Open Enterprise Server 2015 SP1
Novell Samba Administration Guide

June 2016

Novell

Legal Notices

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

Contents

About This Guide

This guide describes the Novell implementation of Samba included in Open Enterprise Server (OES) 2015 SP1, and includes instructions for performing basic configuration and setup tasks.

This guide includes the following sections:

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with OES 2015 SP1. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this and other guides for OES, visit the OES 2015 Documentation Web site (http://www.novell.com/documentation/oes2015/).

Additional Documentation

Samba is an Open Source initiative and has extensive documentation on the Web, including that found at Samba.org (http://www.samba.org).

OES and SLES Platform References in This Guide

All references to OES 2015 SP1 and SLES 11 in this guide refer to the versions of those products that are released with the version of OES 2015 SP1 indicated in the guide title. For example, the release of OES 2015 SP1 included SLES 11 SP4, and the references to SLES 11 refer to SLES 11 SP4 unless otherwise indicated. The Support Pack version of a release is only mentioned in those cases where the distinction is important, for example, when a support pack has a new feature not available in earlier versions.

1 Overview of Samba

Samba is an open source software suite that lets Linux and other non-Windows servers provide file and print services to clients that support the Microsoft SMB (Server Message Block) and CIFS (Common Internet File System) protocols.

This guide focuses on the Samba implementation in Open Enterprise Server (OES) 2015 SP1. For more information about the Samba open source initiative, see Section 1.4, "Web Links," on page 12.

This section covers the following topics:

- Section 1.1, "Samba Basics," on page 9
- Section 1.2, "Samba Functionality in OES 2015 SP1," on page 10
- Section 1.3, "Samba and NSS Volumes," on page 12
- Section 1.4, "Web Links," on page 12

1.1 Samba Basics

The open source Samba software is included as part of SUSE Linux Enterprise Server (SLES) 11 SP4, which is the base operating system for OES 2015 SP1 services. When working with Samba in an OES 2015 SP1 environment, it is important to understand the basic features of Samba and how Samba is configured on OES servers. This section provides an overview of Samba's basic functionality. Section 1.2, "Samba Functionality in OES 2015 SP1," on page 10 explains what is different when Samba is configured for OES.

Using Samba, a Linux machine can be configured as a file and print server for clients that support the SMB and CIFS protocols. Client operating systems that support SMB/CIFS include Windows, OS/2, and Mac OS X. These clients can use their familiar native interfaces to access files on OES servers. For example, Samba lets Windows users access files on an OES server by using Windows Explorer, My Network Places, and mapped drives.

The Samba server software consists of two daemons: smbd for SMB/CIFS services and nmbd for naming services. SUSE Linux includes a kernel module that allows the integration of SMB resources at the Linux system level. You do not need to run any daemon for Samba clients. SUSE Linux includes the smbclient utility, which is a simple FTP-like SMB client that can be used on Linux systems to connect to remote SMB shares, transfer files, and send files to remote shared printers.

Samba servers provide disk storage space to their clients by means of shares. A share is a directory on the server that is exported as a mount point and accessed by an assigned share name. The share provides access to the directory and its subdirectories. Shares can also be created for Windows printers, which clients can also access by their assigned share names.

Samba shares and other configuration options are defined in the `smb.conf` file located in the `/etc/samba` directory. In a non-OES environment, you can edit the configuration file directly, use the management tools SUSE Linux provides in YaST, or use the browser-based SWAT (Samba Web Administration Tool) interface that is included with Samba.

In a non-OES environment, authentication to Samba shares is controlled by means of the smbpasswd tool. This tool is used to manage user accounts and passwords on the Samba server.

Samba version 3 also includes support for NT-style domain authentication. In a non-OES environment, the Linux server running Samba can be configured as a domain controller.

For more information about configuring and managing Samba in a non-OES environment, see the *SLES 11 Administration Guide* (http://www.suse.com/documentation/sles11/book_sle_admin/data/cha_samba.html).

1.2 Samba Functionality in OES 2015 SP1

This section covers the following topics:

- Section 1.2.1, "Samba Differences in OES 2015 SP1," on page 10
- Section 1.2.2, "Software Installed with the Novell Samba Pattern," on page 11
- Section 1.2.3, "Other OES Services That Work with Samba," on page 11
- Section 1.2.4, "Samba Users Are Both Windows and eDirectory Users," on page 11

1.2.1 Samba Differences in OES 2015 SP1

The open source Samba software described in earlier sections is installed automatically on every SLES 11 SP4 server. OES 2015 SP1 uses this base Samba software, but configures it differently and installs additional software to take advantage of enhanced services available in OES 2015 SP1.

The main differences between base Samba on SLES 11 SP4 and OES 2015 SP1 are:

- Samba on OES 2015 SP1 is configured to use the eDirectory LDAP server for secure user authentication.
- In order for eDirectory users to be able to access shares on an OES 2015 SP1 server, they must be created in a container with a Samba-compliant password policy assigned to it and be members of a group that has been properly Linux-enabled.

  OES 2015 SP1 includes a new Samba Management plug-in for iManager that simplifies the process of enabling users for Samba access by automatically making users members of the default Samba Users group that is created for every OES 2015 SP1 Samba server. See Chapter 8, "Managing Samba Servers, Shares, and Users," on page 65 for more information.

- With OES 2015 SP1, Samba shares can be created on Novell Storage Services (NSS) volumes or on NetWare Core Protocol (NCP) volumes on Linux POSIX file systems. This allows access to be controlled by the Novell Trustee Model, which offers more robust and flexible security.
- OES 2015 SP1 does not support Samba running in NT 4 domain mode as either a primary or backup domain controller.
- Samba on OES 2015 SP1 should be managed by using the tools provided with OES, such as the iManager Samba Management plug-in, and not the tools available in SLES 11, such as the YaST Samba Server tool and the browser-based SWAT utility.
- Although Samba can also provide Windows print services, OES print services are provided by iPrint, not by Samba.

A general overview of Samba, in context with other file services in OES, is provided in "Novell Samba" in the *OES 2015 SP1: Planning and Implementation Guide*.

1.2.2   Software Installed with the Novell Samba Pattern

In an OES 2015 SP1 server installation, the Novell Samba pattern is available for selection in the OES Services category. Selecting this pattern installs the following packages:

- novell-samba-cim (Samba Management Loadable CIM Module)

  This package is the CIM (Common Information Model) provider required for the Samba Management plug-in for iManager.
- novell-samba-config (Samba Config for Open Enterprise Server)

  This package configures Samba for integration with NetIQ eDirectory.
- yast2-samba-server (YaST2 Samba Server Configuration)

  This package contains the YaST2 component for Samba server configuration.

Selecting the Novell Samba pattern automatically selects Novell Backup/Storage Management Services (SMS), Novell Linux User Management (LUM), and Novell Remote Manager (NRM).

1.2.3   Other OES Services That Work with Samba

Depending on what you want to do with Samba, you can select other patterns from the OES Services category:

- Novell Cluster Services (NCS): Select this pattern if you want to include this server in a high availability cluster.
- NetIQ eDirectory: Samba in OES 2015 SP1 requires eDirectory.
- Novell iManager: To manage Samba shares and users, Novell iManager must be installed on at least one server in the network.
- Novell NCP Server/Dynamic Storage Technology: Select this pattern if you want to create NCP volumes on NSS or on a Linux POSIX file system such as Reiser, Ext3, or XFS.
- Novell Storage Services (NSS): Select this pattern if you want to create Samba shares on NSS volumes. (NCP Server is automatically selected when you select this pattern.)

IMPORTANT: You cannot select Novell Domain Services for Windows along with the Novell Samba pattern. Domain Services for Windows requires its own specialized configuration of the base Samba software, which is incompatible with the standard OES 2015 SP1 configuration. For more information, see the *OES 2015 SP1: Domain Services for Windows Administration Guide*.

1.2.4   Samba Users Are Both Windows and eDirectory Users

As stated earlier, the purpose of Samba in OES is to allow Windows client users to access data directories on OES servers.

Both the Windows workstations and the OES servers require authenticated access. On the Windows workstation, users log in using their Windows usernames and passwords. When they log in to the OES server, they use their eDirectory usernames and passwords. Samba requires that these usernames and passwords match.

In other words, the Windows usernames on your network workstations and the eDirectory usernames you create for Samba access must be the same and must have the same password.

For example, if you have a Windows workstation user with the username of jsmith and password abcd*1234 that you want to be a Samba user, you must create an eDirectory user with the username of jsmith and password abcd*1234.

One advantage of Samba is that Windows users who have matching eDirectory accounts can access shares on OES 2015 SP1 servers without having the Novell Client for Windows installed on the workstation. After authenticating to Windows, users can see the Samba shares they have rights to access via native Windows interfaces, such as Windows Explorer and My Network Places.

As long as the Novell NCP Server software is installed on the OES 2015 SP1 server, Windows users that have the Novell Client software installed can continue to access files they have rights to on the Linux server via standard Novell interfaces, such as drive mappings.

1.3 Samba and NSS Volumes

You should be aware of the following when using Samba to access NSS volumes on an OES 2015 SP1 server.

1.3.1 Samba on NSS Can Be a Good Combination for Performance

If you will have more than 2,000 files and folders accessed through Samba, you should consider using NSS as the underlying file system. Above that number, Samba on NSS outperforms Samba on traditional Linux volumes, such as Ext3, ReiserFS, or XFS. As you add more files and directories above the 2,000 mark, the performance advantage increases.

1.3.2 Share Access Requires NSS Trustee Rights

Samba-enabled users cannot access an NSS volume using Samba until they are granted NSS trustee rights to the files and directories on that volume. Rights are automatically granted for home directories on NSS volumes that are created in iManager. For other work directories that you want to set up as Samba shares, you must grant users the appropriate access rights.

OES 2015 SP1 provides numerous tools for granting NSS trustee rights to users and groups. For more information, see Section 8.5, "Typical Samba Configuration Scenarios," on page 71.

1.3.3 NSS Volumes Should Be Mounted as Case Insensitive for Use with Samba

Because Windows is case insensitive, it is recommended that NSS volumes be mounted as case insensitive (Lookup Namespace set to Long) when they are to be accessed through Samba.

1.4 Web Links

For more information about the origin, purposes, and functionality of Samba, refer to the following links:

- www.samba.org (http://www.samba.org)
- www.openldap.org\samba-2.2.8\docs\htmldocs\Samba-LDAP-HOWTO.html (http://www.openldap.org)

2 What's New or Changed in Novell Samba

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

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

2.2 What's New (OES 2015)

Samba in OES 2015 has been modified for bug fixes. There are no other changes in the OES 2015 release of Samba.

3 Installing Novell Samba for OES

This section provides instructions for installing and configuring Novell Samba and links to other relevant implementation sections.

- ◆ Section 3.1, "Samba Implementation Overview," on page 15
- ◆ Section 3.2, "Installing the Novell Samba Components," on page 16

3.1 Samba Implementation Overview

Table 3-1 presents an overview of the tasks required to implement Samba on an OES 2015 SP1 server, with links to relevant sections in this guide.

Table 3-1 *Implementation Overview for Samba in OES 2015 SP1*

Task	More information
1. Review Samba overview, caveats, and other information.	To avoid the unexpected, such as users being able to view the content of other users' home directories, review the following sections before you install Samba: ◆ Chapter 1, "Overview of Samba," on page 9 ◆ Section 8.5, "Typical Samba Configuration Scenarios," on page 71 ◆ Appendix A, "Samba Caveats," on page 91.
2. Install the Novell Samba components on the server.	You can install Novell Samba components on your OES 2015 SP1 server as part of the initial server installation, or you can add them later. For more information, see Section 3.2, "Installing the Novell Samba Components," on page 16.
3. Create Samba users in eDirectory.	Network administrators create eDirectory users with the same user names and passwords as the users have on their Windows workstations. For more information, see Section 7.1, "Creating eDirectory Users for Samba," on page 59.
4. Create shares for the users to work in and grant the users access rights to the directories.	Users need to have access to the directories on the OES server where they can create and store data. For more information, see Section 8.5, "Typical Samba Configuration Scenarios," on page 71.
5. Understand the access options available to users and communicate those options to them.	For more information, see Chapter 9, "Using Novell Samba," on page 79.

3.2 Installing the Novell Samba Components

The Novell Samba components can be installed at the same time as Open Enterprise Server, or they can be added to an OES server after the initial installation.

NOTE: These instructions assume you are using the default graphical user interface for SLES 11 SP4 (GNOME) and installing from a network installation source. If you are using the ncurses (text) version of YaST, these instructions provide only an approximate guide through the interface. If you are installing from CDs, insert them when prompted.

3.2.1 Installing Novell Samba During Initial Server Installation

To install Novell Samba as part of an initial OES server installation, follow the general instructions in "Installing OES 2015 SP1 as a New Installation" in the *OES 2015 SP1: Installation Guide*. Take note of the following Samba-specific guidelines as you go through the installation:

- When installing an OES server for Novell Samba, the hostname you specify for the server must be shorter than 13 characters in length. The NetBIOS name for Samba is limited to 15 characters, including the "-W" that is appended to the hostname automatically, which leaves 13 characters for the hostname.

  WARNING: If you enter a hostname that is longer than 13 characters, the Novell Samba setup truncates the NetBIOS name to 15 characters. As a result, iManager won't be able to find the associated server and group objects. If you need to change the NetBIOS name, see Section B.2.3, "Changing the NetBios Name," on page 98.

- Be sure to select the Novell Samba pattern when you are specifying what software you want to install on the server, along with any other OES Services patterns you need for your implementation.
- When you reach the OES Configuration portion of the install, follow the instructions in Section 3.2.3, "Configuring LUM and Novell Samba," on page 17 to configure LUM and Samba correctly for OES 2015 SP1.

3.2.2 Installing Novell Samba After Initial Server Installation

To install Novell Samba on an existing OES 2015 SP1 server:

1 Log in to the server as the `root` user.

2 Start YaST by clicking **Computer > YaST** (located in Favorite Applications).

3 If you don't already have the OES 2015 SP1 software installed as an add-on product, select **Software** > **Add-on Product** and follow the on-screen prompts to specify the location of your OES 2015 SP1 installation media.

4 Select **Open Enterprise Server** > **OES Install and Configuration**.

5 Under OES Services, select **Novell Samba**.

   SMS, LUM, and NRM are automatically selected as well. Select any other patterns you need for the server (such as iManager and NSS), then click **Accept**.

6 When prompted, click **Continue** to install Novell Samba and related RPMs.

7 If prompted for the eDirectory Admin user password, enter it and click **Next**.

8 Continue with Section 3.2.3, "Configuring LUM and Novell Samba," on page 17.

3.2.3 Configuring LUM and Novell Samba

The proper configuration of both LUM and Novell Samba is critical to the successful implementation of Samba on an OES server.

1 In the first LUM configuration screen, review the default settings and make any necessary changes.

1a The UNIX Configuration object is created in the default context shown. You can specify a different location for the Unix Configuration object, but the default should suffice in most implementations. There is one configuration object per eDirectory tree.

1b By default, the UNIX Workstation object is created in the same context as the OES 2015 SP1 server's NCP Server object. It is recommended that you leave this setting at the default.

1c (Optional) If you want to specify a proxy user for LUM, enter a username with context and a password.

1d (Optional) If you want users to have read and write access to each others' home directories, deselect the **Restrict access to the home directories of other users** option.

This option is selected by default, which restricts read and write access to home directories for users other than the owner. The default selection changes the umask setting in `/etc/login.defs` from 022 to 077.

1e Click **Next** to continue.

2 In the second LUM configuration screen, select the PAM-enabled Linux services you want to enable for LUM and Samba users.

2a The only service selected by default is sfcb. If you want eDirectory users to be able to run Linux commands such as login, ssh, and so on, you must enable the services by selecting them in this list.

To select a service, click the checkbox next to its name.

Click **Select All** to select all services in the list.

Click **Deselect All** to deselect all services in the list.

2b Click **Next** to continue.

3 In the Samba configuration screen, specify the **Base context for Samba users** and proxy user settings.
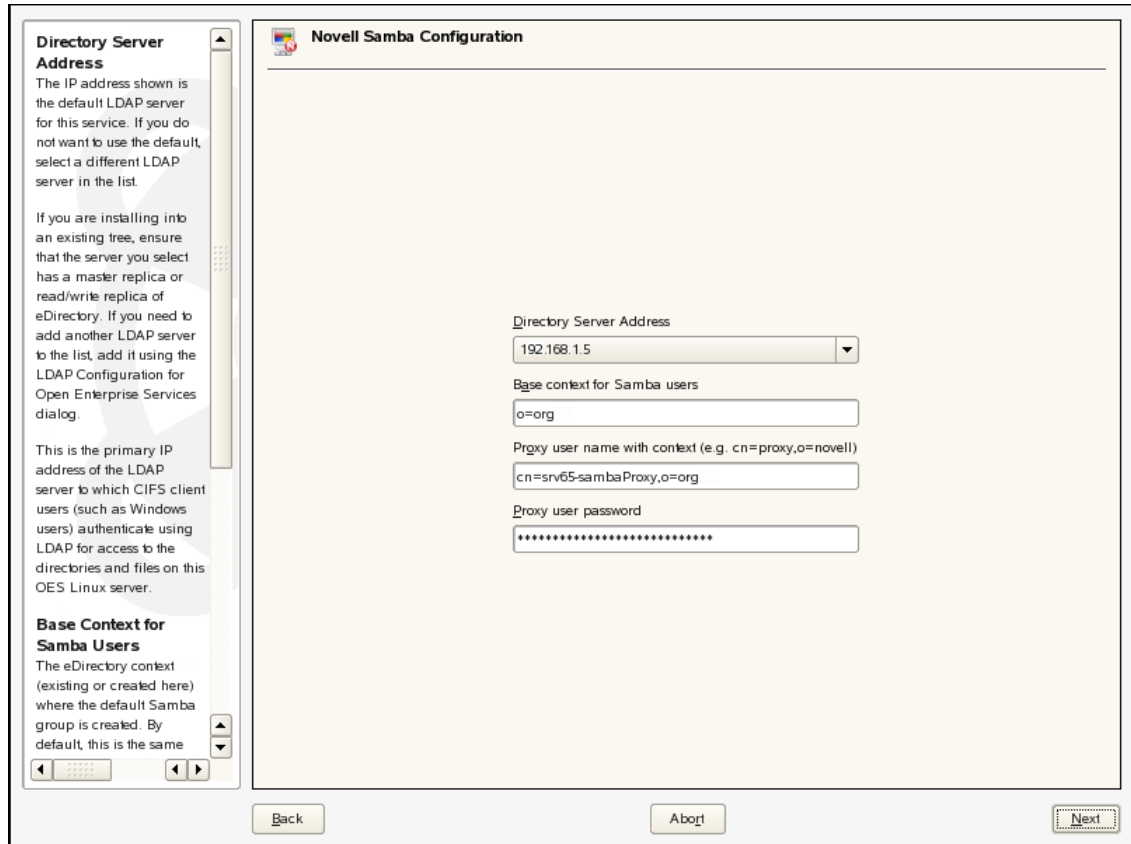
3a By default, the Base Context is set to the context (eDirectory container) where the tree admin user is created. Typically, this is the Organization (O) container, and users are created in Organizational Unit (OU) containers beneath the O container.

If your Samba users are (or will be) located in the same container as admin or in a subcontainer of that container, you do not need to change this setting. Otherwise, specify a container in your tree that is at the same level or above the container where the Samba users will be created.

3b The proxy user is an eDirectory user that has rights to search the tree for Samba users.

The Novell Samba configuration suggests a default proxy user for Samba (cn=*server_name*-sambaProxy,o=org). If you want to use a different eDirectory user as the proxy user, specify the username in typeful format (for example, cn=proxy_user,ou=users,o=novell) and enter a password for the user.

   ◆ If you specify a new user that does not already exist in eDirectory, the user is created and assigned the necessary rights and the password you specify here.

◆ If you specify an existing eDirectory user, it is assumed that you have already assigned the user the necessary rights and no modification is made to the user.

◆ If you specify an existing eDirectory user but specify a new password, you are prompted to change the password for that user.

3c Click **Next** to continue.

4 Follow the on-screen prompts to continue with the OES configuration. When it is completed, click **Finish** to close YaST.

Now that LUM and Novell Samba are installed and configured, you must create eDirectory users and give them access to Samba shares on the OES server.

For instructions, refer to .

4 Running Samba in a Virtualized Environment

Samba runs in a virtualized environment just as it does on a physical OES server and requires no special configuration or other changes.

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

5 Configuring Samba for LVM Volume Groups and Novell Cluster Services

This section describes how to configure Samba on Open Enterprise Server 2015 SP1 with Novell Cluster Services (NCS). Configuring Samba to work in a cluster ensures that the SMB/CIFS file services remain available if there is an unexpected server shutdown. Authentication for Samba users requires that they be NetIQ eDirectory users that are enabled with Linux User Management (LUM).

Although you can use Samba on shared Novell Storage Services (NSS) volumes and shared NCP volumes, the procedure in this section describes how to cluster-enable Linux POSIX volumes on a shared disk for use with Samba. This represents a typical configuration for a pure Samba/CIFS environment where the workstations accessing the shared data are not running the Novell Client software.

If you use both Linux volumes and NSS volumes on the same cluster and you want a pure Samba/CIFS environment where the workstations accessing the shared data are not running the Novell Client software, you can modify a pool cluster resource script to use Novell Samba. For information, see Chapter 6, "Configuring Samba for NSS Pools and Novell Cluster Services," on page 49.

IMPORTANT: If you use only NSS volumes for data in your cluster, consider using Novell CIFS instead of Novell Samba. With Novell CIFS, users are not required to be LUM enabled. For information about configuring Novell CIFS in a cluster and enabling CIFS as an advertising protocol for pool cluster resources, see "Configuring CIFS with Novell Cluster Services for an NSS File System" in the *OES 2015 SP1: Novell CIFS for Linux Administration Guide*.

- Section 5.1, "Benefits of Configuring Samba for High Availability," on page 23
- Section 5.2, "The Samba Template in OES 2015 SP1," on page 24
- Section 5.3, "NCS Installation and Configuration," on page 24
- Section 5.4, "Creating a Samba Cluster Resource with NSSMU and the Generic File System Template," on page 26
- Section 5.5, "Creating a Samba Cluster Resource with the Samba Template," on page 30
- Section 5.6, "Samba Configuration," on page 43

5.1 Benefits of Configuring Samba for High Availability

With Novell Samba installed on a Open Enterprise Server 2015 SP1 (OES 2015 SP1) server, client computers can access and use files on shared storage devices connected to the Linux server. If the server running Samba becomes unaccessible, clients lose their ability to access network files.

Configuring Samba with Novell Cluster Services ensures that Samba is highly available and that network files remain accessible even if the primary Samba server goes down unexpectedly. NCS makes this possible by automatically switching file services from the failed Samba server to another Samba server in the cluster.

5.2 The Samba Template in OES 2015 SP1

Starting with OES 2015 SP1, the Novell Cluster Services Samba template uses a Linux Logical Volume Manager (LVM) volume group on a shared device. The Enterprise Volume Management System (EVMS) has been deprecated in SUSE Linux Enterprise Server 11, and is not used for OES 2015 SP1.

The Samba resource template has been updated to create new resources based on an LVM volume group and logical volume. For information about creating and managing shared Linux POSIX file systems built with an LVM volume group, see "Configuring and Managing Cluster Resources for Shared LVM Volume Groups" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

For Novell Storage Services (NSS) file systems, the Novell Linux Volume Manager (NLVM) replaces EVMS transparently for your pool cluster resources. You create new pool cluster resources using the same procedures as you have done for earlier versions of OES. Your resources and scripts work without changes if you upgrade to OES 2015 SP1.

If you upgrade a shared Linux POSIX file system from a previous OES 1 or OES 2 server, special handling is required. For information, see "Upgrading Clusters from OES 2 SP3 to OES 2015 SP1" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*. After the upgrade, see "Upgrading and Managing Cluster Resources for Linux POSIX Volumes with CSM Containers" for information about managing the CSM-based resources.

5.3 NCS Installation and Configuration

Novell Cluster Services for Linux must be installed on the OES 2015 SP1 server before you can configure Samba to work in a cluster. NCS provides a Samba resource template, which facilitates the configuration of Samba in a cluster environment. This requires that you use Linux Logical Volume Manager commands to set up the volume group and add information to the Samba resource template.

You can alternatively use the Generic File System template (GenericFS_template) for your shared LVM volume group, and add lines from the Samba tempate's scripts for the volume group cluster resource. The Novell Logical Volume Manager (NLVM) commands and NSSMU automatically use the GenericFS_template to create the volume group cluster resource.

Both methods to generate a Samba resource are described below. Choose either method to create your Samba resource, then continue to configure Samba for the resource.

5.3.1 Setting Up a Shared Disk Subsystem

Before you start installing NCS, review the "Shared Disk Scenarios" section of the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide* and identify a hardware configuration that meets your network's needs.

A typical cluster configuration includes a shared disk subsystem (Storage Area Network, or SAN) that is connected to all servers in the cluster. The shared disk subsystem can be connected via Fibre Channel hardware, SCSI adapters, or iSCSI connections. Follow the manufacturer's instructions to set up the shared disk subsystem and ensure that it is functional before proceeding.

For Linux volumes, each shared disk will contain one Linux LVM (Logical Volume Manager) volume group with one Linux POSIX volume.

5.3.2   Preparing the Cluster

Install Novell Cluster Services and configure the cluster. For information, see "Installing, Configuring, and Repairing Novell Cluster Services" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

> **IMPORTANT:** Ensure that you install the latest patches for SUSE Linux Enterprise Server 11 SP4. Clustered LVM volume groups require Linux kernel version 2.6.32.45-0.3 or later.

In addition to selecting Novell Cluster Services as part of the OES 2015 SP1 software installation, you should also select and configure the following:

- ◆ **NetIQ eDirectory:** NetIQ eDirectory must be installed on the network in order for Novell Cluster Services to be able to create the necessary Cluster objects in the tree. All servers in the cluster must be in the same eDirectory tree.

- ◆ **Novell iManager:** Novell iManager is required to configure and manage Novell Cluster Services, and must be installed on at least one server in the same tree as the cluster.

- ◆ **Samba Access for NSS and NCP Volumes:** (Optional) Novell Storage Services (NSS) and NCP Server must be installed if you want to use NSS volumes or NCP volumes on Linux POSIX file systems in the cluster.

- ◆ **Resource IP Address:** A unique IP address is required for each shared disk's cluster resource.

For more information on installing and configuring OES services, see the *OES 2015 SP1: Installation Guide*.

5.3.3   Installing Novell Samba

If you have not already done so, install and configure the Novell Samba pattern on each cluster server that will share the Samba resource. This package can be installed when you install your OES server. You can also install it afterward by using the **Open Enterprise Server > OES Install and Configuration** option in YaST.

When you configure Novell Samba on subsequent OES 2015 SP1 servers after the first server in the tree, you must select the IP address of the master LDAP server (the server holding the master replica of the partition) for the **Directory Server Address** setting, not the IP address of the server you are installing.

Ensure that the **Base Context for Samba Users** is set to the container where you plan to create your Samba users, or to a container above that in the eDirectory tree. By default, the **Base Context for Samba Users** is set to the same container where the eDirectory Admin user is created. The users that you want to access the shared Samba resource must be located in this container or in a subcontainer. If your Samba users are located in a different branch of the tree, you must change the base context setting when you configure Novell Samba.

For more information on installing and configuring Novell Samba, see Chapter 3, "Installing Novell Samba for OES," on page 15.

5.4 Creating a Samba Cluster Resource with NSSMU and the Generic File System Template

Create a Linux LVM volume group cluster resource, then create subdirectories on it that Samba will use. This section describes how to use NSSMU to create and cluster enable an LVM volume group. NSSMU automatically uses the Generic File System template (`Generic_FS_Template`) to create a volume group cluster resource. You can add lines to it from the Samba template to create the Samba cluster resource.

The examples in this section use following setup. Make sure to replace the sample values with information for your configuration.

Variable	Sample Value
Device name for the shared device	`/dev/sdd`
Volume group name	`sambavol44` NSSMU sets the volume group name to be the same as the logical volume. If you use the NLVM `create linux volume` command to create the LVM volume group cluster resource, you can specify a different name for the volume group, such as `sambavg44`.
Volume name	`sambavol44`
Linux POSIX file system	ext3
Volume size	100 GB
Resource IP address	10.10.10.44

Mount device	`/dev/sambavol44/sambavol44`
	
	The mount device path format is
	
	`/dev/<volume_group_name>/<logical_volume_name>`
	
	If you specified a different name for the volume group, such as `sambavg44`, the mount device path is `/dev/sambavg44/sambavol44`.

Mount point	`/mnt/smbvol44` The subdirectory name you use for the mount point can be the same or different than the volume name. This example uses a different name.

5.4.1 Creating an LVM Volume Group Cluster Resource

On the master node of the cluster, create and cluster enable an LVM volume group cluster resource by using NSSMU. The disk will contain one LVM volume group and one logical volume. For information, see "Configuring an LVM Volume Group Cluster Resource with NSS Management Tools" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

5.4.2 Creating Subdirectories on the LVM Volume

While the shared LVM volume is mounted, you must create some subdirectories on it that Samba will use. At this point, the resource you created should still be on the master node.

1 Log in as the `root` user on the master node, then open a terminal console.

2 Verify that the cluster resource is online by entering

```
cluster status
```

If it is not online, bring it online now by entering

```
cluster online <resource> <master_node>
```

3 Create the subdirectory paths `log` and `share/locks` at the root of the mounted volume (`/mnt/smbvol44`) by entering the following commands:

```
mkdir -p /mnt/smbvol44/log
```

```
mkdir -p /mnt/smbvol44/share/locks
```

The subdirectories are created on the mounted volume (not at the file system root (/) directory). These paths reside on the shared volume, and are available on a node only when the shared volume is mounted at the `/mnt/smbvol44` mount point.

4 Verify that the new subdirectories exist and are owned by the `root` user, and the default group is `root`. Also, the directories must have the Linux POSIX permissions of `drwx r_x r_x`.

For example, list the directories and view the Linux POSIX permissions, file owner, and group owner.

```
avalon:/ # dir /mnt/smbvol44
total 8
drwxr-xr-x 2 root root 4096 2011-12-05 14:15 log
drwxr-xr-x 3 root root 4096 2011-12-05 14:16 share
```

5 Continue with Section 6.3, "Modifying the Pool Resource Scripts for Samba," on page 52.

5.4.3 Modifying the Generic File System Scripts for Samba

After the shared storage is properly configured, you must modify the LVM volume group cluster resource in Novell Cluster Services. This includes adding lines for Samba in the load, unload, and monitor scripts.

- ◆ "Modifying the Generic File System Resource Load Script" on page 27
- ◆ "Modifying the Generic File System Resource Unload Script" on page 28
- ◆ "Modifying the Generic File System Resource Monitor Script" on page 29

Modifying the Generic File System Resource Load Script

1 In Novell iManager, log in as an administrator user.

2 In **Roles and Tasks**, select **Clusters > Cluster Manager**, then browse to select the Cluster object for the cluster.

3 Click the name link of the LVM volume group cluster resource to go to its Properties page, then click the **Scripts** tab.

4 View the load script.

The default generic file system load script for the sample setup contains all the information that you entered when you created the resource in NSSMU.

5 Add the following definitions and Samba start lines to the load script.

The configuration file name is the name you will give the Samba configuration file on the shared location. The two Start Samba lines should follow the line that mounts the volume.

The lines are commented out at this time. You uncomment them later when the Samba configuration file is ready.

```
# define the name of the samba config file
#CONFIG_FILE=SambaResource-smb.conf


# start Samba
#exit_on_error /usr/sbin/nmbd --log-basename=$MOUNT_POINT/log --
configfile=$MOUNT_POINT/$CONFIG_FILE

#exit_on_error /usr/sbin/smbd --log-basename=$MOUNT_POINT/log --
configfile=$MOUNT_POINT/$CONFIG_FILE
```

6 Click **Apply**.

7 Continue with "Modifying the Generic File System Resource Unload Script" on page 28.

Modifying the Generic File System Resource Unload Script

1 Continue from "Modifying the Generic File System Resource Load Script" on page 27.

2 On the **Scripts** tab for the generic file system cluster resource, click the **Unload** link to view the unload script.

3 View the unload script.

The default generic file system unload script for the sample setup contains all the information that you entered when you created the resource in NSSMU.

4 Add the following definitions and Samba stop lines to the unload script.

The configuration file name is the name you give the Samba configuration file on the shared location. The two Stop Samba lines should precede the line that unmounts the NSS volume.

The lines are commented out at this time. You uncomment them later when the Samba configuration file is ready.

```
# define the name of the samba config file
#CONFIG_FILE=SambaResource-smb.conf

# request Samba stop
# ignore_error killproc -p $MOUNT_POINT/share/locks/nmbd-$CONFIG_FILE.pid /
usr/sbin/nmbd
# ignore_error killproc -p $MOUNT_POINT/share/locks/smbd-$CONFIG_FILE.pid /
usr/sbin/smbd
```

5 Click **Apply**.

6 Continue with "Modifying the Generic File System Resource Monitor Script" on page 29.

Modifying the Generic File System Resource Monitor Script

1 Continue from "Modifying the Generic File System Resource Unload Script" on page 28.

2 On the **Scripts** tab for the generic file system cluster resource, click the **Monitor** link to view the monitor script.

3 View the monitor script.

The default generic file system monitor script for the sample setup contains all the information that you entered when you created the resource in NSSMU.

4 Add the following definitions and Samba check status lines to the monitor script.

The configuration file name is the name you give the Samba configuration file on the shared location. The two check status Samba lines can follow the check of the NSS volume.

The lines are commented out at this time. You uncomment them later when the Samba configuration file is ready.

```
# define the name of the samba config file
#CONFIG_FILE=SambaResource-smb.conf

# check Samba
#exit_on_error checkproc -p $MOUNT_POINT/share/locks/smbd-$CONFIG_FILE.pid /
usr/sbin/smbd
#exit_on_error checkproc -p $MOUNT_POINT/share/locks/nmbd-$CONFIG_FILE.pid /
usr/sbin/nmbd
```

5 Click **Apply**.

6 At the bottom of the page, click **OK** to save all changes for the pool cluster resource.

IMPORTANT: The changes are not effective until the resource is taken offline and brought online again.

---

7 Continue with Section 5.6, "Samba Configuration," on page 43.

5.5   Creating a Samba Cluster Resource with the Samba Template

The Samba template for Novell Cluster Services requires that you create a shared volume group and then use the Samba template to create a Samba cluster resource. This includes configuring Samba load, unload, and monitor scripts; setting Samba start, failover, and failback modes; and assigning the Samba resource to specific servers in your cluster.

The examples in this section use following setup. Make sure to replace the sample values with the information for your system.

Variable	Sample Value
Device name for the shared device	`/dev/sdd`
Volume group name	`sambavg44`
Volume name	`sambavol44`
Volume size	100 GB
Linux POSIX file system	ext3
Mount device	`/dev/sambavg44/sambavol44`
Mount point	`/mnt/smbvol44`
Resource IP address	10.10.10.44

5.5.1   Creating a Shared Volume with LVM Commands

In order for Samba users to access files on a shared disk, you must prepare the shared storage for this purpose. The procedure involves creating an LVM volume group, a logical volume, and POSIX file system on a single shared disk. You do not create the cluster resource at this time.

For an overview of the LVM commands that you use in the following procedure, see "Using LVM Commands" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

1 Before you begin, make sure you have met the requirements described in "Requirements for Creating LVM Cluster Resources" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

2 Log in to the server as the `root` user, then open a terminal console.

3 If the device you want to use is not initialized, initialize the device:

   3a At the prompt, enter

```
nssmu
```

3b From the NSSMU main menu, select **Devices**, then press Enter.

3c From the list of devices, select the device you want to use, such as `sdd`.

3d View the device information to confirm it is the device you want to initialize.

Devices that have never been initialized do not have a partition type assigned and are annotated as being **Uninitialized**. If the device contains data, ensure that you are prepared to delete all of the data on the device.

WARNING: Initializing a device destroys all data on the device.

3e Press F3 to initialize the device, then press Enter to confirm, or press Esc to abort the operation.

3f Specify a partitioning scheme, then press Enter to finish:

- ◆ **DOS:** Supports devices up to 2 TB in size.
- ◆ **GPT:** Supports devices of any size.

3g View the device information to confirm that it is initialized.

Notice that the Shareable for Clustering parameter is set to **No**. Do not enable it. Clustered LVM will control the share state after you create the volume group.
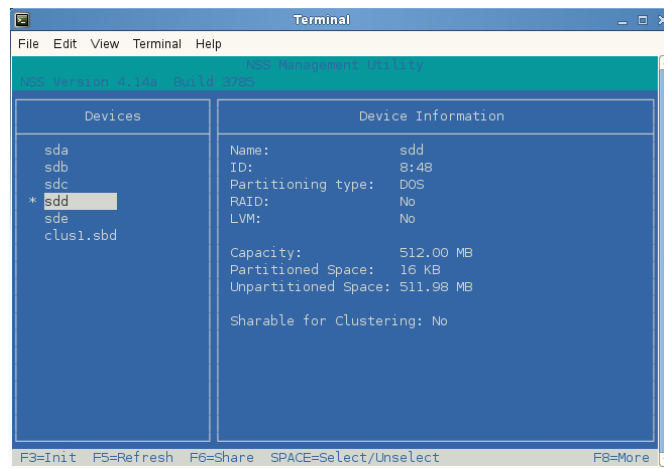
4 Create a clustered Linux LVM volume group and logical volume:

4a Create a physical volume for the device by entering

```
pvcreate <device_name>
```

For example, to create an LVM physical volume on the `/dev/sdd` device, enter

```
pvcreate /dev/sdd
```

4b Create an LVM volume group on the device by entering

```
vgcreate -c y <"vg_name"> <device_name>
```

For example, to create the volume group named `sambavg44` on the `/dev/sdd` device, enter

```
vgcreate -c y "sambavg44" /dev/sdd
```

4c Create a logical volume in the LVM volume group by entering

```
lvcreate -n <"lv_name"> -L <size> <"vg_name">
```

For example, to create a logical volume named `sambavol44` on the `sambavg44` volume group that is 100 GB in size, enter

```
lvcreate -n  "sambavol44" -L 100G "sambavg44"
```

  4d Make a file system on the logical volume by entering

```
mkfs -t <fs_type> <"full_lv_path">
```

For example, to create an Ext3 file system on the `sambavol144` logical volume, enter

```
mkfs -t ext3 "/dev/sambavg44/sambavol44"
```

5 Deactivate the volume group and logical volume. As the `root` user, enter

```
vgchange -a n <"vg_name">
```

For example:

```
vgchange -a n "sambavg44"
```

6 Continue with Section 5.5.2, "Creating a Mount Point for the Volume on Each Node," on page 32.

5.5.2 Creating a Mount Point for the Volume on Each Node

On each OES 2015 SP1 server that will participate in the cluster, you need to create a mount point for the shared file system you just created in Section 5.5.1, "Creating a Shared Volume with LVM Commands," on page 30. The default mount point is /mnt/samba in the Samba resource load, unload, and monitoring scripts.

1 Log in as the `root` user, then open a terminal console.

2 Create the mount point /mnt/smbvol44 by entering:

```
mkdir -p /mnt/smbvol44
```

3 For each node in turn, repeat Step 2 to create the mount point on each cluster server.

4 Continue with Section 5.5.3, "Creating Subdirectories on the LVM Volume," on page 32.

5.5.3 Creating Subdirectories on the LVM Volume

While the shared LVM volume is mounted, you must create some subdirectories on it that Samba will use. At this point, the resource you created should still be on the master node.

To create the subdirectories `log` and `share/locks` at the root of the mounted volume (/mnt/smbvol44):

1 Activate the LVM volume group exclusively on the server by entering

```
vgchange -a ey <"vg_name">
```

For example, to mount the LVM volume group `sambavg44`, enter

```
vgchange -a ey "sambavg44"
```

2 Mount the volume by entering

```
mount -t <fs_type> </dev/vg_name/lv_name> <mount_point>
```

For example, to mount the logical volume `/dev/sambavg44/sambavol44` on the mount point `/mnt/smbvol44,` enter

```
mount -t ext3 /dev/sambavg44/sambavol44 /mnt/smbvol44
```

3 Create the subdirectory paths `log` and `share/locks` at the root of the mounted volume (`/mnt/smbvol44`) by entering the following commands:

```
mkdir -p /mnt/smbvol44/log
```

```
mkdir -p /mnt/smbvol44/share/locks
```

The subdirectories are created on the mounted volume (not at the file system root (/) directory). These paths reside on the shared volume, and are available on a node only when the shared volume is mounted at the `/mnt/smbvol44` mount point.

4 Verify that the new subdirectories exist and are owned by the `root` user, and the default group is `root`. Also, the directories must have the Linux POSIX permissions of `drwx r_x r_x`.

For example, list the directories and view the Linux POSIX permissions, file owner, and group owner.

```
avalon:/ # dir /mnt/smbvol44
total 8
drwxr-xr-x 2 root root 4096 2011-12-05 14:15 log
drwxr-xr-x 3 root root 4096 2011-12-05 14:16 share
```

5 Unmount the volume and deactivate the volume group on this node by entering

```
umount </dev/vg_name/lv_name>
vgchange -a n <"vg_name">
```

For example:

```
umount /dev/sambavg44/sambavol1
vgchange -a n "sambavg44"
```

6 Continue with Section 5.5.4, "Creating a Samba Cluster Resource," on page 33.

5.5.4 Creating a Samba Cluster Resource

Novell Cluster Services includes a Samba resource template, which greatly simplifies the process for creating a Samba cluster resource. The Samba resource template configures the Samba resource by automatically creating Samba load and unload scripts, setting failover and failback modes, and assigning Samba as a resource to all nodes in the cluster.

1 Continue from Section 5.5.3, "Creating Subdirectories on the LVM Volume," on page 32.

The shared file system should still be deactivate on all nodes.

2 Open iManager in a Web browser, then log in as an administrator user.

3 In **Roles and Tasks**, select **Clusters** > **Cluster Options**.

4 In the **Cluster** field, specify the cluster name, or browse and select it.

iManager displays links that you can use to configure and manage your cluster.
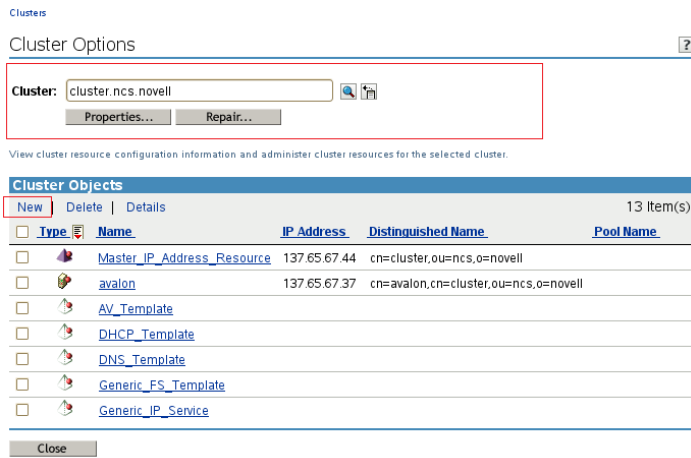
5 Above the Cluster objects, click **New**.

6 Specify **Resource** as the resource type you want to create, then click **Next**.
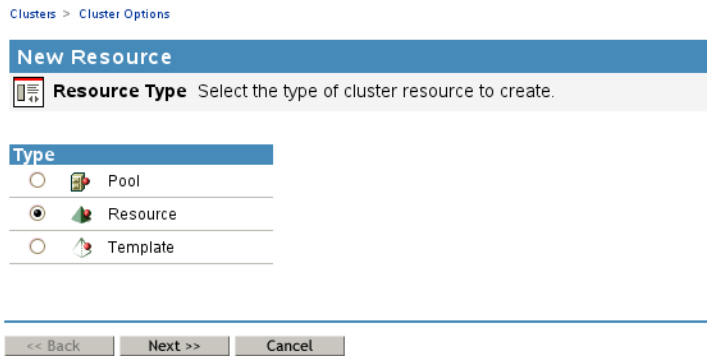
7 Specify a name for the Samba resource.

This is the name that identifies the resource for the cluster-enabled file system, such as `smbvol44`.
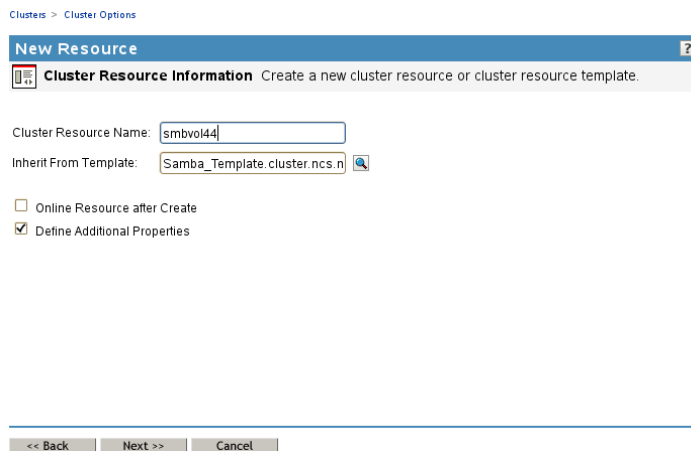
8 In the **Inherit From Template** field, browse to the Cluster object for the cluster, then select the Samba resource template (**Samba_Template**) from the list.

Contents: (click object to select)

   ↰ .. (up one level)
     AV_Template
     DHCP_Template
     DNS_Template
     Generic_FS_Template
     Generic_IP_Service
     iFolder_Template
     iPrint_Template
     MySQL_Template
     Samba_Template
     Xen_Template
     XenLive_Template

9 Select **Define Additional Properties**.

The **Online Resource after Create** option is automatically deselected and should not be selected. You must configure the load, unload, and monitor scripts and the resource settings before you online the Samba resource for the first time.

Clusters > Cluster Options

New Resource   [?]

Cluster Resource Information Create a new cluster resource or cluster resource template.

Cluster Resource Name: smbvol44

Inherit From Template: Samba_Template.cluster.ncs.n 🔍

☐ Online Resource after Create
☑ Define Additional Properties

[<< Back]   [Next >>]   [Cancel]
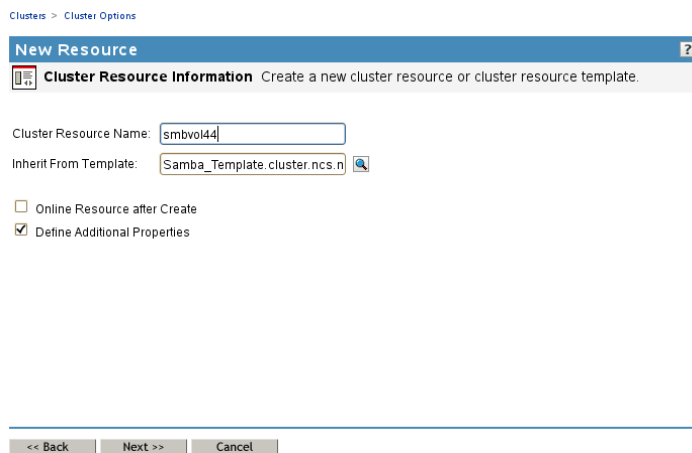
10 Click **Next**, then continue with Section 5.5.5, "Configuring Samba Load, Unload, and Monitor Scripts," on page 35.

5.5.5 Configuring Samba Load, Unload, and Monitor Scripts

Continue the Samba resource configuration by modifying the settings in the load, unload, and monitor scripts to use the Linux POSIX file system that you created in Section 5.5.1, "Creating a Shared Volume with LVM Commands," on page 30.

- "Load Script Configuration" on page 36
- "Unload Script Configuration" on page 37
- "Monitor Script Configuration" on page 39

Load Script Configuration

The Samba load script page should already be displayed.

New Resource ?

📑 **Load Script** Add commands to the load script to start the resource or service.

Script:
```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# define the IP address
RESOURCE_IP=a.b.c.d
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=name
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/samba
# define the mount point
MOUNT_POINT=/mnt/samba

# define the name of the samba config file
```

Timeout: 6   Minutes ▼

[<< Back] [Next >>] [Cancel]

The load script contains commands to start the Samba resource, including mounting the shared file system on a server in the cluster. It is called when you migrate the service or when the primary server fails. You must customize some of the commands in the script for your specific Samba configuration.

1 Edit the following lines for your specific IP address, file system type, volume group, volume, and mount point:

```
# define the IP address
RESOURCE_IP=a.b.c.d
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=name
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/samba
# define the mount point
MOUNT_POINT=/mnt/samba
```

Replace *a.b.c.d* with the IP address for the Samba cluster resource, such as 10.10.10.44. The IP address for the Samba cluster resource allows clients to reconnect to that address regardless of which server is hosting it.

If you created a POSIX file system other than Ext3 (such as ReiserFS or XFS), specify the file system for the `MOUNT_FS` variable. Specify the file system in lowercase.

For the VOLGROUP_NAME variable, replace *name* with the LVM volume group name (such as `sambavg44`) that you created in Section 5.5.1, "Creating a Shared Volume with LVM Commands," on page 30.

For `MOUNT_DEV`, replace *samba* with the name of the volume (such as `sambavol44`) that you created in the LVM volume group in Section 5.5.1, "Creating a Shared Volume with LVM Commands," on page 30.

For `MOUNT_POINT`, replace `/mnt/samba` with the mount point (such as `/mnt/smbvol44`) that you created on each cluster server in Section 5.5.2, "Creating a Mount Point for the Volume on Each Node," on page 32.

For example, set the following values:

```
# define the IP address
RESOURCE_IP=10.10.10.44
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=sambavg44
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/sambavol44
# define the mount point
MOUNT_POINT=/mnt/smbvol44
```

2 Comment out the configuration file definition line by inserting a # (hash mark) at the beginning of the line:

```
# CONFIG_FILE=SambaResource-smb.conf
```

You will uncomment this line later, after the Samba cluster resource configuration is complete.

3 Comment out the two lines under # start Samba by inserting a # (hash mark) at the beginning of each line:

```
# start Samba

#exit_on_error /usr/sbin/nmbd --log-basename=$MOUNT_POINT/log --
configfile=$MOUNT_POINT/$CONFIG_FILE

#exit_on_error /usr/sbin/smbd --log-basename=$MOUNT_POINT/log --
configfile=$MOUNT_POINT/$CONFIG_FILE
```

You will uncomment these lines later, after the Samba cluster resource configuration is complete.

4 Click **Next**, and continue with .

Unload Script Configuration

The Samba unload script page should now be displayed.
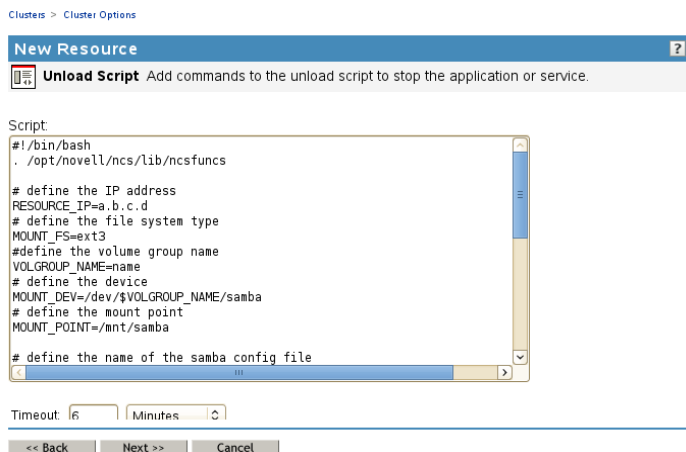
The unload script contains commands to stop the Samba resource, including unmounting the shared file system on a server in the cluster. You must customize some commands for your specific Samba configuration.

1 Edit the following lines for your specific IP address, file system type, volume group, volume, and mount point:

```
# define the IP address
RESOURCE_IP=a.b.c.d
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=name
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/samba
# define the mount point
MOUNT_POINT=/mnt/samba
```

Replace the variables with the same values you specified for the load script.

For example, set the following values:

```
# define the IP address
RESOURCE_IP=10.10.10.44
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=sambavg44
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/sambavol44
# define the mount point
MOUNT_POINT=/mnt/smbvol44
```

2 Comment out the configuration file definition line by inserting a # at the beginning of the line:

```
# CONFIG_FILE=SambaResource-smb.conf
```

You will uncomment this line later, after the Samba cluster resource configuration is complete.

3 Comment out the two lines under `# request Samba stop`, and modify the `.pid` file's directory path from `/var/run/samba` to `$MOUNT_POINT/share/locks` as follows:

```
# request Samba stop
# ignore_error killproc -p $MOUNT_POINT/share/locks/nmbd-$CONFIG_FILE.pid /
usr/sbin/nmbd
# ignore_error killproc -p $MOUNT_POINT/share/locks/smbd-$CONFIG_FILE.pid /
usr/sbin/smbd
```

You will uncomment these lines later, after the Samba cluster resource configuration is complete.

4 Click **Next**, and continue with .

Monitor Script Configuration

The Samba monitor script page should now be displayed.
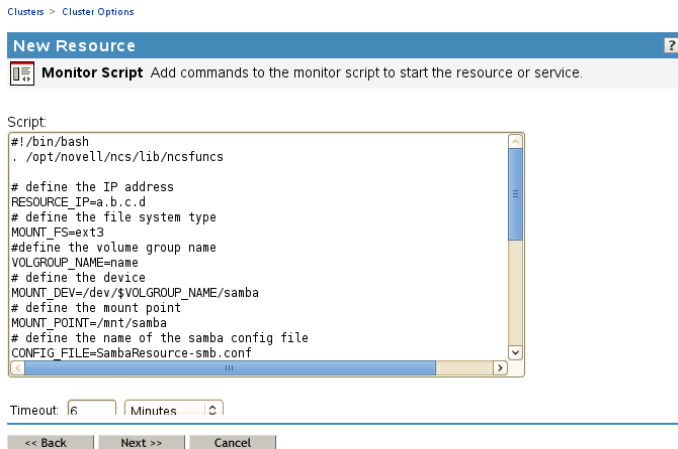
The monitor script contains commands to monitor the status of the Samba resource. You must customize some commands for your specific Samba configuration.

1 Edit the following lines for your specific IP address, file system type, volume group, volume, and mount point:

```
# define the IP address
RESOURCE_IP=a.b.c.d
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=name
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/samba
# define the mount point
MOUNT_POINT=/mnt/samba
```

Replace the variables with the same values you specified for the load and unload scripts.

For example, set the following values:

```
# define the IP address
RESOURCE_IP=10.10.10.44
# define the file system type
MOUNT_FS=ext3
#define the volume group name
VOLGROUP_NAME=sambavg44
# define the device
MOUNT_DEV=/dev/$VOLGROUP_NAME/sambavol44
# define the mount point
MOUNT_POINT=/mnt/smbvol44
```

2 Comment out the configuration file definition line by inserting a # at the beginning of the line:

```
# CONFIG_FILE=SambaResource-smb.conf
```

You will uncomment this line later, after the Samba cluster resource configuration is complete.

3 Comment out the two lines under `# check Samba`, and modify the `.pid` file's directory path from `/var/run/samba` to `$MOUNT_POINT/share/locks` as follows:

```
# check Samba
#exit_on_error checkproc -p $MOUNT_POINT/share/locks/smbd-$CONFIG_FILE.pid /
usr/sbin/smbd
#exit_on_error checkproc -p $MOUNT_POINT/share/locks/nmbd-$CONFIG_FILE.pid /
usr/sbin/nmbd
```

You will uncomment these lines later, after the Samba cluster resource configuration is complete.

4 Click **Next** and continue with Section 5.5.6, "Setting Samba Start, Failover, and Failback Modes," on page 40.

5.5.6 Setting Samba Start, Failover, and Failback Modes

The page to set Start, Failover, and Failback modes should now be displayed.

1 By default, the Samba resource template sets the Samba resource Start mode and Failover mode to Auto and the Failback Mode to Disable. You can change the default settings as needed.

   ◆ If the Start mode is set to Auto, the Samba resource automatically loads on a designated server when the cluster is first brought up. If the Start mode is set to Manual, you can manually start the Samba resource on a specific server when you want, instead of having it automatically start when servers in the cluster are brought up.

   ◆ If the Failover mode is set to Auto, the Samba resource automatically moves to the next server in the Assigned Nodes list if there is a hardware or software failure. If the Failover mode is set to Manual, you can intervene after a failure occurs and before the Samba resource is started on another node.

   ◆ If the Failback mode is set to Disable, the Samba resource continues running on the node it has failed to. If the Failback mode is set to Auto, the Samba resource automatically moves back to its preferred node when the preferred node is brought back online. Set the Failback mode to Manual to prevent the Samba resource from moving back to its preferred node when that node is brought back online, until you are ready to allow it to happen.

2 When you have finished making the desired changes to these settings, click **Next**.

3 Continue with Section 5.5.7, "Editing the Samba Resource Preferred Nodes List," on page 41.

5.5.7 Editing the Samba Resource Preferred Nodes List

The page to view or change the preferred nodes for the Samba resource should now be displayed.
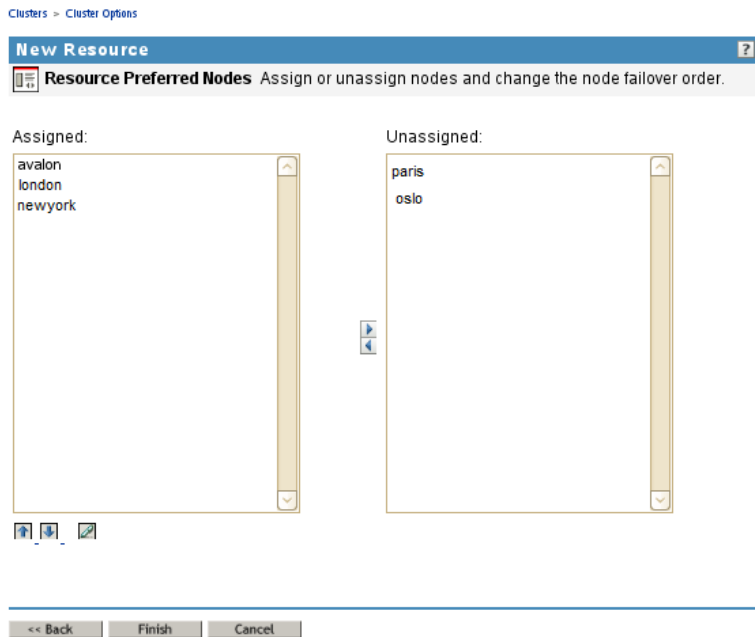
The Samba resource template automatically assigns the Samba resource to all nodes in the cluster. The order of assignment is the order the nodes appear in the resource list.

To view or edit preferred node assignments or change the server failover order:

1 From the list of unassigned nodes, select a server you want the resource assigned to, then click the right-arrow button to move the selected server to the **Assigned Nodes** list.

Repeat this step for all servers you want assigned to the resource. You can also use the left-arrow button to unassign servers from the resource.

2 Click **Edit** (pen icon) to open the **Assigned Nodes** list in a text editor. Reorder the entries, then click **OK**.

You can also click the up-arrow and down-arrow buttons to change the failover order of the servers assigned to the resource.

3 Click **Apply** or **Finish** to save preferred node assignment changes.

The newly created resource appears in the **Cluster Objects** list.
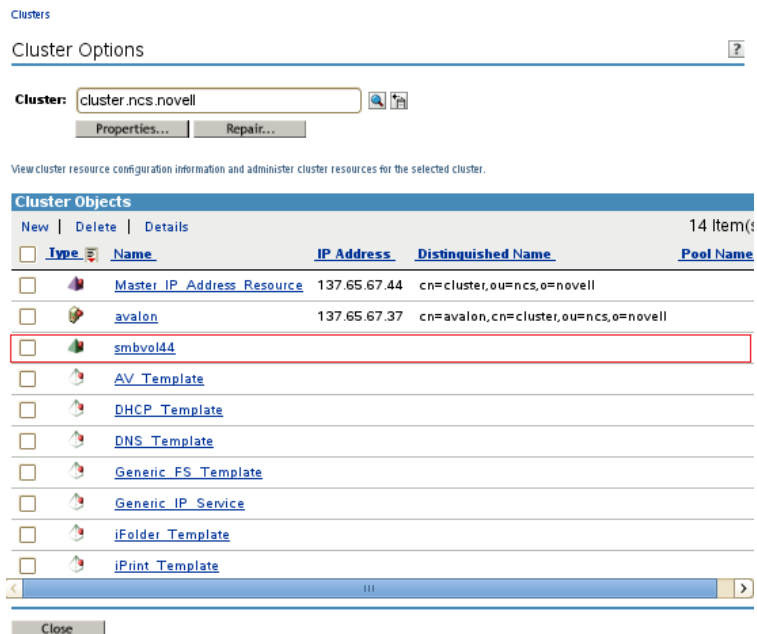
4 Continue with Section 5.5.8, "Verifying the Samba Cluster Resource Configuration," on page 42.

5.5.8 Verifying the Samba Cluster Resource Configuration

At this point, it is a good practice to verify the configuration of the Samba cluster resource.

1 Bring the cluster resource online by entering the following command on one node:

```
cluster online <samba_resource_name> <node_name>
```

If the resource is in a comatose state, you must take the resource offline, then try again to online the resource.

For example, enter the following command to online the resource, then view its confirmation message:

```
cluster online smbvol44 server1

  Status for Resource: smbvol44
  Loading on server 1   Lives: 1
  Revision: 1
```

2 Enter the following commands and verify that the IP address of the node and the shared file system are listed:

```
ip add
```

```
server1:/mnt # ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet 127.0.0.2/8 brd 127.255.255.255 scope host secondary lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:14:c9:64 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.37/22  brd 10.10.10.255  scope global eth0
    inet 10.10.10.43/22  brd 10.10.10.255  scope global secondary eth0
    inet 10.10.10.44/22  brd 10.10.10.255  scope global secondary eth0
    inet6 fe80::20c:29ff:fe14:c964/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:14:c9:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.25.172/24 brd 192.168.25.255 scope global eth1
    inet6 fe80::20c:29ff:fe14:c96e/64 scope link
       valid_lft forever preferred_lft forever
```

df -h

```
server1:/mnt # df -h
Filesystem           Size  Used Avail Use% Mounted on
/dev/sda3            8.4G  3.9G  4.1G  50% /
devtmpfs             973M  140K  973M   1% /dev
tmpfs                973M  284K  972M   1% /dev/shm
/dev/sda1            190M   35M  146M  20% /boot
admin                4.0M     0  4.0M   0% /_admin
/dev/sr0             682M  682M     0 100% /media/OES11-addon-x86_64.0291.1.001
/dev/mapper/mysambavg44-mysambavol44
                     492M   11M  457M   3% /mnt/smbvol144
```

3 Migrate the Samba resource to each node in its Preferred Nodes list, and verify that the migration is successful:

3a Cluster migrate the Samba resource to a node in the Preferred Nodes list:

```
cluster migrate <samba_resource_name> <node_name>
```

3b Check whether the migration operation was successful:

```
cluster status
```

3c Correct any configuration problems before continuing.

4 After you have verified the resource, bring the Samba cluster resource online on its most preferred node.

5 Continue with .

5.6   Samba Configuration

Now that you have installed and configured Novell Cluster Services and created the Samba cluster resource, you are ready to configure Samba on each cluster server.

- Section 5.6.1, "Preparing the Cluster Servers," on page 44
- Section 5.6.2, "Creating a Samba Share," on page 44
- Section 5.6.3, "Editing the Samba Resource Configuration File," on page 45
- Section 5.6.4, "Modifying and Bringing the Samba Cluster Resource Online," on page 46
- Section 5.6.5, "Creating Samba Users and a Group for Cluster Access," on page 47

5.6.1 Preparing the Cluster Servers

1 If you have not already done so, install and configure the Novell Samba pattern on each cluster server that will share the Samba resource.

Ensure that the **Base Context for Samba Users** is set to the container where you plan to create your Samba users, or to a container above that in the eDirectory tree.

For more information on installing and configuring Novell Samba, see Chapter 3, "Installing Novell Samba for OES," on page 15.

2 Enter the following command on all preferred nodes in the cluster that are assigned to the Samba resource:

```
chkconfig smb off
```

This command ensures that Samba is not started until it is required for a resource migration or failover.

3 Continue with Section 5.6.2, "Creating a Samba Share," on page 44.

5.6.2 Creating a Samba Share

In OES, you can use the new Samba management plug-in for iManager to create a new Samba share, instead of manually adding a share definition in the `/etc/samba/smb.conf` file.

1 In iManager's Roles and Tasks, select **File Protocols** > **Samba**.

2 In the **Server** field, browse and select the server where the Samba resource is currently online.

3 Wait for the general Samba information to be displayed, then click the **Shares** tab.

4 Click **New** and follow the on-screen prompts to create a share that maps to the mount point you defined for the Samba cluster resource.

- **Share Name:** Specify the share name, such as `smbvol44`.

- **Path:** Specify the path of the mount path you defined for the Samba resource, such as `/mnt/smbvol44`.

- **Comment:** Specify a brief description about the purpose of this share, such as `Samba Resource`.

- **Inherit ACLs:** Select this option.
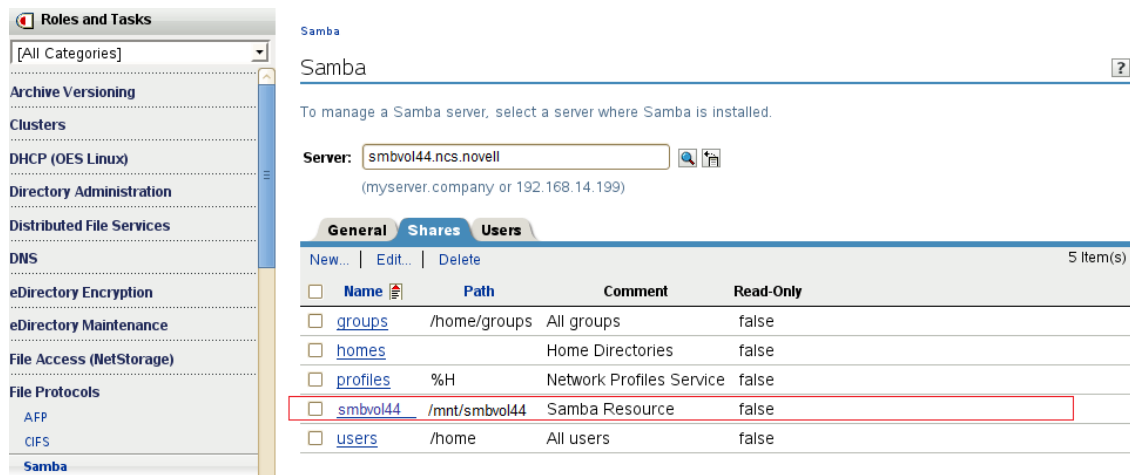
5 Click **OK** to save and apply the settings.

6 Continue with .

5.6.3 Editing the Samba Resource Configuration File

1 While the shared volume is mounted at the mount point, copy the `smb.conf` file from the `/etc/samba` directory on the primary cluster server to the mount point directory `/mnt/smbvol44` that you created in .

2 On the shared volume location, rename the copied `smb.conf` file to match the name specified for the `CONFIG_FILE` variable in the Samba cluster resource load and unload scripts.

For example, if you keep the default name, you rename the file as S`ambaResource-smb.conf`. This file is used by the load, unload, and monitor scripts to manage this clustered instance of Samba.

3 Open the `SambaResource-smb.conf` file in a text editor, then modify the file as follows:

3a In the `Entries made by OES install` section, locate the following line:

`passdb backend = NDS_ldapsam:ldaps//`*xxx.xxx.xxx.xxx*`:636`

Verify that *xxx.xxx.xxx.xxx* is the IP address of the master LDAP server for your eDirectory tree.

3b Add the following lines to the `[global]` section:

`bind interfaces only = yes`

`interfaces = `*resource_ipaddress*

`pid directory = $MOUNT_POINT/share/locks`

Replace *resource_ipaddress* with the IP address you plan to assign to the Samba cluster resource.

3c In the line `netbios name = %h-W`, change *%h-W* to something unique, such as the name you will give the Samba virtual server.

`netbios name = smbvol44-W`

4 (Conditional) If you have other instances of Samba running locally on servers in your cluster, modify the local `/etc/samba/smb.conf` file on each server where a local Samba instance is running:

4a Log in to the node as the `root` user.

4b In a text editor, open the local copy of the `/etc/samba/smb.conf` file.

4c Add the following lines to the `[global]` section:

```
bind interfaces only = yes

interfaces = server_ipaddress
```

Replace *server_ipaddress* with the IP address of the individual server where the instance of Samba is running.

Adding these lines to the server's local `smb.conf` file eliminates conflicts caused by running multiple instances of Samba on that server (that is, running a local instance and one or more shared instances).

4d Remove (or comment out) the section that defines the instance of the share you created.

The share should be active only in the shared `SambaResource-smb.conf` file on the cluster resource.

4e Save your changes.

5 Continue with Section 5.6.4, "Modifying and Bringing the Samba Cluster Resource Online," on page 46.

5.6.4 Modifying and Bringing the Samba Cluster Resource Online

You are now ready to modify the Samba resource load, unload, and monitor scripts to uncomment the lines you commented out in Section 5.5.5, "Configuring Samba Load, Unload, and Monitor Scripts," on page 35, and bring the Samba cluster resource online.

1 At a terminal console prompt, enter the following command to take the Samba cluster resource offline:

```
cluster offline resource_name
```

For example, enter

```
cluster offline smbvol44
   Status for Resource: smbvol44
   Unloading on <servername> Lives: 1
   Revision: 1
```

2 Enter the following command on all cluster nodes to stop Samba:

```
rcsmb stop
```

3 In iManager, uncomment the Samba configuration lines you previously commented out in the resource load, unload, and monitor scripts in Section 5.5.5, "Configuring Samba Load, Unload, and Monitor Scripts," on page 35.

To find the scripts, select **Clusters > Cluster Options**, select the Samba resource's name link, then select the **Scripts** tab. Click the **Load**, **Unload**, and **Monitor** script links to view and modify each script.

4 Bring the Samba cluster resource online. Select **Clusters > Cluster Manager**, select the check box next to the Samba resource, then click **Online**. The resource is brought online on a preferred node.

You can also enter the following command at a terminal console prompt to specify a node.

```
cluster online cluster_name node_name
```

5 Continue with Section 5.6.5, "Creating Samba Users and a Group for Cluster Access," on page 47.

5.6.5 Creating Samba Users and a Group for Cluster Access

The procedure for creating Samba users to access the shared Samba cluster resource is similar to the procedure for creating Samba users in a non-clustered environment. However, because you want to use only one group to provide access for all of the Samba servers in the cluster, you cannot use the default Samba users groups that are created automatically on each Samba server. Instead, you must create a single LUM-enabled group for the cluster and make your Samba users members of that group.

NOTE: The instructions below assume that you have not yet created the Samba user accounts in eDirectory. If you have existing users that you want to access the Samba cluster resource, you must individually assign them a Universal Password.

---

1 In iManager, select **Directory Administration** > **Create Object** and create a new Organizational Unit container for the Samba cluster users.

2 Select **Passwords** > **Password Policies** and assign the Samba **Default Password Policy** to the new container.

3 Select **Users** > **Create User** and create accounts for the Samba cluster users in the new container.

4 Select **Groups** > **Create Group** and create a new group for your Samba cluster users.

5 Select **Linux User Management** > **Enable Groups for Linux** and LUM-enable the group. Associate the group with the UNIX Workstation objects for all of the cluster servers.

6 Select **Groups** > **Modify Group** and add the Samba cluster users as members of the group.

7 Select **File Protocols** > **Samba** and select the primary cluster server as the Samba server to configure.

8 Click the **Users** tab, select **Add**, and add all of the Samba cluster users.

9 At the terminal prompt, enter the following commands to grant the necessary access rights to the shared Samba resource:

```
chmod 775 path
```

```
chgrp group_name path
```

Replace *path* with the mount point of the shared Samba file system (in our example, `/mnt/smbvol44`) and *group_name* with the name of the LUM-enabled group you created for Samba cluster access.

The Samba cluster users gain access rights to the shared resource because of their membership in the specified group.

You should now be able to log in as one of the Samba cluster users at a Windows workstation (without the Novell Client installed on it) and access files on the shared Samba resource. Access to this resource should continue uninterrupted when the cluster resource is migrated between preferred nodes or if there is an unexpected server failure.

6 Configuring Samba for NSS Pools and Novell Cluster Services

This section describes how to configure Samba for Novell Storage Services (NSS) pools on Open Enterprise Server 2015 SP1 (OES 2015 SP1) with Novell Cluster Services (NCS). Configuring Samba to work in a cluster ensures that the SMB/CIFS file services remain available if there is an unexpected server shutdown. Authentication for Samba users requires that they be NetIQ eDirectory users that are enabled with Linux User Management (LUM).

Novell Samba is an alternative to Novell CIFS for NSS pool access when you have both Linux volumes and NSS volumes on your servers and you want to provide access to both volume types with only SMB/CIFS. For information about configuring Novell Samba for Linux Logical Volume Manager (LVM) volume groups, see Chapter 5, "Configuring Samba for LVM Volume Groups and Novell Cluster Services," on page 23.

IMPORTANT: If you use only NSS volumes for data in your cluster, consider using Novell CIFS instead of Novell Samba. With Novell CIFS, users are not required to be LUM enabled. For information about configuring Novell CIFS in a cluster and enabling CIFS as an advertising protocol for pool cluster resources, see "Configuring CIFS with Novell Cluster Services for an NSS File System" in the *OES 2015 SP1: Novell CIFS for Linux Administration Guide*.

- Section 6.1, "NCS Installation and Configuration," on page 49
- Section 6.2, "Creating and Preparing a Pool Cluster Resource," on page 50
- Section 6.3, "Modifying the Pool Resource Scripts for Samba," on page 52
- Section 6.4, "Samba Configuration," on page 55

6.1 NCS Installation and Configuration

Novell Cluster Services for Linux must be installed on the OES 2015 SP1 server before you can configure Samba to work in a cluster. The Samba template provides scripts for a clustered Linux Logical Volume Manager (LVM) volume group, not for NSS pools. You can use lines from the Samba template's scripts for the NSS pool cluster resource.

- Section 6.1.1, "Preparing the Cluster," on page 49
- Section 6.1.2, "Installing Novell Samba," on page 50

6.1.1 Preparing the Cluster

Install Novell Cluster Services and configure the cluster. For information, see "Installing, Configuring, and Repairing Novell Cluster Services" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*.

6.1.2 Installing Novell Samba

If you have not already done so, install and configure the Novell Samba pattern on each cluster server that will share the Samba resource.

Ensure that the **Base Context for Samba Users** is set to the container where you plan to create your Samba users, or to a container above that in the eDirectory tree.

For more information on installing and configuring Novell Samba, see Chapter 3, "Installing Novell Samba for OES," on page 15.

6.2 Creating and Preparing a Pool Cluster Resource

Create a pool cluster resource, then create subdirectories on it that Samba will use.

The examples in this section use following setup. Make sure to replace the sample values with information for your configuration.

Variable	Sample Value
NSS pool name	POOL44
Volume name	VOL44
Clustered Volume name	clus1_VOL44
	\\CLUS1-POOL44-SERVER\VOL44
Mount point for the NSS volume	/media/nss/VOL44

- Section 6.2.1, "Creating a Pool Cluster Resource," on page 50
- Section 6.2.2, "Creating Subdirectories on the NSS Volume," on page 50

6.2.1 Creating a Pool Cluster Resource

Create and cluster enable an NSS pool and volume as described in "Configuring and Managing Cluster Resources for Shared NSS Pools and Volumes" in the *OES 2015 SP1: Novell Cluster Services for Linux Administration Guide*. The shared disk will contain one NSS pool and one NSS volume. You specify NCP as an advertising protocol because it is required by NSS. You can also specify Apple Filing Protocol (AFP) as an advertising protocol for the resource. The CIFS option is not selected because the option is for Novell CIFS.

6.2.2 Creating Subdirectories on the NSS Volume

You must create some subdirectories for Samba to use on the shared NSS pool that you created in Section 6.1, "NCS Installation and Configuration," on page 49.

1 Log in to Novell iManager as an administrator user.

2 In **Roles and Tasks**, select **Clusters > Cluster Manager**, then browse to select the Cluster object for the cluster.

3 Verify that the pool resource is online. If it is offline, select the check box next to the pool resource name, then click **Online**.

4 At the root of the clustered volume, create the `log` subdirectory:

   4a In **Roles and Tasks**, select **Files and Folders > New Folder**.

   4b In the **Path** field, browse to locate the clustered volume object (`clus1_VOL44`), then select the clustered volume's object , such as `\\CLUS1-POOL44-SERVER\VOL44`.

   4c In the **Folder Name** field, type `log`, then click **OK**.

5 At the root of the clustered volume, create the `share` subdirectory:

   5a In **Roles and Tasks**, select **Files and Folders > New Folder**.

   5b In the **Path** field, browse to locate the clustered volume object (`clus1_VOL44`), then select the clustered volume's object , such as `\\CLUS1-POOL44-SERVER\VOL44`.

   5c In the **Folder Name** field, type `share`, then click **OK**.

6 In the `share` folder, create the `locks` subdirectory:

   6a In **Roles and Tasks**, select **Files and Folders > New Folder**.

   6b In the **Path** field, browse to locate and select the `share` folder, such as `\\CLUS1-POOL44-SERVER\VOL44:share`.

   6c In the **Folder Name** field, type `locks`, then click **OK**.

7 In the iManager toolbar, select **View Objects** to go to the Tree View.

8 In the Tree View, browse the file system tree to verify that the folders have been created:
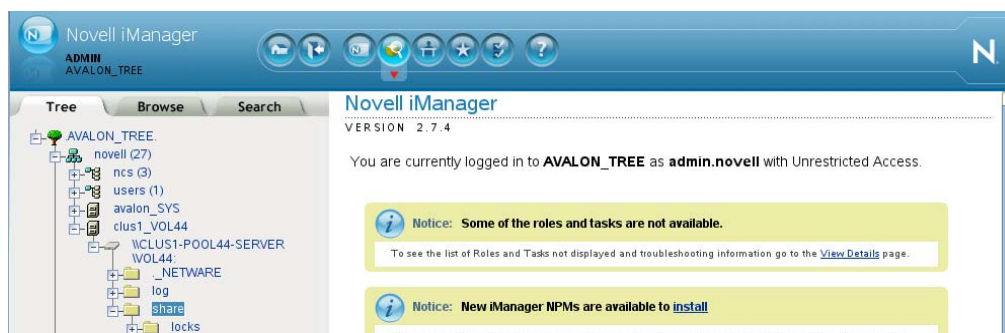
9 Continue with Section 6.3, "Modifying the Pool Resource Scripts for Samba," on page 52.

6.3 Modifying the Pool Resource Scripts for Samba

After the shared storage is properly configured, you must modify the pool cluster resource in Novell Cluster Services. This includes adding lines for Samba in the load, unload, and monitor scripts.

The examples in this section use following setup. Make sure to replace the sample values with the information for your system.

Variable	Sample Value
NSS pool name	`POOL44`
NSS volume name	`VOL44`
Pool resource IP address	10.10.10.44
NCP virtual server name	`CLUS1-POOL44-SERVER`
Volume ID	252
	Valid values are 0 to 254. By convention, volume IDs for clustered volumes are assigned as 254 and downwards.

6.3.1 Modifying the Pool Resource Load Script

1 In Novell iManager, log in as an administrator user.

2 In **Roles and Tasks**, select **Clusters > Cluster Manager**, then browse to select the Cluster object for the cluster.

3 Click the name link of the pool cluster resource to go to its Properties page, then click the **Scripts** tab.

4 View the load script.

The default pool resource load script for the sample setup is shown below. Replace the variable values in bold with the actual values for your setup.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error add_secondary_ipaddress 10.10.10.44
exit_on_error nss /poolact=POOL44
exit_on_error ncpcon mount VOL44=252

exit_on_error ncpcon bind --ncpservername=CLUS1-POOL44-SERVER
    --ipaddress=10.10.10.44

exit 0
```

5 Add the following definitions and Samba start lines to the load script.

You must specify the Linux path for the NSS volume as the MOUNT_POINT value. The configuration file name is the name you give the Samba configuration file on the shared location. The two Start Samba lines should follow the line that mounts the NSS volume.

The lines are commented out at this time. You uncomment them later when the Samba configuration file is ready.

```
# define the Linux mount point for the NSS volume
#MOUNT_POINT=/media/nss/VOL44

# define the name of the samba config file
#CONFIG_FILE=SambaResource-smb.conf


# start Samba
#exit_on_error /usr/sbin/nmbd --log-basename=$MOUNT_POINT/log --
configfile=$MOUNT_POINT/$CONFIG_FILE

#exit_on_error /usr/sbin/smbd --log-basename=$MOUNT_POINT/log --
configfile=$MOUNT_POINT/$CONFIG_FILE
```

6 Click **Apply**.

7 Continue with Section 6.3.2, "Modifying the Pool Resource Unload Script," on page 53.

6.3.2   Modifying the Pool Resource Unload Script

1 Continue from Section 6.3.1, "Modifying the Pool Resource Load Script," on page 52.

2 On the **Scripts** tab for the pool cluster resource, click the **Unload** link to view the unload script.

3 View the unload script.

The default pool resource unload script for the sample setup is shown below. Replace the variable values in bold with the actual values for your setup.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

ignore_error ncpcon unbind --ncpservername=CLUS1-POOL44-SERVER --
ipaddress=10.10.10.44

ignore_error nss /pooldeact=POOL44
ignore_error del_secondary_ipaddress 10.10.10.44

exit 0
```

4 Add the following definitions and Samba stop lines to the unload script.

You must specify the Linux path for the NSS volume as the MOUNT_POINT value. The configuration file name is the name you give the Samba configuration file on the shared location. The two Stop Samba lines should precede the line that unmounts the NSS volume.

The lines are commented out at this time. You uncomment them later when the Samba configuration file is ready.

```
# define the Linux mount point for the NSS volume
#MOUNT_POINT=/media/nss/VOL44


# define the name of the samba config file
#CONFIG_FILE=SambaResource-smb.conf

# request Samba stop
#ignore_error killproc -p $MOUNT_POINT/nmbd-$CONFIG_FILE.pid /usr/sbin/nmbd
#ignore_error killproc -p $MOUNT_POINT/smbd-$CONFIG_FILE.pid /usr/sbin/smbd
```

5 Click **Apply**.

6 Continue with Section 6.3.3, "Modifying the Pool Resource Monitor Script," on page 54.

6.3.3 Modifying the Pool Resource Monitor Script

1 Continue from Section 6.3.2, "Modifying the Pool Resource Unload Script," on page 53.

2 On the **Scripts** tab for the pool cluster resource, click the **Monitor** link to view the monitor script.

3 View the monitor script.

The default pool resource monitor script for the sample setup is shown below. Replace the variable values in bold with the actual values for your setup.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error status_fs /dev/pool/POOL44 /opt/novell/nss/mnt/.pools/POOL44
nsspool

exit_on_error status_secondary_ipaddress 10.10.10.44
exit_on_error ncpcon volume VOL44

exit 0
```

4 Add the following definitions and Samba check status lines to the monitor script.

You must specify the Linux path for the NSS volume as the MOUNT_POINT value. The configuration file name is the name you give the Samba configuration file on the shared location. The two check status Samba lines can follow the check of the NSS volume.

The lines are commented out at this time. You uncomment them later when the Samba configuration file is ready.

```
# define the Linux mount point for the NSS volume
#MOUNT_POINT=/media/nss/VOL44


# define the name of the samba config file
#CONFIG_FILE=SambaResource-smb.conf

# check Samba
#exit_on_error checkproc -p $MOUNT_POINT/share/locks/smbd-$CONFIG_FILE.pid /
usr/sbin/smbd
#exit_on_error checkproc -p $MOUNT_POINT/share/locks/nmbd-$CONFIG_FILE.pid /
usr/sbin/nmbd
```

5 Click **Apply**.

6 At the bottom of the page, click **OK** to save all changes for the pool cluster resource.

IMPORTANT: The changes are not effective until the resource is taken offline and brought online again.

---

7 Continue with Section 6.4, "Samba Configuration," on page 55.

6.4   Samba Configuration

Now that you have installed and configured Novell Cluster Services and created the Samba cluster resource, you are ready to configure Samba on each cluster server.

- Section 6.4.1, "Disabling Samba Start at Reboot," on page 55
- Section 6.4.2, "Creating a Samba Share," on page 55
- Section 6.4.3, "Editing the Samba Resource Configuration File," on page 56
- Section 6.4.4, "Bringing the Samba Cluster Resource Online," on page 57
- Section 6.4.5, "Creating Samba Users and a Group for Cluster Access," on page 57

6.4.1   Disabling Samba Start at Reboot

If you do not have a local Samba instance running on each server, you can disable Samba from being started when the server boots. The resource starts a Samba instance when the resource is brought online.

1 Enter the following command on all preferred nodes in the cluster that are assigned to the Samba resource:

```
chkconfig smb off
```

This command ensures that Samba is not started until it is required for a resource migration or failover.

2 Continue with Section 6.4.2, "Creating a Samba Share," on page 55.

6.4.2   Creating a Samba Share

In OES, you can use the new Samba management plug-in for iManager to create a new Samba share, instead of manually adding a share definition in the `/etc/samba/smb.conf` file.

1 In iManager's Roles and Tasks, select **File Protocols** > **Samba**.

2 In the **Server** field, browse and select the server where the Samba resource is currently online.

3 Wait for the general Samba information to be displayed, then click the **Shares** tab.

4 Click **New** and follow the on-screen prompts to create a share that maps to the mount point you defined for the Samba cluster resource.

- **Share Name:** Specify the share name, such as `smbvol44`.
- **Path:** Specify the path of the mount path you defined for the Samba Resource, such as `/media/nss/VOL44`.
- **Comment:** Specify a brief description about the purpose of this share, such as `NSS VOL44 Samba Resource`.
- **Inherit ACLs:** Select this option.

5 Click **OK** to save and apply the settings.

6 Continue with Section 6.4.3, "Editing the Samba Resource Configuration File," on page 56.

6.4.3 Editing the Samba Resource Configuration File

1 While the shared volume is mounted, copy the `smb.conf` file from the `/etc/samba` directory on the primary cluster server to the mount point directory, such as `/media/nss/VOL44`.

2 On the shared volume location, rename the copied `smb.conf` file to match the name specified for the `CONFIG_FILE` variable in the Samba cluster resource load and unload scripts.

For example, if you keep the default name, you rename the file as S`ambaResource-smb.conf`. This file is used by the load, unload, and monitor scripts to manage this clustered instance of Samba.

3 Open the `SambaResource-smb.conf` file in a text editor, then modify the file as follows:

   3a In the `Entries made by OES install` section, locate the following line:

       `passdb backend = NDS_ldapsam:ldaps//`*`xxx.xxx.xxx.xxx`*`:636`

       Verify that *xxx.xxx.xxx.xxx* is the IP address of the master LDAP server for your eDirectory tree.

   3b Add the following lines to the `[global]` section:

       `bind interfaces only = yes`

       `interfaces = `*`resource_ipaddress`*

       `pid directory = $MOUNT_POINT/share/locks`

       Replace *resource_ipaddress* with the IP address you plan to assign to the Samba cluster resource.

   3c In the line `netbios name = %h-W`, change *%h-W* to something unique, such as the name you will give the Samba virtual server.

       `netbios name = smbvol44-W`

4 (Conditional) If you have other instances of Samba running locally on servers in your cluster, modify the local `/etc/samba/smb.conf` file on each server where a local Samba instance is running:

   4a Log in to the node as the `root` user.

   4b In a text editor, open the local copy of the `/etc/samba/smb.conf` file.

   4c Add the following lines to the `[global]` section:

       `bind interfaces only = yes`

       `interfaces = `*`server_ipaddress`*

       Replace *server_ipaddress* with the IP address of the individual server where the instance of Samba is running.

       Adding these lines to the server's local `smb.conf` file eliminates conflicts caused by running multiple instances of Samba on that server (that is, running a local instance and one or more shared instances).

   4d Remove (or comment out) the section that defines the instance of the share you created.

       The share should be active only in the shared `SambaResource-smb.conf` file on the cluster resource.

   4e Save your changes.

5 Continue with .

6.4.4 Bringing the Samba Cluster Resource Online

You are now ready to modify the Samba resource load, unload, and monitor scripts to uncomment the lines you commented out in Section 6.3, "Modifying the Pool Resource Scripts for Samba," on page 52, and bring the Samba cluster resource online.

1 At a terminal console prompt, enter the following command to take the Samba cluster resource offline:

```
cluster offline resource_name
```

For example, enter

```
cluster offline POOL44_SERVER
  Status for Resource: POOL44_SERVER
  Unloading on <servername> Lives: 1
  Revision: 1
```

2 Enter the following command on all cluster nodes to stop Samba:

```
rcsmb stop
```

3 Using iManager, uncomment the Samba configuration lines you previously commented out in the resource load, unload, and monitor scripts in Section 6.3, "Modifying the Pool Resource Scripts for Samba," on page 52.

To find the scripts, select **Clusters > Cluster Options**, select the Samba resource's name link to go to its Properties page, then select the **Scripts** tab. Click the **Load**, **Unload**, and **Monitor** script links to view and modify each script. Click **OK** to save and apply your changes.

4 Bring the pool cluster resource online. Select **Clusters > Cluster Manager**, select the check box next to the pool cluster resource, then click **Online**. The resource is brought online on a preferred node.

You can also enter the following command at a terminal console prompt to specify a node.

```
cluster online cluster_name node_name
```

5 Continue with Section 6.4.5, "Creating Samba Users and a Group for Cluster Access," on page 57.

6.4.5 Creating Samba Users and a Group for Cluster Access

The procedure for creating Samba users to access the shared Samba cluster resource is similar to the procedure for creating Samba users in a non-clustered environment. However, because you want to use only one group to provide access for all of the Samba servers in the cluster, you cannot use the default Samba users groups that are created automatically on each Samba server. Instead, you must create a single LUM-enabled group for the cluster and make your Samba users members of that group.

NOTE: The instructions below assume that you have not yet created the Samba user accounts in eDirectory. If you have existing users that you want to access the Samba cluster resource, you must individually assign them a Universal Password.

---

1 In iManager, select **Directory Administration** > **Create Object** and create a new Organizational Unit container for the Samba cluster users.

2 Select **Passwords** > **Password Policies** and assign the Samba Default Password Policy to the new container.

3 Select **Users** > **Create User** and create accounts for the Samba cluster users in the new container.

4 Select **Groups** > **Create Group** and create a new group for your Samba cluster users.

5 Select **Linux User Management** > **Enable Groups for Linux** and LUM-enable the group. Associate the group with the UNIX Workstation objects for all of the cluster servers.

6 Select **Groups** > **Modify Group** and add the Samba cluster users as members of the group.

7 Select **File Protocols** > **Samba** and select the primary cluster server as the Samba server to configure.

8 Click the **Users** tab, select **Add**, and add all of the Samba cluster users.

9 At the terminal prompt, enter the following commands to grant the necessary access rights to the shared Samba resource:

```
chmod 775 path
```

```
chgrp group_name path
```

Replace *path* with the mount point of the shared Samba file system (in our example, `/mnt/smbvol44`) and *group_name* with the name of the LUM-enabled group you created for Samba cluster access.

The Samba cluster users gain access rights to the shared resource because of their membership in the specified group.

You should now be able to log in as one of the Samba cluster users at a Windows workstation (without the Novell Client installed on it) and access files on the shared Samba resource. Access to this resource should continue uninterrupted when the cluster resource is migrated between preferred nodes or if there is an unexpected server failure.

7 Creating Users and Groups for Samba

The procedures for creating and enabling Samba users have been greatly simplified in Open Enterprise Server 2015 SP1(OES 2015 SP1). If your implementation allows you to use the default Samba password policy and the default Samba users group, many of the steps that were done manually in OES 1.0 can be eliminated.

This section covers the following topics:

- Section 7.1, "Creating eDirectory Users for Samba," on page 59
- Section 7.2, "Creating a Samba Group," on page 61

7.1 Creating eDirectory Users for Samba

- Section 7.1.1, "Creating an eDirectory Container for User Objects," on page 59
- Section 7.1.2, "Creating eDirectory Users in iManager," on page 60

7.1.1 Creating an eDirectory Container for User Objects

IMPORTANT: Samba users must be created in a container at or below the Base Context for Samba Users that you specified when you installed Samba. By default, the base context is the container where the eDirectory admin user object resides. If you need to change the context, see the instructions in Section B.2.4, "Changing the LDAP Suffix," on page 99.

The eDirectory users must also be assigned a Samba-compliant password policy, such as the Samba Default Password Policy provided in OES. A password policy can be assigned to individual users containers, or partitions. It is generally easier to assign the policy at the container level. For more information, see the online help for the iManager **Passwords** task.

Step 3 below instructs you on how to assign the default Samba policy to User object containers. However, you also have two other options:

- If you want to create a new policy, go to Section 11.2.3, "Creating a New Samba-Qualified Password Policy," on page 88.
- If you want to modify an existing policy, go to Section 11.2.4, "Modifying an Existing Password Policy for Samba," on page 89.

If you create your own policy or modify an existing policy, be sure to select the appropriate policy in place of the Samba Default Password Policy in Step 3 on page 59.

User objects that don't meet these requirements cannot be enabled for Samba access.

1 In your browser, enter the iManager URL (http://*IP_address_or_DNS_name*/iManager.html) and log in as the eDirectory Admin user or equivalent.

2 In the Roles and Tasks view, select **Directory Administration > Create Object > Organizational Unit** and create the OU object at the correct context for your Samba users.

3 To assign the default Samba Password Policy to the new container, select **Passwords** > **Password Policies** > **Samba Default Password Policy**.

4 On the Password Policy page, click the **Policy Assignment** tab.

5 Browse 🔍 to and select the container object you created for your Samba users, then click **OK > OK**.

6 Continue with .

7.1.2 Creating eDirectory Users in iManager

IMPORTANT: If you want to create home directories for your users as part of the user-creation process, you must create an NSS volume or an NCP volume for the directories before completing the following procedure. For more information, see "Managing NSS Volumes" in the *OES 2015 SP1: NSS File System Administration Guide for Linux* or "Creating NCP Volumes on Linux File Systems" in the *OES 2015 SP1: NCP Server for Linux Administration Guide*.

1 In iManager's Roles and Tasks view, select **Users > Create User**.

TIP: To see whether a User object already exists, click the **View Objects** icon. Click the **Search** tab. Set the **Type** to **User**, and click **Search**. All currently defined User objects are listed.

2 For **Username**, specify the corresponding Windows user account name. You must also specify the user's last name in the Last Name field. Specifying the first name is optional.

3 For **Context**, be sure to select the container you created for your Samba users in .

4 For **Password**, specify an eDirectory password that matches the Windows password for the user.

IMPORTANT: Do not select **Set simple password** even though the interface indicates it is required for native Windows file access. As long as the Samba Password Policy has been set on the container or partition before you create the user, a Universal Password is created by default, which makes it much easier for users to keep their passwords synchronized.

5 (Conditional) If you have an NSS or NCP volume available and you want the user's home directory to be created automatically, select the **Create Home Directory** option.

Browse 🔍 to and select the volume, then specify the path to where you want the user's home directory to be created.

NOTE: The path you specify must already exist on the NSS or NCP volume.

6 Type or select any other information you want associated with the user, such as **Title** and **Location**.

7 Click **OK**.

8 Click **Repeat Task** to create another user, or click **OK** to finish.

9 After creating eDirectory users for all of your Windows workstation users that you want to have Samba access, continue with .

7.2 Creating a Samba Group

The Novell Samba configuration automatically creates a default Samba users group for every Samba server. This group is already LUM-enabled and is designed to make the process of enabling users for Samba easier. Read Section 7.2.1, "About the Default Samba Users Group," on page 61 to determine whether this default group can meet your needs or whether you need to create your own Samba group.

7.2.1 About the Default Samba Users Group

A default Samba users group is created automatically on every OES server that has Novell Samba installed. The default group is named *server_name*-W-SambaUserGroup. When you use the Samba management plug-in for iManager to add Samba users, the users are automatically made members of this group. Removing Samba users with the plug-in only removes the users as members of the default Samba users group. It does not affect their membership in other groups that might be created for Samba access.

The default Samba users group does not specify SSH as an allowed service. If you want to allow your Samba users SSH access (for instance, if you are using NetStorage and you want your Samba users to access NetStorage Storage Location Objects based on SSH), you must either modify the default Samba users group to allow SSH access or create a new Samba group that is LUM-enabled and specifies SSH as an allowed service. If you create a new group, the Samba users must be removed from the default Samba users group because SSH access is only granted when all of the groups to which a user belongs allow it. For more information, see "SSH Services on OES 2015" in the *OES 2015 SP1: Planning and Implementation Guide*.

If the default Samba users group meets the needs of your Samba implementation, skip to Section 8.4, "Managing Samba Users," on page 69 to continue the process of adding users to your Samba server.

If you need to create your own Samba group, continue with Section 7.2.2, "Creating an eDirectory Group and Assigning Users to It," on page 61.

7.2.2 Creating an eDirectory Group and Assigning Users to It

If you cannot use the default Samba group, you can create a new Group object for managing a subset of Samba users.

1 If your eDirectory users are already members of a group you can enable for Linux access, skip to Section 7.2.3, "Enabling the Group for Linux Access (LUM)," on page 62.

2 Click **Groups > Create Group**,

3 Type a name for the group.

4 Select a context for the group. Although Group objects are often in the same container as the User objects assigned to them, this is not required.

5 Click **OK**.

6 Click **Modify**.

7 Select the **Members** tab.

8 Browse 🔍 to the users you want to add to the group, click each User object, then click **OK**.

9 Click **Apply > OK**.

10 Continue with Section 7.2.3, "Enabling the Group for Linux Access (LUM)," on page 62.

7.2.3 Enabling the Group for Linux Access (LUM)

1 Enable the group you just created for Linux access by selecting **Linux User Management > Enable Groups for Linux**.

2 In the Enable Groups for Linux page, select the group you just created.

3 Make sure that the **Linux-Enable All Users in These Groups** option is selected, then click **Next**.

4 Confirm that you want to enable the users for Linux by clicking **Next**.

5 Browse 🔍 to and select the UNIX Workstation - *server_name* object of each server you want users to have Samba access to, then click **OK.**

   UNIX Workstation objects are created in the same context as the servers they represent.

6 Click **Next**, then click **Finish**.

7 To add eDirectory users as Samba users in iManager, see Section 8.4, "Managing Samba Users," on page 69.

   With the Samba plug-in for iManager, you can add up to 500 users at once. An alternative command line method for Samba-enabling existing users is to use the `smbbulkadd` utility as explained in Section 7.2.4, "Samba-Enabling Users with smbbulkadd," on page 62.

7.2.4 Samba-Enabling Users with smbbulkadd

You can enable multiple eDirectory users for Samba by running the `smbbulkadd` utility at the terminal prompt.

Prerequisites

☐ The users must already exist in eDirectory and must be assigned a Samba-qualified password policy, as described in Section 7.1.1, "Creating an eDirectory Container for User Objects," on page 59.

☐ The users must also be members of a Samba group that has been LUM-enabled for Linux access.

   You can either make the users members of the default Samba users group, which is already LUM-enabled, or create your own Samba group as instructed in Section 7.2.2, "Creating an eDirectory Group and Assigning Users to It," on page 61 and Section 7.2.3, "Enabling the Group for Linux Access (LUM)," on page 62).

   If you need to add a large number of users to a LUM-enabled group, you can run the `nambulkadd` utility to perform the LUM-enabling and group assignment tasks that are prerequisite to running `smbbulkadd`. When you run `numbulkadd`, you specify the primary group and/or secondary group(s) when LUM-enabling users. You can then run `smbbulkadd` to update the User objects to include Samba-specific schema information.

   For instructions on how to run `nambulkadd`, see "Using Command Line Utilities to Manage Users and Groups" in the *OES 2015 SP1: Linux User Management Administration Guide*.

Running the smbbulkadd Utility

To enable Linux-enabled users for Samba access, do the following:

1 Using your favorite Linux text editor (such as gedit or vi), create a text file that lists the following information for each user on a separate line. Be sure to include a blank line at the end of the file as indicated:

```
-u username -x edir,context -p password
(blank line—no text)
```

where *username* is the eDirectory username, *edir,context* is the full eDirectory context of the user expressed using LDAP (comma-delimited) syntax, and *password* is the same password used to log in to the Windows workstation.

IMPORTANT: Both the eDirectory password and the Universal Password will be set to the password you specify.

For example, to Samba-enable three Linux-enabled eDirectory users named win1, win2, and win3 in users.doc.company, with the passwords pass1, pass2, and pass3, respectively, you could create a file named `smbusers.txt` in the `/tmp` directory with the following contents:

```
-u win1 -x ou=users,ou=doc,o=company -p pass1

-u win2 -x ou=users,ou=doc,o=company -p pass2

-u win3 -x ou=users,ou=doc,o=company -p pass3

(blank line—no text)
```

NOTE: You can also create the text file on a Macintosh or Windows workstation, but you must convert the file to UNIX text format using the `dos2unix` utility before using it with smbbulkadd.

---

2 While logged in to the server as the `root` user, run the `smbbulkadd` command.

To see the various command options, enter `smbbulkadd` at the shell prompt.

For example, to process the `smbusers.txt` file mentioned in the example in Step 1, you would enter the following command at the shell prompt:

```
smbbulkadd -a cn=admin,o=company -w adpass -f /tmp/smbusers.txt
```

where *adpass* is the eDirectory Admin user password.

The system reports the status for each user being enabled for Samba.

3 Check the status reported to ensure that all users were enabled. If not, correct any errors in the `smbusers.txt` file, such as no blank line at the end, and run `smbbulkadd` again.

Users that are already enabled are ignored.

4 After your users are enabled to use Samba file services, you need to grant access rights to the Samba shares. For instructions, see Section 8.5, "Typical Samba Configuration Scenarios," on page 71.

8 Managing Samba Servers, Shares, and Users

Open Enterprise Server 2015 SP1(OES 2015 SP1) includes a Samba management plug-in for iManager to help administrators manage Samba servers, shares, and users. Whenever possible, you should use the iManager plug-in to manage Samba, as documented in this section.

This section covers the following topics:

8.1 About the Samba Management Plug-in

The Samba management plug-in for iManager is designed to help administrators work with Samba servers in the OES environment. It uses a Common Information Model (CIM) provider to exchange management information with OES servers that are running Samba 3.*x* in an OES-supported configuration.

The Samba management plug-in cannot be used to manage Samba 3.*x* running on a SUSE Linux Enterprise Server 10 (non-OES) server.

8.2 Managing the Samba Server

This section covers the following tasks that are performed via the Samba management plug-in for iManager:

8.2.1 Selecting a Samba Server to Manage

To select the Samba server you want to manage:

1 Start iManager by pointing your browser to the following URL:

   `http://IP_address_or_DNS_name/iManager.html`

   Substitute the IP address or DNS name of a server that has iManager installed.

2 In the Roles and Tasks view, select **File Protocols** > **Samba**.

3 Use one of these methods to select a server:

- ◆ Type the eDirectory distinguished name or IP address for the server you want to manage (for example: srv1.servers.novell or 192.168.2.1), then click **OK**.

- ◆ Click the Search icon to open the eDirectory Object Selector. Browse or search the list to locate the server you want to manage, then click the server name.

- ◆ Click the Object History icon to select a server you have recently managed.

NOTE: The browse and search functions find only NetWare Core Protocol (NCP) Server objects. If you want to manage Samba on an OES server that doesn't have an NCP Server object (for example, if NetIQ eDirectory is not running on the server), you must enter the server's IP address.

8.2.2 Viewing General Information about the Samba Server

After iManager connects to an OES server running Samba, the **General** page is displayed.
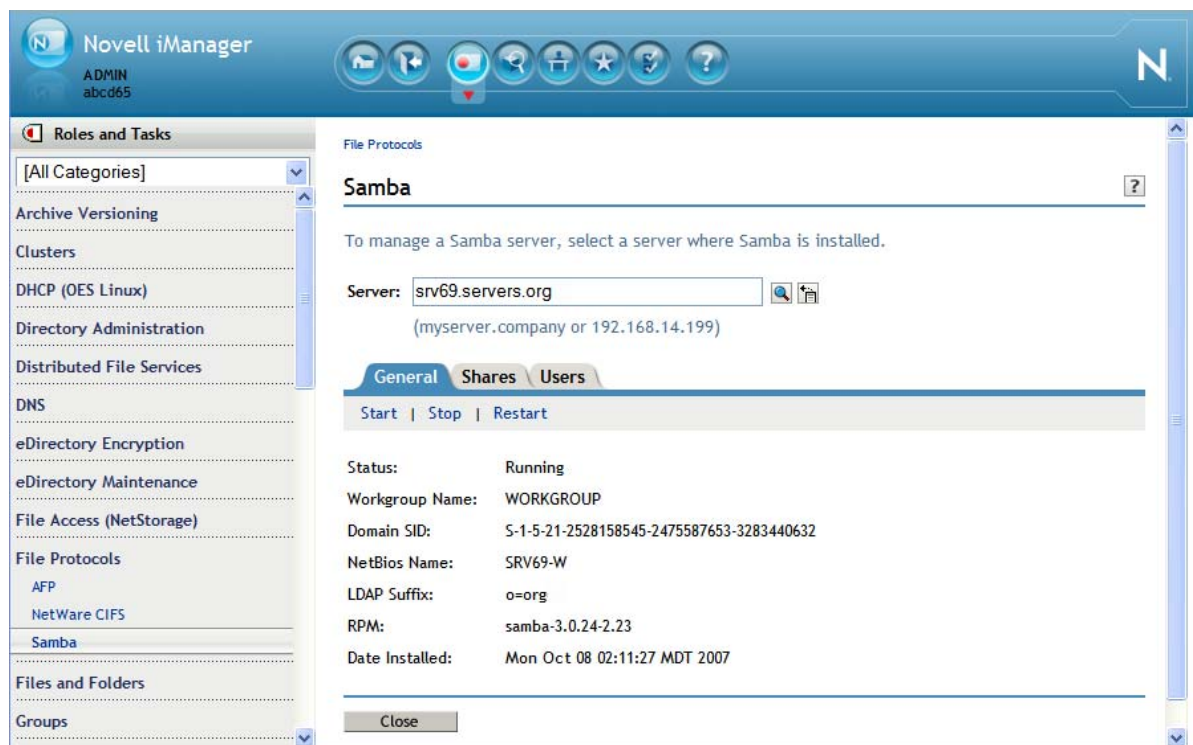
This page provides the following information:

- ◆ Status: The current status of the Samba server (Running or Stopped).

- ◆ Workgroup Name: The workgroup name configured for the server. The default workgroup name for OES Samba servers is WORKGROUP.

- ◆ Domain SID: The unique Security ID number generated for this particular combination of machine name (hostname) and domain name (workgroup).

- ◆ NetBios Name: The name displayed for the server when browsing the network; by default, the DNS hostname with "-W" appended to it. This prevents a name collision with the NCP Server object.

- LDAP Suffix: The eDirectory context where the Samba domain object (*hostname*-W) is created and where the default Samba group (*hostname*-W-SambaUserGroup) is located. It is also the base context that the Samba server uses to search for User objects in eDirectory.
- RPM: The name and version of the Samba software running on the server.
- Date Installed: The date and time the server was installed.

For more detailed information, including how to reconfigure the Workgroup Name, NetBios Name, and LDAP Suffix, see Section B.2, "Changing the Samba Server Configuration," on page 98.

8.2.3 Starting and Stopping the Samba Server

You must restart Samba every time you make a manual change to the Samba configuration file (`/etc/samba/smb.conf`). You do not need to restart Samba after making changes via the Samba management plug-in for iManager.

These tasks are available on the Samba management **General** page in iManager:

- To start Samba, click **Start**.
- To stop Samba, click **Stop**.
- To restart Samba, click **Restart**. (Restart is the same as a Stop followed by a Start.)

8.3 Managing Samba Shares

In Samba, a share is a location on the server's file system that is made available for multiple users on the network to access and store files. These appear to Windows users as normal folders accessible via the network.

This section covers the following share-related tasks that are performed via the Samba management plug-in in iManager:

- Section 8.3.1, "Viewing the Existing Samba Shares," on page 67
- Section 8.3.2, "Creating a Samba Share," on page 68
- Section 8.3.3, "Editing a Samba Share," on page 68
- Section 8.3.4, "Deleting a Samba Share," on page 69

8.3.1 Viewing the Existing Samba Shares

The default Samba shares on an OES server include the following:

- [homes] is a special section of the Samba configuration that defines parameters for the automatic creation of home directories.
- [users] is a standard location for users' private work areas (`/home`).
- [groups] is a standard location for group work areas (`/home/groups`).
- [profiles] is a special section that defines parameters for network profiles.

Refer to the SLES 11 Samba documentation (http://www.suse.com/documentation/sles11/book_sle_admin/data/cha_samba.html) for more information about these default share entries.

The list also includes any additional shares you have created on the server.

8.3.2 Creating a Samba Share

To create a new Samba share:

1 Select the **Shares** tab and click **New**.

2 In the **Share Name** field, type a name that complies with the naming guidelines shown. The share name does not have to match the folder name. It should be a descriptive label that reflects the share's purpose.

3 In the **Path** field, type the full path to the folder you want to share; for example, `/home/projects/xyz/data`. The folder must already exist on the OES server. The share includes this folder and its subfolders.

4 (Optional) In the **Comment** field, type a description that identifies the share; for example, "Data directory for the XYZ project".

5 Select whether you want the share to be Read-Only (the default is no, or Read-Write) and whether you want the inherit ACLs feature enabled (the default is yes).

6 Click **OK** to create the share.

Or click **Cancel** to return to the previous page without creating the share.

8.3.3 Editing a Samba Share

To edit an existing Samba share:

1 Select the **Shares** tab and either click the name of the share, or select the share and click **Edit**.

2 In the **Path** field, type another existing path for the share.

3 In the **Comment** field, edit the comment string associated with the share.

4 Select whether you want the share to be Read-Only (the default is no, or Read-Write) and whether you want the inherit ACLs feature enabled (the default is yes).

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

Or click **Cancel** to return to the previous page without saving the changes.

8.3.4 Deleting a Samba Share

To delete one or more Samba shares:

1 Select the **Shares** tab.

2 Select the shares you want to delete, then click **Delete**.

8.4 Managing Samba Users

The **Users** page displays the eDirectory users that have been granted access to this Samba server, along with their context and group membership information.

This section covers the following user-related tasks that are performed via the Samba management plug-in in iManager:

8.4.1 Adding Samba Users

Adding a user enables Samba access by making the user a member of the default Samba Users Group.

IMPORTANT: Before you add eDirectory users to give them access to this Samba server, make sure that the users have been created in a container with a Samba-compliant password policy and that they have Universal Passwords. You cannot assign a password policy to a group; only to containers, partitions, and individual users.

Adding users automatically LUM enables them if they are not already LUM-enabled and Samba enables them if they are not already Samba-enabled. It also makes each user a member of the default Samba group for this server (*server_name*-W-SambaUserGroup) and makes that group the primary group.

NOTE: The default Samba group denies access to the ssh service even if it has been LUM-enabled. It grants access to all other LUM-enabled services running on this server. The exact list depends on which services you selected when you configured Linux User Management. You can enable or disable access to these services by editing the Linux profile of the group (**Groups** > **Modify Group** > specify group > **Linux Profile** > **Linux Services**).

The Samba plug-in only adds and removes users from the default Samba group. If you want to use another group specifically for enabling Samba access, create a new group with the desired Samba users as members, then use the Linux User Management plug-in to enable the group for Linux. You can also modify the new group's Linux profile to enable access to LUM-enabled services. Then use the smbbulkadd command-line tool, referencing the users in the new group, to Samba-enable the users.

If a user is already a member of another LUM-enabled group, adding the user as a Samba user changes the user's primary group to the default Samba group. Depending on how you have set up group access to Linux services on this particular workstation, the user might lose access to Linux services that were previously allowed.

To add one or more new Samba users for this server:

1 Select the **Users** tab.
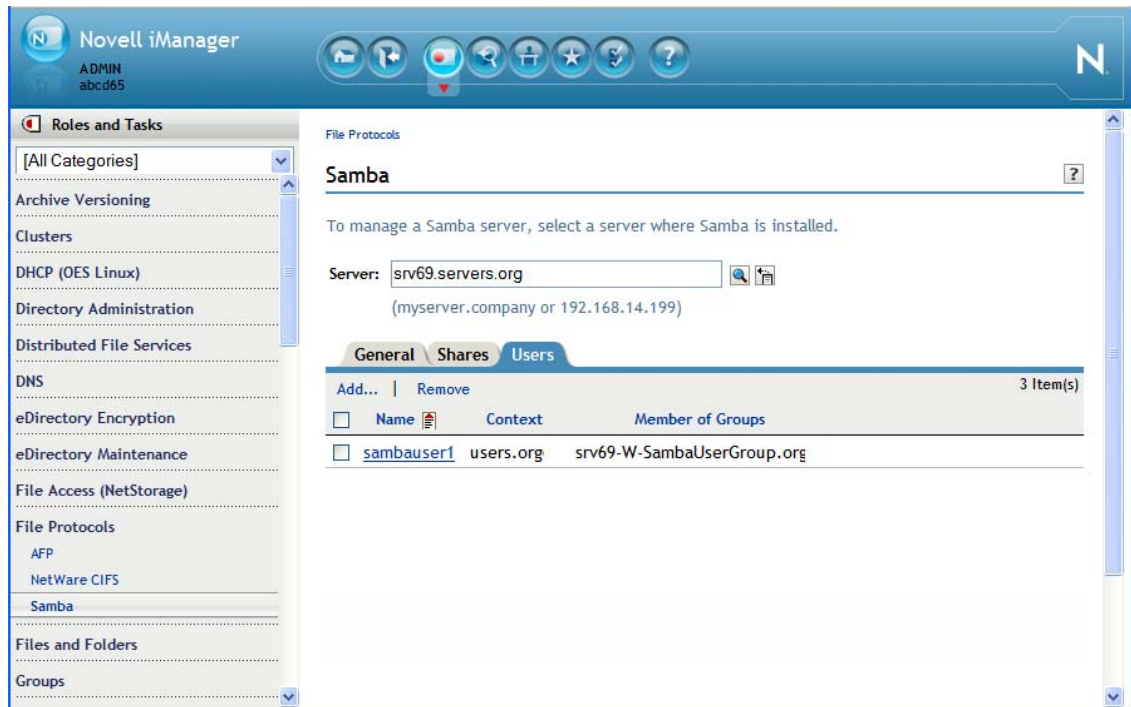
2 Click **Add**.

3 Use one of the following methods to select the users you want to give access to this server:

* To select a single User object to add, click **Select a Single Object**.

* To select multiple User objects to add, click **Select Multiple Objects**.

* To select User objects to add from a list, click **Simple Selection**.

* Click the Search icon to open the Object Selector and browse or search the list to locate the User objects you want to add.

* Click the Object History icon to select User objects you have recently managed.

4 Click **OK** to finish adding the users.

Or click **Cancel** to return to the previous page without adding the selected users.

8.4.2 Removing Samba Users

Removing a user revokes that user's membership in the default Samba group, which disables that user's Samba access. It does not delete the User object in eDirectory or remove the user's UID.

IMPORTANT: Removing users does not disable Samba access if the users are members of other LUM-enabled groups associated with this Samba server. If a user is a member of only the default Samba Users Group, removing the user disables that user's access to any Linux services that were enabled for the group. If the user is a member of other groups, the user retains LUM access to Linux services enabled for those groups.

To remove one or more users as Samba users for this server:

1 Select the **Users** tab.

2 Select the users you want to remove.

3 Click **Remove**.

8.5 Typical Samba Configuration Scenarios

Samba configurations can be as simple or as complex as you need them to be. This section contains some basic guidelines and examples for using the Samba Management plug-in for iManager and other tools to set up Samba access in an OES environment.

8.5.1 Setting Up a Workgroup and Shares (Access Points)

Users need to be able to access the Samba server in My Network Places and Windows Explorer just as they would a Windows server. This means that the server needs to be assigned to a workgroup and it needs to publish Windows shares (access points) that are visible to users.

The Importance of Changing the Default Workgroup Setting

When users browse the network from Windows workstations, they can typically see only the Windows workstations and servers in the same workgroup. Because WORKGROUP is the default workgroup name for all Windows 2000 and Windows XP workstations in an OES network, the WORKGROUP workgroup can contain hundreds of workstations and servers, rendering it nearly unusable.

For instructions on how to change the workgroup setting for your Samba server, see Section B.2.1, "Changing the Workgroup Name," on page 98.

Types of Samba Shares

By default, the Samba server publishes certain preconfigured shares. However, these defaults are insufficient for many Samba installations. For example, the **users** share, as it is defined by default, provides access by authenticated users to all the home directories on a traditional Linux volume.

Before your users can access Samba services, they must have rights to one or more work directories on the Samba server. There are various kinds of work areas: private, shared by a group, or publicly available. Home directories are usually private, whereas collaboration directories are shared by a group.

The following sections provide guidelines for customizing the default share configurations and setting up shares for private and group access.

8.5.2 Creating Private Home Directories for Samba Users

If you have previously administered Samba servers outside of an OES context, you might expect that user home directories are automatically created the first time a user logs in to the Samba server.

This is not the case in OES because Samba is not a PAM-enabled service. (See "OES Services That Require LUM-Enabled Access" in the *OES 2015 SP1: Planning and Implementation Guide*.) Therefore, if you plan to provide Samba users with home directories, you must determine an alternate method for creating them.

Types of Volumes for Home Directories

On an OES server, there are three basic types of volumes you can use for creating home directories:

- Traditional Linux volumes (`/home`)
- Traditional Linux volumes that are also configured as NCP volumes
- NSS volumes (which are also NCP volumes by definition)

Table 8-1 summarizes the Samba accessibility to home directories for each volume type:

Table 8-1   Home Directory Accessibility by Volume Type

Volume Type	Creation Method	Access Control	Initial Accessibility	Notes and Caveats
Traditional Linux	Log in as the user to a PAM-enabled service (Samba is not PAM-enabled. Therefore, logging in to Samba doesn't create home directories, as explained in Section A.5, "Home Directory Creation Is Not Automatic," on page 92.)	POSIX file attributes	- Visible - all home directories can be seen by an authenticated user. - Browseable - the content of all home directories is browseable. - Modifiable - owners can modify the content of their own home directories. Group and Other users can't modify the content of directories they don't own.	To make the contents of home (and other) directories private (non-browseable), use chmod to change the file attributes so that only the owner has rights. For instructions, see "Providing a Private Work Directory" in the *OES 2015 SP1: Planning and Implementation Guide*. Alternatively, you can modify the [homes] share in the smb.conf file as explained in Section 8.5.3, "Creating Home Directories on Traditional Linux Volumes," on page 74. Following these instructions hides the home directories in Samba because users see only their home directory contents and not the home directory itself.

Volume Type	Creation Method	Access Control	Initial Accessibility	Notes and Caveats
NCP on Traditional Linux	iManager at user-creation time	POSIX file attributes	◆ Visible - all home directories can be seen by an authenticated user. ◆ Browseable - initially no users can see directory contents. This is because the users are not the directory owners from a POSIX perspective. See the additional explanation in the next column. ◆ Modifiable - initially the user can't modify directory contents because the user is not the directory owner from a POSIX perspective. See the additional explanation in the next column.	To make these home directories browseable and modifiable for the directory owner, you must use `chown` to change the POSIX owner from the eDirectory Admin user to the actual user. For instructions, see Section 8.5.4, "Creating Home Directories Using iManager," on page 76. After changing POSIX directory ownership, other users are still not able to browse or modify directory contents because iManager assigns no POSIX Group or Other file attributes when it creates the directory.
	Log in as the user to a PAM-enabled service (Samba is not PAM-enabled. Therefore, logging in to Samba doesn't create home directories, as explained in Section A.5, "Home Directory Creation Is Not Automatic," on page 92.	POSIX file attributes	◆ Visible - all home directories can be seen by an authenticated user. ◆ Browseable - the content of all home directories is browseable. ◆ Modifiable - owners can modify the content of their own home directories. Group and Other users can't modify the content of directories they don't own.	To make the contents of these home directories private (non-browseable), use chmod to change the file attributes so that only the owner has rights. For more information, see "Providing a Private Work Directory" in the *OES 2015 SP1: Planning and Implementation Guide*

Volume Type	Creation Method	Access Control	Initial Accessibility	Notes and Caveats
NSS	iManager at user-creation time	NCP trustee assignments in combination with NSS directory and file attributes	- Visible - only the user's home directory - Browseable - only the user's home directory - Modifiable - only the user's home directory	NSS displays its directory and file attributes as POSIX permissions for compatibility with services that require them, such as Samba. However, the underlying access for Samba users is controlled by NSS. For more information, see "Understanding File System Access Control Using Trustees" in the *OES 2015 SP1: File Systems Management Guide*.

Methods for Creating Home Directories

There are several methods for creating home directories on traditional Linux volumes. See Section 8.5.3, "Creating Home Directories on Traditional Linux Volumes," on page 74.

You can create home directories on NSS/NCP volumes automatically when you create Samba users in eDirectory. See Section 8.5.4, "Creating Home Directories Using iManager," on page 76.

8.5.3   Creating Home Directories on Traditional Linux Volumes

On traditional Linux volumes, you should create home directories after the users are enabled for Linux access (LUM) and Samba. This will ensure that the required access rights are automatically assigned. In order to grant a user access to Samba shares on a POSIX file system, the user must be a member of a LUM-enabled group.

Logging In to Create Home Directories

Home directories are automatically created and appropriate file access rights are automatically assigned the first time an eDirectory user who is enabled for Linux access (LUM) logs in to the OES server using PAM-enabled services, such as login, ssh, ftp, or a telnet connection. For more information, see "OES Services That Require LUM-Enabled Access" in the *OES 2015 SP1: Planning and Implementation Guide*.

The simplest approach for many network administrators is to log in to the OES server as the `root` user and use the `su` command at the shell prompt to create a home directory for each user, as follows:

```
su username exit
```

where *username* is the login name of the user for which the home directory is being created.

Alternatively, if your users access the OES server using a PAM-enabled service, you could have them log in to the server to create their own home directories.

Editing the [homes] Share in the smb.conf File

Use the information in Table 8-2 and a text editor, such as gedit or vi, to provide access for your network users to only their individual home directories.

For additional information about the `smb.conf` file, see "The smb.conf Configuration File" on page 95.

Table 8-2 *Customizing the /etc/samba/smb.conf file for Home Directory Access Only*

Section	Entry Name	Description	Recommended Action
[homes]		This sets up a share named homes. The primary purpose of this standard Samba share is to expose only the home directories of your Samba users. The parameters in this section provide private access to home directories, which is the expectation of most network administrators.	1. To learn more about the parameters in this and other sections, search the Web for information about the `smb.conf` file.
	path =	This parameter is not needed if user Home directories are contained in `/home` on the server because the path for this share defaults to `/home/%S`—the Home directory of the logged in user.	1. To provide access to home directories in a non-standard (other than `/home/%S`) location, specify the full path from the root of the file system. 2. Be sure to end the path with `/%S`. Otherwise, all the Home directories will be visible to each Samba user.
[*all other share names*]		These set up various other shares that are not needed for private home directory access. In fact, the [users] share actually makes all the home directories visible to every Samba user.	1. To preserve file contents for future reference while also removing these shares, comment out each line of the rest of the file, by inserting a pound sign (#) at the beginning of each line. Otherwise, delete these lines.

You must restart Samba for the changes you have made in the configuration file to take effect. Complete the following steps:

1 Save the `smb.conf` file.

2 Enter the following command at a terminal prompt:

```
/etc/init.d/smb restart
```

Using Linux User Management Commands to Create Home Directories

You can use either the `namuseradd` or `namusermod` command with the `-m` option to create home directories, as documented in "Using Command Line Utilities to Manage Users and Groups" in the *OES 2015 SP1: Linux User Management Administration Guide*.

8.5.4 Creating Home Directories Using iManager

If you plan to create home directories for eDirectory users on an NSS/NCP volume (the volume must exist and be mounted), and you have the NCP server installed and running (the OES default), you can create user home directories in iManager at the same time you create the user objects. (iManager cannot create home directories on traditional Linux volumes that are not also NCP volumes.)

There is one important caveat: directories created using this method are owned from a POSIX perspective by the eDirectory user who creates the user. It is important to understand the implications of this caveat:

- ◆ For NSS volumes, POSIX ownership has no bearing on Samba access to NSS volumes because NSS controls access based on the Novell trustee model.

- ◆ For NCP volumes on Linux POSIX file systems, POSIX ownership is an issue for Samba access when the NCP volume is defined on a Linux POSIX file system. Because access to Linux POSIX file systems is controlled through POSIX, users cannot access their own home directories until ownership is changed.

  You can reassign directory ownership after the user is enabled for Samba by using the `chown` command.

  For example, to change ownership of the `/home/user1` directory from the Admin user to user1, you would enter

  ```
  chown -R user1: /home/user1
  ```

  The `-R` option applies the operation recursively to all subdirectories and files.

When assigning trustee rights for access to Samba shares on NSS volumes, it is often easier to grant trustee rights to groups rather than to individual users. Keep in mind that a Samba user only needs to be a member of one LUM-enabled group. If you use the Samba Management plug-in for iManager, users are automatically made members of the default Samba users group, which is LUM-enabled. It is not necessary to LUM-enable other groups that are created solely for the purpose of granting trustee rights to the NSS file system.

8.5.5 Creating a Share for Group Access: NSS/NCP Example

You can create shares with unique names, such as volumes that users are familiar with, and provide access to them.

For example, if your Samba users keep their work files on an NSS volume named PROJECTS, you could create a share to the `/media/nss/PROJECTS` directory.

1 In iManager, select **File Protocols** > **Samba** and select your Samba server.

2 Click the **Shares** tab and select **New**.

3 Specify the following information to create the new share:
   - ◆ Share Name: `projects`

◆ Path: `/media/nss/PROJECTS`

◆ Comment: `Project folders`

◆ Read-Only: No

◆ Inherit ACLs: Yes

Click **OK**.

4 Using iManager > **Files and Folders**, create folders for each project and assign trustee rights.

For example, you could create folders named `wheel` and `lever` and assign the following trustee rights:

◆ For `projects:wheel`, assign user1 all rights and user2 Read and File Scan rights.

◆ For `projects:lever`, assign user2 all rights and user1 Read and File Scan rights.

Because Samba access to NSS volumes is controlled by NCP trustee rights, user1 and user2 can now work in their respective project folders, and they can see but not change the contents of the project folder belonging to their coworker. Adjusting POSIX permissions is not required.

NOTE: You can also assign trustee rights from the command line. The `rights` command available at the terminal prompt is for working with NSS volumes only. For information on using the rights utility at the shell prompt, enter `rights`.

The `rights` command in the `ncpcon` utility is for working with any NCP volume, including NCP volumes defined on Linux POSIX file systems. For information about the `ncpcon rights` command, run `ncpcon` and enter `help rights`.

8.5.6   Creating a Share for Group Access: POSIX Example

You can create shares for groups to use.

For example, if you have a group of Samba users who want to collaborate regarding usability ideas, you could create a `usability` folder and grant access to it by using Linux commands.

This example shows how to create a share by editing the `smb.conf` file.

1 Create a folder named `usability` in `/usr`.

2 Create a [usability] share in the `smb.conf` file by inserting the following lines:

```
[usability]
 comment = Usability Ideas
 path = /usr/usability
 browseable = Yes
 read only = No
 inherit acls = Yes
```

3 Save the `smb.conf` file.

4 Restart Samba by entering the following command at the terminal prompt:

`/etc/init.d/smb restart`

5 Create a LUM-enabled group and assign the Samba users to it. For example, create a group called usetest.

6 Change the group owner of the `/usr/usability` folder to usetest and grant the usetest group read, write and execute rights by entering the following at a terminal prompt:

```
chown -R :usetest /usr/usability

chmod -R 775 /usr/usability
```

The users would then be able to collaborate with each other in the /usr/usability folder.

For more information on creating group work directories, see "Providing a Group Work Area" in the *OES 2015 SP1: Planning and Implementation Guide*.

8.5.7 Aligning Samba and Novell Client Access

If you plan to have users access files and directories through both Samba and the Novell Client software, be sure to read "Aligning NCP and POSIX File Access Rights" in the *OES 2015 SP1: Planning and Implementation Guide* and follow the directions there.

8.6 What's Next

After preparing the Samba environment for your network users, you need to inform the users about their access options. Continue with Chapter 9, "Using Novell Samba," on page 79.

9 Using Novell Samba

When Novell Samba is properly configured on your Open Enterprise Server 2015 SP1(OES 2015 SP1) Linux server, the Windows users on your network can access the shares you create by completing one or more of the following tasks.

9.1 Adding a Network Place

From a Windows 2000 or XP workstation, you can add a Network Place (formerly known as a Web folder) that points to a share on the OES server by doing the following:

IMPORTANT: The directory you are linking to must already exist on the OES server and fall within the scope of a defined share. Also, the directory's owner (eDirectory Samba user) must have the same login name and password as a user on the Windows workstation you are using.

Share names and the server directories they point to are defined by using the Samba Management plug-in for iManager or by editing the `/etc/samba/smb.conf` file on the OES server. For more information and setting up shares, see Section 8.5, "Typical Samba Configuration Scenarios," on page 71.

1 Log in to your Windows workstation.

2 From your desktop, access **My Network Places**.

3 Double-click **Add Network Place**.

4 On Windows XP, do the following:

    4a In the Add Network Wizard dialog box, click **Next**.

    4b Select **Choose another network location**, then click **Next**.

    4c In the **Internet or network address** field, type either the IP address of the server or the Samba server name followed by the share name as follows:

    *Samba_host_or_IP**share_name*

    where *Samba_host_or_IP* is the IP address or name of the Samba server (by default this is *hostname*-W) and *share_name* is a share name specified in the `/etc/samba/smb.conf` file (the most common share name is "homes").

    Share names and the server directories they point to are defined in the /etc/samba/ smb.conf file on the OES server. For more information and setting up shares, see Section 8.5.1, "Setting Up a Workgroup and Shares (Access Points)," on page 71.

    4d Click **Next**.

    4e (Optional) modify the name of the Network Place to a more intuitive name, such as **My Home Directory**.

    4f Click **Next**.

4g Click **Finish**.

The folder opens, ready for access.

5 On Windows 2000, do the following:

5a In the Location field, type the Samba server name and share name as follows:

\\Samba_host_name\share_name

where *Samba_host_name* is the name of the Samba server (by default this is *hostname*-W) and *share_name* is a share name specified in the `/etc/samba/smb.conf` file (the most common share name is "homes").

For example, to access the `homes` share on a server with the host name `myserver`, you would type `\\myserver-w\homes` in the **Location** field.

5b Click **Next**.

5c (Optional) modify the name of the Network Place to a more intuitive name, such as **My Home Directory**.

5d Click **Finish**.

The folder opens, ready for access.

Network places are persistent and are automatically made available in Network Neighborhood each time the user logs in.

9.2 Adding a Web Folder

Using the Internet Explorer browser, you can add a Web folder that points to a share on the OES server by doing the following:

IMPORTANT: The directory you are linking to must already exist on the OES server and fall within the scope of a defined share. Also, the directory's owner (eDirectory Samba user) must have the same login name and password as a user on the Windows workstation you are using.

Share names and the server directories they point to are defined by using the Samba Management plug-in for iManager or by editing the `/etc/samba/smb.conf` file on the OES server. For more information and setting up shares, see Section 8.5, "Typical Samba Configuration Scenarios," on page 71.

---

1 Log in to your Windows workstation.

2 Open Internet Explorer.

3 Click **File > Open**.

4 Click **Open as Web Folder**.

5 In the **Open** field, type the Samba server name and share name as follows:

\\DNS_Name_or_IP\share_name

where *DNS_Name_or_IP* is the IP address or DNS name of the Samba server and *share_name* is a share name specified in the /etc/samba/smb.conf file (the most common share name is "homes").

For example, to access the `homes` share on a server with the host name `myserver`, you would type `\\myserver.full.dns.name\homes` in the **Location** field.

6 Click **OK**.

7 To make the folder automatically available, click **Favorites > Add to Favorites > OK**.

9.3 Mapping Drives to Shares

From a Windows 2000 or XP workstation, you can map a network drive letter that points to a share on the OES server by doing the following:

IMPORTANT: The directory you are linking to must already exist on the OES server, and the directory's owner (eDirectory Samba user) must have the same login name and password as the logged in user on the Windows workstation you are using.

---

1 Log in to your Windows workstation.

2 From your desktop, access **My Computer > Tools > Map Network Drive**.

3 From the **Drive** drop-down menu, select an unused drive letter.

4 In the **Folder** field, type the Samba server name and share name as follows:

*Samba_host_name**share_name*

where *Samba_host_name* is the name of the Samba server (by default this is *hostname*-W) and *share_name* is a share name specified in the /etc/samba/smb.conf file (the most common share name is "homes").

For example, to access the `homes` share on a server with the host name `myserver`, you would type `\\myserver-w\homes` in the **Folder** field.

5 Click **Finish**.

The folder opens, ready for access.

10 Troubleshooting Samba

The following sections should help you solve Samba access problems. If you don't find the answers you need, please use the User Comments feature in the online documentation to let us know what is missing.

This section covers the following issues:

10.1 I Can't Enable eDirectory Users for Samba

Check the following:

- When you configure Novell Samba, the **Base Context for Samba Users** must be set at or above the context where the User objects for Samba have been created.

  If you have installed Samba and need to modify the **Base Context for Samba Users** setting on your server, follow the instructions in Section B.2.4, "Changing the LDAP Suffix," on page 99.

- Samba users must be created in a container or partition that has a Samba-qualified password policy assigned to it.

- Samba users must be members of a LUM-enabled group.

10.2 Users Can See Everyone's Home Directories

The Linux (POSIX) file security model is public by default, whereas the traditional Novell model is private. For a comparison of the two models, see "Comparing the Linux and the Novell Trustee File Security Models" in the *OES 2015 SP1: Planning and Implementation Guide*.

You can adjust the default permissions on Linux to more closely match the traditional Novell model by following the instructions in "Aligning NCP and POSIX File Access Rights" in the *OES 2015 SP1: Planning and Implementation Guide*.

10.3 Users Can't Log In to the Samba Server

To access Samba, users must meet the requirements found in "Samba Users Are Both Windows and eDirectory Users" on page 11.

The Samba Proxy User password stored on the OES Server must match the corresponding user's password in eDirectory.

10.4 Users Can't See Their Home Directories

Check for the following:

- Does the directory exist? The Samba implementation in OES doesn't automatically create home directories when users log in to Samba.
- Does the directory exist in the share path? By default, the [homes] share points to individual home directories in /home at the root of the file system. If the home directories were created in another location (for example, through iManager on an NCP volume that doesn't point to /home), you need to either include a path statement in the [homes] share definition that points to the correct location, or create another share that users can access.
- Do users have the necessary access rights to their home directories? The granting of appropriate access rights does not happen automatically in all Samba configurations. Depending on the type of volume the home directories are created on and whether or not you define home directories when the users are created, you might need to adjust access rights manually.

For more information, see Section 8.5.2, "Creating Private Home Directories for Samba Users," on page 72.

10.5 Users Get Errors When Trying to Access Their Directories

The most common cause for this problem involves home directories that were created in iManager on NCP volumes that point to Linux POSIX file systems.

Home directories created in iManager are owned (from a POSIX standpoint) by the Admin user who creates the user object. If a Samba share points to a Linux POSIX file system, then the Samba user must have POSIX access rights to access directory contents. For more information, see "Creating Private Home Directories for Samba Users" on page 72.

10.6 I Get Errors When Creating a Samba Share in iManager

When using the Samba Management plug-in for iManager to create a new Samba share, make sure the path you type in the **Path** field already exists on the OES server.

If the path doesn't exist, the following error is displayed: Samba Error. Could not create the Samba share.

10.7 I Get Errors When Adding Samba Users in iManager

When using the Samba Management plug-in for iManager to add Samba users to a Samba server, the users must already be assigned a Samba-qualified password policy.

If you try to add a user that does not have a Samba-qualified password policy, the following error is displayed: `Could not Samba enable the user for group xxx. Received an error when checking for a universal password. Error: Cannot continue because the user does not appear to have a universal password.`

10.8 Concurrent Samba Client Logins Are Limited

On Samba servers with 100 or more users, the number of concurrent smbclient logins seems to be limited and connection timeouts are occurring. The following error is displayed: `Session setup failed: Call timed out: server did not respond after 20000 milliseconds.`

To resolve this issue, edit the `sldap.conf` file on the OES server to index the ldapsearch with the "value" rule to ensure faster searches. The line to look for is:

```
index       sambaSID      eq
```

For more information, refer to the OpenLDAP documentation available on the Web.

IMPORTANT: OpenLDAP instructions do not apply to eDirectory LDAP. For more information, see the eDirectory documentation on the Web (http://www.novell.com/documentation/edir88/edir88/data/a5tuuu5.html).

10.9 "Could Not Samba Enable the User" Errors in iManager

If you see `username: Could not Samba enable the user for group SERVERNAME-W-SambaUserGroup` errors when using the Samba management plug-in for iManager to add users, check the following:

Samba user objects.

- ◆ Make sure that iManager plug-in is installed on a server running a currently supported operating system
- ◆ Add a local replica of the partition containing the Samba user objects to the server that is running the Novell Samba software.
- ◆ If you have servers running unsupported versions of NetWare in your tree, make sure those servers do not hold a replica of the partition containing the Samba user objects.

11 Security Considerations for Samba

This section outlines security issues when using the Novell Samba configuration on an Open Enterprise Server 2015 SP1(OES 2015 SP1) server.

11.1 Security Implications

If you plan to implement Samba on your network, be aware of the following security implications:

- Section 11.1.1, "Universal Password," on page 87
- Section 11.1.2, "Samba Access vs. Novell Client Access," on page 87

11.1.1 Universal Password

By default, Samba uses Novell Universal Password (UP) for authentication. Changing the default UP setting is not recommended.

Before using Samba, you might want to investigate the implications for using Universal Password as documented in "Universal Password" in the *NetIQ Modular Authentication Services Administration Guide*.

Alternatively, you might choose to provide Windows users with file services using Novell Client software, Novell iFolder, or NetStorage. For more information, see "File Services" in the *OES 2015 SP1: Planning and Implementation Guide*.

For more information on Samba password options, see Section 11.2, "Samba Passwords," on page 87.

11.1.2 Samba Access vs. Novell Client Access

Samba uses the POSIX/Linux security model. Novell Client software and other NCP access methods use the NetWare security model.

Providing similar access priviledges for both Samba users and Novell Client (NCP) users, requires additional steps as explained in "Aligning NCP and POSIX File Access Rights" in the *OES 2015 SP1: Planning and Implementation Guide*.

11.2 Samba Passwords

Before creating or enabling eDirectory users for Samba access, it is important to understand certain requirements regarding Samba passwords.

The preferred method for Samba authentication in OES involves the use of a Universal Password (UP) policy in eDirectory. The primary reason for this is that it eliminates the need for password synchronization when users change their passwords in eDirectory.

The first time you install Samba on an OES server in a given eDirectory tree, the install creates a Universal Password (UP) policy in the tree named **Samba Default Password Policy**. The policy is located in eDirectory > **Security** > **Password Policies**.

The following sections explain the issues associated with Universal Password and Samba.

11.2.1 Setting a Universal Password for an Existing User

You can set a Universal Password for an existing eDirectory user by using iManager > **Passwords** > **Set Universal Password**. However, if you do this, you have changed the user's password and you must notify the user of the change.

Some organizations have set up portals for users to change their passwords. After a password policy is set, send the users to the portal to reset the password so both the NDS and Universal Password are set.

11.2.2 Be Sure to Use Samba-Qualified Universal Password Policies

For a Password Policy to qualify for use by Samba users, the following configuration options must be enabled on the iManager > **Passwords** > **Password Policies** > the **Universal Password** tabbed page:

- Enable Universal Password
- Allow Admin to Retrieve Password

11.2.3 Creating a New Samba-Qualified Password Policy

1 Log in to iManager, then click **Passwords** > **Password Policies** > **New**.

2 Name the policy, then click **Next**.

3 At the **Would you like to enable Universal Password?** prompt, click **Yes**.

4 Click **View Options**.

5 Select the **Allow Admin to Retrieve Password** option.

6 Continue creating the policy and in Step 7 of 8 assign it as follows:

If you are using the smbbulkadd utility to enable Samba users you must assign it to either

- Each User object being enabled

  or

- The Organizational Unit of your User objects

If you are using iManager to enable Samba Users, assign the policy to either

- Each User object being enabled
- The Organization Unit of your User objects

  or

- The Organization object at the root of the tree above the User objects.

7 Click **Next**.

8 Click **Finish**.

9 Click **Close**.

11.2.4　Modifying an Existing Password Policy for Samba

1 Log in to iManager, then click **Passwords** > **Password Policies**

2 Select a policy, then click **Edit**.

3 Make whatever changes you need.

4 In the drop-down list, click **Configuration Options**, or in Internet Explorer click the **Universal Password** tab, then click the **Configuration Options** link.

5 Make sure the **Enable Universal Password** and the **Allow Admin to Retrieve Password** options are both selected.

6 In the drop-down list, click **Policy Assignment**, or in Internet Explorer click the **Policy Assignment** tab.

7 If you are using the smbbulkadd utility to enable Samba users you must assign it to either

- Each User object being enabled

  or

- The Organizational Unit of your User objects

If you are using iManager to enable Samba Users, assign the policy to either

- Each User object being enabled

- The Organization Unit of your User objects

  or

- The Organization object at the root of the tree above the User objects.

8 Click **Apply**.

9 Click **OK**.

A Samba Caveats

This section explains the following known caveats for the Novell Samba implementation in Open Enterprise Server 2015 SP1(OES 2015 SP1).

- Section A.1, "Setting the Base Context for Samba Users," on page 91
- Section A.2, "LDAP Search Delays and Samba," on page 91
- Section A.3, "The Samba Proxy User," on page 92
- Section A.4, "Windows XP SP2 Wrongly Reports File Deletion," on page 92
- Section A.5, "Home Directory Creation Is Not Automatic," on page 92
- Section A.6, "Enabling Users for Samba Disables Access to NetStorage SSH Storage Locations," on page 92
- Section A.7, "NetBios Name for Samba Is Limited to 15 Characters in Length," on page 93
- Section A.8, "Use cifs Option When Mounting Samba Shares," on page 93

A.1 Setting the Base Context for Samba Users

When you install Samba services on OES, the default value of the **Base Context for Samba Users** field is the eDirectory context where the admin user is created.

If your User objects for Samba reside in the same context as admin or in a sub-context of that container, you do not need to change the default setting.

If your User objects for Samba are not located in the same context as admin or in a subcontext, you must change the **Base Context for Samba Users** setting at install time to a context that includes (either directly or as a sub-context) the Samba users.

If you need to change the base context after you have already installed and configured Novell Samba, see Section 3.2.2, "Installing Novell Samba After Initial Server Installation," on page 16.

A.2 LDAP Search Delays and Samba

When the number of objects in a tree is very large (greater than 100,000), users can experience substantial LDAP authentication delays when accessing Samba on an OES server.

To reduce the search time, you have the following options:

- Set the object cache high enough that all the objects being searched are cached in memory. For more information, see the *NetIQ eDirectory 8.8 SP8 Tuning Guide*.
- Index the objectClass attribute (the attribute that is compared during the LDAP search). For more information, see "Index Manager" in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.
- Add an eDirectory replica to the server where the search is taking place. For more information, see "Adding a Replica" in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

A.3 The Samba Proxy User

When you install Novell Samba, you are asked to specify a Samba proxy user for LDAP authentication through eDirectory.

By default, the Samba proxy user is created in the container specified as the Base Context for Samba Users and is named *servername*-sambaProxyUser. You specify the password for this user when you configure Novell Samba.

You can specify another eDirectory user as the Samba proxy user. If you do, be aware of the following:

- If you specify a user that doesn't already exist in eDirectory, the user account is created and granted the necessary rights. You must also specify a password for the new user.
- If you specify an existing eDirectory user, it is assumed that you have already created the user account with the necessary rights and no modifications are made to the existing user.

    If you specify an existing eDirectory user but enter a new password, you are prompted to change the password for that user.

A.4 Windows XP SP2 Wrongly Reports File Deletion

Windows XP SP2 wrongly reports file deletions to Samba users under specific conditions as follows:

1. The files are on an NSS volume.
2. Users don't have the Erase right to the files.
3. Users try to delete the files.
4. The system reports that the files were deleted.
5. Refreshing the window shows that the files still exist.

Windows XP SP1 and earlier correctly reports that the files cannot be deleted.

A.5 Home Directory Creation Is Not Automatic

Unlike many Samba implementations, the Novell Samba configuration in OES does not support automatic creation of home directories when users log in to the Samba server. For more information, see Section 8.5.2, "Creating Private Home Directories for Samba Users," on page 72.

A.6 Enabling Users for Samba Disables Access to NetStorage SSH Storage Locations

Because the default Samba users group does not include SSH as an allowed service, using the Samba Management plug-in for iManager to add a user to an OES Samba server disables that user's access to NetStorage Storage Locations based on SSH.

For information on how to resolve this issue, see "Providing SSH Access for Samba Users" in the *OES 2015 SP1: Planning and Implementation Guide*.

A.7 NetBios Name for Samba Is Limited to 15 Characters in Length

When you install Novell Samba, the NetBios name for the Samba server defaults to the DNS hostname with "-W" appended to it. For example, if you specify the hostname of server1 during the OES installation, the NetBios name assigned to the Samba server is server1-W.

Because the length of the NetBios name for Samba is limited to 15 characters, you must ensure that the DNS hostname you specify is no longer than 13 characters. This allows the "-W" to be appended and still be within the 15 character limit for the NetBios name.

If your DNS hostname is longer than 13 characters, the NetBios name is truncated and iManager will not be able to find the Samba server and other Samba-related objects.

You can change the NetBios name by editing the `smb.conf` file. However, if you do this, you must delete the Samba-related eDirectory objects and rerun the Novell Samba configuration.

A.8 Use cifs Option When Mounting Samba Shares

When mounting a Samba share on an OES server, use

```
mount -t cifs
```

Do not use the `smbmount` command or `mount -t smbfs`. The `smbfs` open source code is no longer being maintained by the community and has been replaced by the `cifs` open source code.

B   Samba Configuration Files

This section covers the following topics:

B.1   Component Information

The Samba distribution included with Open Enterprise Server 2015 SP1(OES 2015 SP1) consists of the RPMs and configuration files outlined in this section.

B.1.1   Samba RPM

OES includes a customized configuration package for the Samba software that is installed on every SLES 11 server. This package is named `novell-samba-3.4.`*`xxx`*.

In compliance with Samba standards, Novell has added the switches `-with-ldapsam` and `-with-ssl` to provide secure LDAP authentication support for Samba users.

B.1.2   The smb.conf Configuration File

In compliance with Linux Standards Base (LSB) requirements, the Samba configuration file (`smb.conf`) is placed in the `/etc/samba` directory on the OES server.

The Novell implementation of Samba modifies the `smb.conf` file that ships with SLES 11 as explained in Table B-1.

Table B-1   Modified/Added Entries in the smb.conf File

Section	Entry Name	Description	Change or Default Setting Information
[global]	workgroup =	Specifies the Windows workgroup that the Samba server either joins (if it exists) or creates (if the name is new).	This is modified from TUX-NET to WORKGROUP.

Section	Entry Name	Description	Change or Default Setting Information
	netbios name =	Sets the NetBIOS name that a Samba server is known and advertised as. If Samba is installed for the first time by OES, Novell appends -W to the hostname for this entry. This is necessary to prevent a conflict with NCP on Linux, which uses the hostname. Extra steps must be taken if you need to change this setting. For more information, see Section A.7, "NetBios Name for Samba Is Limited to 15 Characters in Length," on page 93.	This entry is added. Default: netbios name = %h-W %h is the server's DNS host name.
	passdb backend =	Specifies that Samba account information is stored in eDirectory LDAP database.	This entry is added. Do not modify this line.
	ldap admin dn =	Specifies the Distinguished Name (DN) of the proxy user that Samba uses for contacting the eDirectory LDAP server to retrieve user account information for users requesting access to Samba shares. For more information, see Section A.3, "The Samba Proxy User," on page 92.	This entry is added. Example: ldap admin dn = cn=admin,o=novell
	ldap suffix =	Specifies the context that is used to search for the Samba user objects in eDirectory. A search from this context down through the tree must find the Samba users. You cannot correct problems with this context by simply modifying this field with a text editor. Instead you must follow the instructions in Section A.1, "Setting the Base Context for Samba Users," on page 91.	This entry is added. The default setting is specified during install time as the Base context for Samba users.
	ldap passwd sync =	Specifies that password encoding support is on or off.	This entry is added. Default: ldap password sync = on
	security =	Specifies the security mode. The value must be set to user. For more information, see samba.org (http://www.samba.org) on the Web.	This entry is added. Default (required): security = user
	encrypt passwords =	Specifies that passwords received from Windows clients are encrypted. The value must be set to yes. For more information, see samba.org (http://www.samba.org) on the Web.	This entry is added. Default (required): encrypt passwords = yes

Section	Entry Name	Description	Change or Default Setting Information
	server string =	Specifies the string that is displayed for the Samba server in Windows Explorer, My Network Places, and for mapped drives.	This entry is not added, but is supported on OES Samba servers.
		The default (even when no value is specified) is "Samba %v" where %v is the Samba version.	Default: no value specified
		When you set the value to a null string (server string = ""), no extra information is displayed for the Samba server.	

A full explanation of the `smb.conf` file is beyond the scope of this guide. Table B-2 briefly explains the purpose of other sections found in the file. For detailed explanations, search for `smb.conf` on the Web.

Table B-2   *Brief Summary of the Other Entries in the smb.conf File*

Section	Description
[profiles]	This section sets up a network profiles service for playing media files through Samba.
[users]	This section sets up a share that displays all the home directories in `/home`.
[groups]	This section sets up a share that displays any directories contained in `/home/groups`.
[printers] [print$]	These sections set up a share for Samba printing, which is not supported on OES. Because iPrint is the OES printing solution, the OES installation comments out these sections in the `smb.conf` file.

B.1.3 The ldap.conf Configuration File

Samba on Linux uses the OpenLDAP client libraries `libldap.so` and `libldap_r.so`. `ldap.conf` is the configuration file for OpenLDAP.

In compliance with Linux Standards Base (LSB) requirements, we have placed the `ldap.conf` file in the `/etc/openldap` directory on the OES server.

If you install the OES server into an existing tree, you must specify a trusted root certificate during OES installation if you want to use SSL. The `ldap.conf` file on your OES server then has the following certificate-related entries:

- TLS_CACERT /etc/ssl/*certname*.cert
- TLS_REQCERT demand

If you are installing a new directory tree, the `ldap.conf` file has the following entry:

- TLS_REQCERT allow

For more information on the `ldap.conf` file, see the ldap.conf man page.

B.2 Changing the Samba Server Configuration

This section describes how to change the configuration settings that are displayed on the **General** page in the Samba management plug-in for iManager (see).

B.2.1 Changing the Workgroup Name

The workgroup name specifies the Windows workgroup that the Samba server either joins (if it exists) or creates (if the name is new). In OES, the default workgroup name is modified from TUX-NET (the default for SLES 11) to WORKGROUP.

When users browse the network from Windows workstations, they can typically see only the Windows workstations and servers in the same workgroup. Because WORKGROUP is the default workgroup name for all Windows 2000 and Windows XP workstations, the WORKGROUP workgroup can contain hundreds of workstations and servers, rendering it nearly unusable.

To change the workgroup name for your Samba server, use a text editor such as gedit or vi to open the `/etc/samba/smb.conf` file and locate the workgroup name setting in the [global] section:

```
[global]
```

```
workgroup=workgroup
```

Replace the value with a name for the workgroup that you want users to see when they browse in Network Neighborhood. For example, you could change the entry to read:

```
[global]
```

```
workgroup=wg001
```

After saving the `smb.conf` file, you must restart the Samba server for the change to take effect.

B.2.2 Understanding the Domain SID

A SID is a security identifier that is used by Windows networking operations to identify an object. A unique SID is generated every time a Samba server with a new combination of machine name (hostname) and domain name (workgroup) is started. The format of a SID is as follows:

S-1-5-21-7623811015-3361044348-030300820

S means the string is a SID. 1 is the revision level. 5 is the identifier authority value. The remainder of the string is the domain or local computer identifier.

It should not be necessary to change the SID for an OES Samba server.

B.2.3 Changing the NetBios Name

The NetBios name is the name that a Samba server is known and advertised as. When Samba is installed on an OES server, Novell appends "-W" to the DNS hostname for this entry. This is necessary to prevent a conflict with the name of an NCP server on Linux, which uses the hostname. In addition, although NetBIOS uses a completely independent naming convention from DNS, using a NetBios name that corresponds to the DNS hostname makes administration easier.

You should not need to change the default NetBios name for your Samba server. However, if you entered a DNS hostname that is longer than 13 characters when you installed OES, the NetBios name is truncated and iManager won't be able to find the associated server and group objects.

The NetBios name can be changed by editing the "netbios name =" entry in the [global] section of the `/etc/samba/smb.conf` file. After editing and saving the `smb.conf` file, you must restart the Samba server for the change to take effect.

You must also delete the Samba-related eDirectory objects and regenerate them by rerunning the Novell Samba configuration in YaST.

B.2.4 Changing the LDAP Suffix

The LDAP suffix specifies the eDirectory context where the following Samba-related objects are created:

- Samba domain object (*hostname*-W)
- Default Samba group (*hostname*-W-SambaUserGroup)
- Samba proxy user (*servername*-sambaProxy)
- UNIX Configuration object

> **NOTE:** The UNIX Workstation object that represents the Samba server is created as part of the LUM configuration and therefore can be located elsewhere in the tree.

The LDAP suffix is also the base context that Samba uses to search for User objects in eDirectory. A search from this context down through the tree must be able to find the Samba users. If the Base Context is set incorrectly, you see the "sambaDomain Object Error" message, because an eDirectory search cannot find the Samba user objects.

The default setting is specified during the OES installation as the **Base Context for Samba Users**. To change this setting, you must rerun the OES configuration in YaST. Doing so creates new Samba-related objects in the new context. To avoid confusion, you should delete the old Samba objects. Be sure to make all of your existing Samba users members of the new default Samba users group before you delete the old one. If you want to keep the same proxy user, make sure the proxy user has correct rights to the new base context.