFS service would authorize the users as AD users while mapping a share. Therefore, mapping of shares would fail until the eDirectory trustee ACLs are migrated to AD users.

However, mapping will continue to work with eDirectory trustees. In this case (during transition phase to OES 2015 or later), to map OES 2015 (or later) shares as eDirectory users from the same clients, the domain administrator must disable Kerberos as a supported authentication mechanism on the OES 2015 (or later) server. Disabling Kerberos forces the clients to authenticate with the OES 2015 (or later) server using NTLM.

- "Disabling Kerberos Authentication" on page 92
- "Authenticating Using NTLM" on page 93
- "Migrating eDirectory Trustee ACLs to Active Directory Users and Groups" on page 93
- "Re-enabling Kerberos Authentication" on page 93
- "Recommendations for a Cluster Resource" on page 94

Disabling Kerberos Authentication

You can disable Kerberos authentications against the OES 2015 (or later) server by removing the Service Principals of the OES 2015 (or later) server.

You must perform the following actions on the DC server of the Active Directory domain to which the OES 2015 (or later) server is joined.

NOTE: You can also remove SPNs using the command-line tool Setspn. For more information, see Setspn on the Microsoft TechNet Library.

---

1. Open the Active Directory Users and Computers MMC (`dsa.msc`).
2. Right-click the computer object of the OES 2015 (or later) server and select **Properties** from the shortcut menu.
3. In the properties window, select the **Attribute Editor** tab.
4. From the **Attributes** list, select **servicePrincipalName**.
5. Click **Edit**.

6 Note down the Values of the Attribute "**servicePrincipalName**". You will require them to re-enable Kerberos.

7 Select a **Value**, and then click **Remove**. Repeat the step until you remove all the Values.

8 Click **OK**.

9 Click **OK** on the Properties window.

Authenticating Using NTLM

If the users are logged in to the clients, they must logout and login again. The changes will be effective only upon the next login.

Now, the clients authenticate to the OES 2015 (or later) server using NTLM. The users can map and access CIFS shares provisioned to them using their eDirectory user credentials.

At this stage, you can map eDirectory trustee ACLs to Active Directory users using NURM.

Migrating eDirectory Trustee ACLs to Active Directory Users and Groups

1 Ensure that pools and volumes are AD-enabled.

For more information, see NSS Management Utility (NSSMU) Quick Reference in the Storage Services File System (NSS) Administration Guide for Linux.

2 Point your browser to `https://<IP address or the host name of the OES2018 SP1 server>/storm`.

3 Specify the user name or FQDN of the eDirectory administrator in the **User Name** field, specify the password, then click **Login**.

4 Connect to Active Directory by specifying the Active Directory administrator or administrator equivalent user credentials.

5 Create User Maps to map eDirectory and Active Directory users and groups.

6 Map User Rights to assign rights to Active Directory users on the NSS resources.

For more information, see NURM (OES User Rights Map) in the NSS AD Administration Guide.

Re-enabling Kerberos Authentication

Once ACL migration is done, you re-enable Kerberos authentication.

On the DC server, using the String Editor, add the Values of the Attribute "**servicePrincipalName**" that you have removed earlier.

NOTE: You can also add SPNs using the command-line tool Setspn. For more information, see Setspn on the Microsoft TechNet Library.

Now, the clients authenticate to the OES server using Kerberos. The users can map and access CIFS shares provisioned to them using their Active Directory user credentials.

Recommendations for a Cluster Resource

1. Join the OES 2015 (or later) node where the cluster resource is running to the Active Directory domain.

   For more information, see Joining the Cluster Node to an Active Directory Domain in the OES Cluster Services for Linux Administration Guide.

2. AD media upgrade the cluster pool and AD-enable the volume(s).

   For more information, see NSS Media Upgrade in the Storage Services File System (NSS) Administration Guide for Linux.

3. Migrate the ACLs through NURM.

   For more information, see NURM (OES User Rights Map) in the NSS AD Administration Guide.

4. Join the cluster resource to the Active Directory domain.

   For more information, see Joining the Cluster Resource to an Active Directory Domain in the OES Cluster Services for Linux Administration Guide.

11.3.3 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.

11.3.4 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.

11.3.5 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.

11.3.6 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 121.

11.4 Startup

- Section 11.4.1, "CIFS Is Not Starting," on page 95

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 **OES 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 4.2, “Installing CIFS after the OES Installation,” on page 27.

11.5 Migration

- Section 11.5.1, “CIFS Does Not Start After Migration Is Completed On The Target server,” on page 96
- Section 11.5.2, “After Migration, the CIFS Server Does Not Come up on the Target Server by Default,” on page 96

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

- Section 11.6.1, “Unable to See the Contents of the Target That a DFS Junction Points To,” on page 96
- Section 11.6.2, “The Mac Client does not Display a Complete List of Available Shares,” on page 97
- Section 11.6.3, “Copying Multiple Large Files using Finder from a Mac OS X Client to an OES CIFS Share Fails,” on page 97

11.6.1 Unable to See the Contents of the Target That a 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 with SMB V1 dialect 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 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 CIFS Server. The CIFS server must be restarted after this option is modified.

11.7 DFS

- Section 11.7.1, “Unable to Resolve DFS junctions from Windows Clients,” on page 97
- Section 11.7.2, “Junction Target Changes Require DFSUTIL Command Execution to Clear the Cache,” on page 98
- Section 11.7.3, “Unable To Access DFS Junctions On a CIFS Share From the Windows Client,” on page 98
- Section 11.7.4, “After Modifying the Junction Target, Accessing the Junction Still Leads to the Old Target,” on page 98

11.7.1 Unable to Resolve DFS junctions from Windows Clients

Cause: You cannot access DFS junctions if you login to the desktop as Active Directory user and map the CIFS drive as eDirectory user.

Action: To access DFS junctions, it is recommended to map the CIFS drive with the same Active Directory user credentials as you login in the Windows workstation.

11.7.2 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.

11.7.3 Unable To Access DFS Junctions On a 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.

11.7.4 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

- Section 11.8.1, “Files Deleted from Redirected Folder are Not Available in NFARM Salvage Purge List on Windows Clients,” on page 99
- Section 11.8.2, “After Successful Folder Redirection, Multiple Login or Logout Requests Observed in Log File,” on page 99
- Section 11.8.3, “Executing --join or --leave-domain in novell-ad-util Fails with an Error “Insufficient rights to do the operation, perform kinit.”,” on page 99
- Section 11.8.4, “Not Able to Change Authentication Mode in iManager,” on page 100

- Section 11.8.5, “Offline Files Synchronization Fails,” on page 100
- Section 11.8.6, “Synchronization of Offline Files Caching Fails with an Error “The process cannot access the file because it is being used by another process.”,” on page 100
- Section 11.8.7, “Windows or Mac Unable to Resolve the NetBIOS Name of the CIFS Server,” on page 100
- Section 11.8.8, “Temporary Files Created On the OES Server By MS Office 2010 Are Not Deleted,” on page 102
- Section 11.8.9, “Users Created Using UID Qualifier Cannot Access CIFS Shares,” on page 102
- Section 11.8.10, “Troubleshooting NIT,” on page 102

11.8.1 Files Deleted from Redirected Folder are Not Available in NFARM Salvage Purge List on Windows Clients

Cause: When a file from a redirected folder is deleted by pressing Del or from the **File** menu, the file is moved to the folder specific recycle bin rather than completely deleting it. This is a Windows client behavior.

Action: The Windows client behavior can be changed by using the registry setting `NukeOnDelete` at `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\KnownFolder`.

Set `NukeOnDelete (REG_DWORD) 0 (move to recycle bin) or 1 (delete)` to `1`. The files will not be moved to recycle bin but will be completely deleted and available in the NFARM salvage purge list.

11.8.2 After Successful Folder Redirection, Multiple Login or Logout Requests Observed in Log File

The Windows client sends multiple login or logout requests based on the number of CIFS connections to the OES server and this gets logged in the `audit.log` or `messages` files. This is a Windows behavior observed after successful folder redirection operation.

11.8.3 Executing --join or --leave-domain in novell-ad-util Fails with an Error “Insufficient rights to do the operation, perform kinit.”

Cause: The cached Kerberos credentials does not have supervisor rights to add or remove OES objects from the computer directory.

Action: Execute `kinit` to obtain the Kerberos credentials of an AD supervisory user. For example, `kinit Administrator@EXAMPLE.COM`.

Where “Administrator” is domain admin or an user with sufficient rights and “EXAMPLE.COM” is the AD domain.

NOTE: Ensure that the AD domain name is in capitals.

11.8.4 Not Able to Change Authentication Mode in iManager

If SMB2 or SMB3 is the current dialect, iManager plug-in prevents changing the authentication mode from 'Local' to 'Domain (Passthru)'. It throws the error message, "The parameters to CIFS_SetServerConfiguration are not valid for this server type".

11.8.5 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.

11.8.6 Synchronization of Offline Files Caching Fails with an 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 5.11, “Enabling Offline Files Support,” on page 54 and Section 13.3.5, “Oplocks,” on page 111.

11.8.7 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, 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 Client for Open Enterprise Server.

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**.

11.8.8 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.

11.8.9 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.

11.8.10 Troubleshooting NIT

- "Unspecified GSS failure. Minor code may provide more information (Ticket expired)" on page 102
- "Invalid UID Obtained" on page 102
- "Unable to fetch tree name, error:11" on page 103

Unspecified GSS failure. Minor code may provide more information (Ticket expired)

Description: Ticket Granting Ticket (TGT) expiration errors are seen if the NIT setting `ad-tgt-refresh-timeout` is more than the "Maximum lifetime for a user ticket" in the Kerberos policy of the domain.

Action: To avoid TGT expiration errors, ensure that the `ad-tgt-refresh-timeout` value is less than Active Directory TGT expiration time.

Invalid UID Obtained

Description: If the Active Directory user is denied access possibly the user is not assigned a valid UID.

Cause: Run the `nitconfig get` command and check if `ad-uid-generate-mode` parameter is set to 0. Setting this parameter to 0 means NIT operates in Fetch mode for Active Directory users and tries to fetch UIDs for those users from Active Directory. If the users do not have UIDs assigned in Active Directory you might encounter this error.

Action: When you choose to fetch UID for Active Directory users, NIT fetches the `uidNumber` attribute set in Active Directory for all the Active Directory users. If UID is not set for a particular user, that user cannot access NSS file systems. If you are configuring NIT in fetch mode for Active Directory users, ensure that the Active Directory users who require access to NSS filesystems have

UID numbers set in the Active Directory. Add the uidNumber attribute explicitly to the Global Catalog server as it is not part of default attributes. For more information about replicating UID numbers to the Global Catalog server, refer to the Microsoft Support website.

Unable to fetch tree name, error:11

Description: eDirectory is down and NIT is not able to fetch tree name.

Action:

1. Start eDirectory by running the `rcndsd start` command.
2. Start NIT by running the `rcnovell-nit start` command

12 Security Guidelines for CIFS

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

- Section 12.1, “Using Credentials,” on page 105
- Section 12.2, “Using OES Credential Store,” on page 105
- Section 12.3, “Using VPN Connections,” on page 105
- Section 12.4, “Using SMB Signing,” on page 105
- Section 12.5, “Other Security Considerations,” on page 105

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 OES Credential Store

We recommend that you select OES Credential Store 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 36.

12.5 Other Security Considerations

OES 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.

- Section 13.1, “eDirectory,” on page 107
- Section 13.2, “NSS,” on page 108
- Section 13.3, “CIFS,” on page 110
- Section 13.4, “NCP,” on page 112

13.1 eDirectory

- Section 13.1.1, “FLAIM Database,” on page 107
- Section 13.1.2, “Thread Pool,” on page 107

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 and later, 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 Tuning Guide.

13.2 NSS

- Section 13.2.1, “IDCacheSize,” on page 108
- Section 13.2.2, “Minimum Buffer Cache,” on page 109
- Section 13.2.3, “Setting the Name Cache Size,” on page 109

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 Storage Services File System (NSS) Administration Guide for Linux.

13.3 CIFS

- Section 13.3.1, “Maximum Cached Subdirectories Per Volume,” on page 110
- Section 13.3.2, “Maximum Cached Files Per Volume,” on page 110
- Section 13.3.3, “Subtree Search,” on page 111
- Section 13.3.4, “Information and Debug Logs,” on page 111
- Section 13.3.5, “Oplocks,” on page 111
- Section 13.3.6, “Leasing,” on page 111
- Section 13.3.7, “Cross Protocol Locks,” on page 112
- Section 13.3.8, “SMB Signing,” on page 112
- Section 13.3.9, “Dynamic FID Pool,” on page 112

Based on the number of files and folders in a volume, you can configure the cache limits. If the volume has millions of files and folders, the default settings do not hold good. Tune the following cache settings discreetly.

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 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 larger 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.

13.3.3 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.

If you enable subtree search, it is recommended to enable Invalid User cache feature.

```
-UT TIMEOUT-PERIOD, --block-invalid-users --timeout-period=TIMEOUT-PERIOD
```

Enables CIFS 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.

Specifies the amount of time a user should be considered as invalid to ignore authentication requests.

Specify the timeout period in minutes and the range should be between 0 and 525600.

By default, caching the invalid user logins is disabled.

13.3.4 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 [--log-level debug]`

To enable or disable the Info Log, use the following command: `novcifs [--log-level info]`

13.3.5 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).

13.3.6 Leasing

Leasing available with the SMB 2.1 or later is an enhancement to Oplocks. It provides better performance compared to Oplocks by increasing the amount of caching and by reducing the number of cache break. This option is enabled by default. Leasing can be enabled only if Oplocks is enabled.

Recommendation: For better performance, leasing should be enabled.

```
novcifs --leasing=yes|no
```

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.

13.3.9 Dynamic FID Pool

At any point in time, by default, the CIFS service allows 65k files on the server to be in open state irrespective of the number of user sessions established. You can increase this limit to 600k by enabling the dynamic FID pool option. Enabling this option allows each user session to open up to 65k files, with a maximum number of open files not exceeding 600k collectively from all the user sessions established.

13.4 NCP

- Section 13.4.1, “Thread Pools,” on page 112
- Section 13.4.2, “Cache Settings,” on page 113

13.4.1 Thread Pools

To manage the thread pools in NCP, see Managing NCP Threads in the 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 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) server.

To access the man page, 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`* `-c` *`COMMENT`*`, --share --add --path=`*`PATH`* `--name=`*`SHARENAME`* `--comment=`*`COMMENT`* `]`

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

`[-sap` *`PATH`* `-n` *`SHARENAME`* `-c` *`COMMENT`* `-v` *`VIRTUALSERVERFDN`*`, --share --add --path=`*`PATH`* `--name=`*`SHARENAME`* `--comment=`*`COMMENT`* `--vserver=`*`VIRTUALSERVERFDN`*`]`

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

`[-s --enable-encryption=yes|no -n` *`SHARE-NAME`*`, --share --enable-encryption=yes|no --name=`*`SHARE-NAME`*`]`

`[-s --folder-redirection=yes|no -n <share_name>]`

`[-s --atm-backup=yes|no -n SHARENAME, --share --atm-backup =yes|no --name SHARENAME]`

`[-s --mfa=yes|no -n SHARENAME, --share --mfa=yes|no --name SHARENAME]`

`[-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 V`*`IRTUALSERVERFDN`* `-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]

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

[--list-servers]

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

[--dialect=SMB|SMB2|SMB3]

[--user-quota-sync <primary_volume>]

[--user-quota-sync <primary_volume> --percent <percentage>]

[--change-notify yes|no]

[--enum-shares-over-nullsession=yes|no]

[--check-share-visibility-rights=yes|no]

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

[--negotiate-ntstatus=yes|no]

[--dfs-support=yes|no]

[--dns-suffix=DNS-SUFFIX]

[--display-user-addr=yes|no]

[--alternate-data-stream-enabled=yes|no]

[--disable-smbv1-sessions=win-mac|mac|none|all]

```
[--encrypt-data=yes|no]
[--reject-unencrypted-access=yes|no]
[--log-level error|debug|info]
[--dos-names=yes|no]
[--disable-ntlmssp=yes|no]
[--block-unmanaged-cis-reads=yes|no]
[--leasing=yes|no]
[--directory-leasing=yes|no]
[--zerocopy=yes|no]
[--large-mtu=yes|no]
[--mfa=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 -c COMMENT | --share --add --path=PATH --
name=SHARENAME --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 -c COMMENT -v VIRTUALSERVERFDN | --share --add --path=PATH --name=SHARENAME --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 SMB 3.0 Encryption at Share Level

`-s --enable-encryption yes|no -n SHARE-NAME, --share --enable-encryption=yes|no --name=SHARE-NAME`

Enables or disables the encryption at the share level. If encryption is enabled at global level using the option `--encrypt-data=yes|no`, you need not enable encryption again at the share level. You can use this option to enable encryption for a specific share when encryption is disabled at global level. If this option is enabled, all the sessions established from the clients, which support encryption, to the specified share are encrypted. By default, this option is disabled.

Example:

`novcifs -s --enable-encryption yes -n VOL1` enables SMB encryption for the share named VOL1.

Enabling or Disabling Folder Redirection

`-s --folder-redirection=yes|no -n <share_name> --share --folder-redirection =yes|no --name=SHARENAME`

Enables or disables the file share to host the redirected folders. By default, this option is disabled.

Enabling or Disabling ATM Backup at Share Level

`-s --atm-backup=yes|no -n SHARENAME, --share --atm-backup =yes|no --name= SHARENAME`

Enables or disables share to be Apple Time Machine (ATM) backup target. Enable this option to

let ATM running on the Mac clients to backup their data to the specified share. This feature works only when --leasing is enabled with SMB3 or later connections.

Enabling or Disabling MFA at Share Level

```
-s --mfa=yes|no -n SHARENAME, --share --mfa=yes|no --name SHARENAME
```

Enables or disables MFA at share level. If enabled, access to the share requires MFA. By default, this option is disabled.

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. By default, it is disabled.

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.

By default, the LMCompatibilityLevel is set to 0.

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 File Compression

```
novcifs [--compression=yes|no]
```

Enables or disables the compression of files as they transfer over the network.

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` or `systemctl restsrt novell-cifs.service` 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. By default, caching the invalid user logins is enabled.

```
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.

NOTE: Use special USER-NAME "MachineAccounts" to add machine accounts ending with the $ symbol as default invalid users. But, if there are valid user names ending with the $ symbol, then do not use the special USER-NAME "MachineAccounts". When "MachineAccounts" is added as default invalid users, if a machine account tries to log in as an eDirectory user, the authentication request is denied. If it tries to log in as an Active Directory user, the tree connect request is denied.

Adding "MachineAccounts" to the permanent list of blocked user accounts makes cifsd service to deny Session Setup requests for computer accounts, without attempting to resolve or find the account in eDirectory which prevents exhaustion of eDirectory, when repetitive SMB authentication requests for a computer account is generated by Windows (background) processes that run as Local System account.

This makes cifsd service to deny the Tree Connect requests from Active Directory computer accounts without verifying the effective rights of such accounts with NSS, which prevents file system access performance degradation when repetitive attempts to access a CIFS share are generated by Windows (background) processes that run as Local System account.

This also avoids error messages in cifs log related to access failures for computer accounts.

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]
```

Monitoring CIFS Health Status

```
novcifs --get-health-status
```

Displays the health status of CIFS service. If the status is unhealthy, then the cause for the status is also displayed with the status.

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 6, “CIFS Monitoring and Management,” on page 57.

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.

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

In releases earlier than OES 2015, 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 2015 (or 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 non OES 2015 (or later) nodes 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.
```

Toggling between SMB Versions

Sets the highest dialect for the CIFS server to communicate with the clients. Toggling between the dialects may cause difference in server behavior. Restart the CIFS service any time you modify this option.

```
novcifs --dialect=SMB|SMB2|SMB3
```

SMB Sets the highest dialect supported to NT LM 0.12 (SMB v1).

SMB2 Sets the highest dialect supported to SMB 2.1 (SMB v2). SMB1 and SMB2 clients can connect to the server.

SMB3 Sets the highest dialect supported to SMB 3.00 (SMB v3). SMB1, SMB2, and SMB3 clients can connect to the server.

By default, SMB v3 option is enabled.

Beginning with OES 2018 SP3, the SMB v1 sessions are disabled by default. To enable all SMB v1 sessions, set the option `--disable-smbv1-sessions=none`.

Synchronizing Users Quotas

Synchronizes the users quotas from the primary volume to the secondary volume of a DST shadow volume pair.

```
--user-quota-sync <primary_volume>
```

Duplicates all of the user quotas that are set currently on the specified primary volume to the secondary volume.

```
--user-quota-sync <primary_volume> --percent <percentage>
```

Duplicates all of the user quotas that are set currently on the specified primary volume as a specified percentage to the secondary volume. The percentage value must also be specified after the volume name.

A percent value of 100 is a one-to-one quota assignment. A percent value of 50 assigns a quota that is one-half the size of the quota set on the primary volume. A percent value of 200 assigns a quota that is twice the size of the quota set on the primary volume.

Enabling or Disabling File System Change Notifications to the Clients

```
--change-notify yes|no
```

When enabled, the client gets notifications about the changes happening on the directory which is currently being browsed or used through the Windows Explorer or Mac finder. These notifications enable the client to automatically refresh the Windows Explorer or Mac finder. The users need not press F5 to get the updated view as they will always be viewing the actual contents of the file system.

The client will be notified when one or more of the following events occur: A file or a folder is created, deleted, renamed, or moved, and metadata is changed.

Impact of enabling file system change notifications: Along with responding to the client's requests, the file server will also have to notify about every change happening on the directory to the client even if the change was done by the same client. It does increase the load on server.

Performance can be sluggish particularly when multiple users accessing or operating on the same directory.

Impact of disabling file system change notifications: Certain applications like Windows Explorer (Windows), Mac Finder, etc., expect change notifications feature to be supported or enabled. Else they end up in continuously querying the server about changes with humongous number of requests per second. The client tries to pull changes from the server and this might impact the performance of the server.

However, you can also add or modify the following Windows registry keys on the Windows client side so as to not let the client continuously query about the changes on the server.

Location: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

Key 1: NoRemoteChangeNotify (DWORD type with value set to 1)

Key 2: NoRemoteRecursiveEvents (DWORD type with value set to 1)

NOTE: By doing so, users are be forced to press F5 to get the updated view or changes on the file system. In addition, the same registry settings have to be applied on all the client machines.

IMPORTANT: The SMB client on SLED machines does not support the Change Notifications feature. Therefore, the changes on the OES file system will not be automatically reflected in the file browsers such as Nautilus.

Similarly, all client platforms do not request the server to send change notifications if the users browse using the command line.

Enabling or Disabling Enumeration of Shares Over Null Session

`--enum-shares-over-nullsession=yes|no`

Enables or disables enumeration of shares over a null session. By default enumeration of shares over a null session is enabled. If GUEST access is enabled, enumeration of shares over a null session is still allowed even if `enum-shares-over-nullsession` is disabled.

If `--check-share-visibility-rights` is enabled, it takes precedence and null sessions do not list any shares. Only shares with Public rights are displayed.

Enabling or Disabling Display of Shares Depending on Trustees

`--check-share-visibility-rights=yes|no`

Enables or disables the display of shares depending on the trustee rights of the user or group.

On enabling this option, an user can view only those shares (local or cluster resource) that he or she has trustee rights on and also the shares with Public rights. To view the shares a user must be added as a user or group trustee.

By default, this option is disabled.

Setting Oplock Break Acknowledgement Timeout Period

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

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 or lease on a file.

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

Enabling or Disabling Negotiating NTSTATUS Capability

`--negotiate-ntstatus=yes|no`

Enables or disables negotiating NTSTATUS capability of the CIFS server.

If this option is enabled, server will set NTSTATUS capability bit in Negotiate Protocol response. This is required for certain SMBv1 clients to proceed with the session setup especially when extended security mechanisms are used. By default, this option is disabled. It is recommended to enable this option only when the client fails to connect to OES because of NTSTATUS capability.

If this option is enabled, CIFS server will set NTSTATUS capability bit during the negotiation phase. This is required for certain type of clients like printers to connect to the CIFS server using SMBv1 as the dialect. By default, this option is disabled. It is recommended to enable this option only when certain type of clients like printers fail to connect to the CIFS server.

Enabling or Disabling DFS Support

`--dfs-support=yes|no`

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

Setting DNS Suffix

`--dns-suffix=DNS-SUFFIX`

Sets DNS suffix to be used in DFS referral target node server name. By default, target node server name is only the NetBIOS name without any DNS suffix.To clear the DNS suffix configuration, set an empty string.

Updating Client IP Address Details

`--display-user-addr=yes|no`

Enables or disables updation of client IP address details for the logged in user in the eDirectory user object. Before enabling this option, the common proxy user must be given write permission on the Network Address attribute at the user level or at the parent container level. By default, this option is disabled.

Enabling or Disabling Alternate Data Stream

`--alternate-data-stream-enabled=yes|no`

Enables or disables the alternate data stream. By default, this option is disabled.

Disabling SMB v1 sessions

`--disable-smbv1-sessions=win-mac|mac|none|all`

Disables the SMB v1 session from the specified clients.

`win-mac` disables SMB v1 session from the Windows and Mac OS X clients.

`mac` disables SMB v1 session from Mac OS X clients.

`none` does not disable SMB v1 sessions from any of the clients.

`all` disables SMB v1 session from all clients.

NOTE: NURM and NFARM in Mac works only over SMB v1.

Enabling or Disabling SMB 3.0 Encryption at Global Level

`--encrypt-data=yes|no`

Enables or disables the global level encryption, which is applicable to all the shares on the server. If this option is enabled, all the sessions established from the clients, which support encryption, to the server are encrypted. By default, this option is disabled.

Example:

`novcifs --encrypt-data=yes` enables SMB encryption for all the shares on the server.

Selecting a Cipher among the Supported Ciphers

`[--preferred-cipher=AES-128-GCM|AES-128-CCM|AES-256-GCM|AES-256-CCM|NONE]`

CIFS supports AES-256-GCM and AES-256-CCM cryptographic suites for SMB 3.1.1 encryption. The server negotiates these advanced cipher methods when connecting to the client. AES-128-GCM andAES-128-CCM cryptographic suites are still supported for SMB 3.1.1.

`AES-128-GCM` sets AES-128-GCM as a cipher for encryption.

`AES-128-CCM` sets AES-128-CCM as a cipher for encryption.

`AES-256-GCM` sets AES-256-GCM as a cipher for encryption.

`AES-256-CCM` sets AES-256-CCM as a cipher for encryption.

Example: `novcifs --preferred-cipher=AES-128-GCM|NONE` sets AES-128-GCM as prefered cipher.

SMB Multichannel Operations

SMB multichannel is an SMB3.0 feature that increases network performance and the availability of file servers. SMB multichannel operation is allowed by default over the network interface which holds the IP address used for mapping the share. Additional interfaces can be enabled for smb multi-channel operation using this option.

Enabling and Disabling SMB Multichannel:

`novcifs --multi-channel={yes|no}`

Enables or disables SMB multichannel operations.

Adding a multi-channel interface name:

`novcifs --multi-channel-interface --add --interface-name=<NETWORK-INTERFACE-NAME>`

Allows you to add additional interfaces for smb multi-channel operation.

Removing a multi-channel interface name:

`novcifs --multi-channel-interface --remove --interface-name=<NETWORK-INTERFACE-NAME>`

Allows you to remove an interface from smb multi channel support.

Displays the list of all the multi-channel interfaces:

`novcifs --multi-channel-interface --list`

Displays the list of all the interfaces which are enabled for smb multi channel operation.

Enabling or Disabling Unencrypted Access to the Share

`--reject-unencrypted-access=yes|no`

Enables or disables the unencrypted access to the shares exported by the server. If this option is disabled, the clients that do not support encryption can also access the encryption enabled shares. By default, this option is enabled.

Example:

`novcifs --reject-unencrypted-access=no` allows SMB clients that do not support encryption to access the encrypted shares.

Setting the Log Level

`--log-level error|debug|info`

Sets the log level for the server to log messages in. By default, the log level is set to `error`.

`error` logs the critical, error, warnings, and events log.

`debug` logs all the debug, info, critical, error, warnings, and events log.

`info` logs all the info, critical, error, warnings, and events log.

Enabling or Disabling DOS File Name Support

`--dos-names=yes|no`

Enables or disables the DOS file name support. By default, this option is enabled. When this option is disabled, file operations using DOS file name is prevented. Disabling it improves the CIFS server performance especially during directory enumeration.

Enabling or Disabling NTLMSSP Authentication

`--disable-ntlmssp=yes|no`

Disables or enables the NTLMSSP authentication. Setting this option to yes avoids the false NTLMSSP login attempts in an AD only environment. By default, NTLMSSP authentication is enabled.

NOTE: If NTLMSSP authentication is disabled, an eDirectory anonymous (guest) login or null login cannot be performed. But an AD guest login can be performed.

Managing CIS Reads

`--block-unmanaged-cis-reads=yes|no`

Disables or enables users with unmanaged workstation (CIS Client not installed on the workstation) from accessing files uploaded to the cloud. If this option is enabled, only those users with a managed workstation (CIS Client installed on the workstation) can access the files uploaded to the cloud. If this option is disabled, users with managed or unmanaged workstation can access the files uploaded to the cloud. By default, this option is disabled. Restart the CIFS server any time you modify this option.

Leasing

`--leasing=yes|no`

Enables or disables the file leasing for SMB 2.1 or later connections. Leasing is an enhancement to legacy oplocks, which facilitates better file caching by clients, and thereby improves the overall performance. By default, this option is enabled. Leasing works only if oplock is enabled. To configure the lease break timeout, use the `--oplock-lease-break-ack-timeout` option.

Directory Leasing

`--directory-leasing=yes|no`

Enables or disables directory leasing for SMB 3.0 or later connections. Directory leasing enables clients to cache the meta data of directories and thereby improves the overall performance.

By default, this option is enabled. Directory Leasing works only if oplock and leasing are enabled. To configure the lease break timeout, use the `--oplock-lease-break-ack-timeout` option.

Enabling or Disabling Large MTU

`--large-mtu=yes|no`

Enables or disables large MTU support. The Maximum Transmission Unit (MTU) is the size of the biggest data unit that can be transmitted in a single SMB2 packet on a network. With large MTU, maximum data unit size can be up to 1 MB as opposed to 64 KB of a normal MTU. Large MTU support enables a server to support multi-credit operations and is available in SMB 2.1 or later. By default, this option is disabled.

Enabling or Disabling MFA at Server Level

`--mfa=yes|no`

Enables or disables MFA at server level. If this option is enabled, access to any share on the server requires MFA. By default, this option is disabled.

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.

`/usr/sbin/rcnovell-cifs`

Initialization script for CIFS. You can use systemctl commands or rcnovell-cifs commands for start, stop, and restart operations.

`/var/log/cifs/cifs.log`

CIFS server log file.

Examples

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

B Comparing CIFS on NetWare and CIFS on OES 2018 or Later

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

Table B-1 *CIFS services on NetWare and OES 2018 or later*

Service	NetWare	OES 2018 or later
Kerberos Authentication for Active Directory Users	No	Yes
Extended Security Support (NTLMSSP) for eDirectory Users	No	Yes
SMB 2.0 (SMB 2.002) Verb Compliance	No	Yes
Direct hosted "NetBIOS-less" SMB traffic over port 445 (TCP)	No	Yes
File System Change Notifications Support	No	Yes
Sync user quotas between primary and shadow volumes for eDirectory and Active Directory users using `novcifs` command options	No	Yes
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

Service	NetWare	OES 2018 or later
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

C Configuration and Log Files

Table C-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 C-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 an 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.