www.novell.com/documentation

Planning and Implementation Guide

Open Enterprise Server 2 SP3

June 5, 2013

Novell®

Legal Notices

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

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

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

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

Purpose

This guide provides:

- Planning and implementation instructions
- Service overviews
- Links to detailed information in other service-specific guides.

Audience

This guide is designed to help network administrators

- Understand Open Enterprise Server 2 services prior to installing them.
- Make pre-installation planning decisions.
- Understand installation options for each platform.
- Implement the services after they are installed.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with OES 2. 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

Changes to this guide are summarized in a Documentation Updates appendix at the end of this guide. The lack of such an appendix indicates that no changes have been made since the initial product release.

Additional Documentation

The *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare* is the hands-on counterpart to this guide and helps network administrators:

- Set up a basic lab with an OES 2 server, a virtualized NetWare server, a test tree, and user objects that represent the different types of users in OES 2.
- Use the exercises in the guide to explore how OES 2 services work.
- Continue exploring to gain a sound understanding of how OES 2 can benefit their organization.

Additional documentation is also found on the OES 2 Documentation Web site (http://www.novell.com/documentation/oes2).

Documentation Conventions

The terms OES 2, and OES 2 SP1, SP2, and SP3 are all used in this guide. A support pack is mentioned to differentiate something that is new or changed in that support pack release of OES 2. All statements that refer to OES 2 also apply to OES 2 SP3 (the latest support pack) unless otherwise indicated.

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

When a single pathname can be written with a backslash for some platforms, or a forward slash for other platforms, the pathname is presented with a forward slash to reflect the Linux* convention. Users of platforms that require a backslash, such as NetWare, should use backslashes as required by the software.

1 What’s New or Changed

This section summarizes the new features for each release of Novell Open Enterprise Server (OES) 2.

- Section 1.1, “New or Changed with the April 2013 Patch Release,” on page 15
- Section 1.2, “New or Changed with the January 2013 Patch Release,” on page 15
- Section 1.3, “New or Changed with the September 2011 Patch Release,” on page 17
- Section 1.4, “New or Changed in OES 2 SP3,” on page 17
- Section 1.5, “New or Changed in OES 2 SP2,” on page 18
- Section 1.6, “New in OES 2 SP1,” on page 20
- Section 1.7, “New in OES 2 (Initial Release),” on page 22
- Section 1.8, “Links to What's New Sections,” on page 23
- Section 1.9, “Where’s NetWare?,” on page 24

1.1 New or Changed with the April 2013 Patch Release

- Section 1.1.1, “Upgrade to eDirectory 8.8.7,” on page 15

1.1.1 Upgrade to eDirectory 8.8.7

An upgrade to Novell eDirectory 8.8 SP7 is available in the April 2013 Scheduled Maintenance for OES 2 SP3. For information about the eDirectory upgrade, see TID 7011599 (http://www.novell.com/support/kb/doc.php?id=7011599) in the Novell Knowledgebase.

There will be no further eDirectory 8.8 SP6 patches for the OES platform. Previous patches for Novell eDirectory 8.8 SP6 are available on Novell Patch Finder (http://download.novell.com/patch/finder/#familyId=112&productId=29503).

1.2 New or Changed with the January 2013 Patch Release

- Section 1.2.1, “Upgrade to Novell iManager 2.7.6,” on page 16
- Section 1.2.2, “Novell Client Support for Windows 8 and Server 2012,” on page 16
- Section 1.2.3, “New Novell Cluster Services Plug-in for iManager 2.7.5 and Later,” on page 16
- Section 1.2.4, “OES Client Services Support for Windows 8 and IE 10,” on page 16
- Section 1.2.5, “OES Client Services Do Not Support Windows Server 2012,” on page 17
- Section 1.2.6, “OES Client Services Support for Mac OS X 10.8 and Safari 6.0,” on page 17

1.2.1 Upgrade to Novell iManager 2.7.6

The January 2013 Scheduled Maintenance for OES 2 SP3 includes a channel upgrade from Novell iManager 2.7.5 to Novell iManager 2.7.6.

Novell iManager 2.7.6 provides the following enhancements:

- Microsoft Internet Explorer 10 certification in the desktop user interface view on Windows 8 (excluding Windows 8 RT) and Windows Server 2012.
- Apple Safari 6.0 certification on Mac OSX Mountain Lion (version 10.8).
- iManager Workstation certification on Windows 8 Enterprise Edition (32-bit and 64-bit).
- Manager 2.7.6 support for Tomcat 7.0.32. and Java 1.7.0_04 versions.

iManager documentation links in this guide have been updated to reflect this change.

iManager 2.7.6 documentation is available on the Web (https://www.netiq.com/documentation/imanager/). For earlier iManager versions, see "Previous Releases" (https://www.netiq.com/documentation/imanager27/#prev).

1.2.2 Novell Client Support for Windows 8 and Server 2012

The January 2013 Scheduled Maintenance for OES 2 SP3 announces the availability of Novell Client 2 SP3 for Windows with support for:

- Windows 8 (32-bit and 64-bit) excluding Windows 8 RT
- Windows Server 2012 (64-bit)

Novell Client 2 documentation links in this guide have been updated to reflect the release of SP3.

Novell Client 2 SP3 for Windows documentation is available on the Web (http://www.novell.com/documentation/windows_client/). Documentation for earlier versions is available under Previous Releases (http://www.novell.com/documentation/windows_client/#previous).

1.2.3 New Novell Cluster Services Plug-in for iManager 2.7.5 and Later

The Clusters plug-in for Novell iManager 2.7.5 or later supports the management of OES and NetWare clusters and resources. The availability of different cluster management features depends on the version of Novell Cluster Services and the server platform that are installed on the cluster being managed. A comparison of the old and new interface is available in "What's New (January 2013 Patches)" (http://www.novell.com/documentation/oes2/clus_admin_lx/data/ncs_new_jan2013.html) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux* (http://www.novell.com/documentation/oes2/clus_admin_lx/data/h4hgu4hs.html).

1.2.4 OES Client Services Support for Windows 8 and IE 10

In the January 2013 Scheduled Maintenance for OES 2 SP3, OES client services added support for user access from Windows 8 clients (excluding Windows 8 RT), with the exception of Domain Services for Windows (DSfW). DSfW was not tested with Windows 8 clients and does not support them.

Client applications are supported to run on Windows 8 clients in the desktop user interface view.

Web-based client access is supported for the Internet Explorer 10 Web browser in the desktop user interface view for Windows 7 clients and Windows 8 clients.

1.2.5 OES Client Services Do Not Support Windows Server 2012

In the January 2013 Scheduled Maintenance for OES 2 SP3, OES client services were not tested with Windows Server 2012 servers. Client access support for Windows Server 2012 is not planned for OES 2 SP3.

1.2.6 OES Client Services Support for Mac OS X 10.8 and Safari 6.0

In the January 2013 Scheduled Maintenance for OES 2 SP3, OES client services added support for user access from Mac OS X Mountain Lion (version 10.8) clients, with the exception of Domain Services for Windows (DSfW) and Novell iFolder:

- DSfW was not tested with Mac OS X 10.8 clients and does not support them. DSfW support for Mac OS X 10.8 clients is planned for a future release.
- The iFolder client does not run on Mac OS X 10.8 clients and does not support them.

Web-based client access is supported for the Apple Safari 6.0 Web browser on Mac OS X 10.8 clients. Safari 6.0 is not supported by DSfW and iFolder.

1.3 New or Changed with the September 2011 Patch Release

With the release of the September 2011 patches for OES 2 SP3, the base platform has been upgraded to SLES 10 SP4.

SLES 10 SP4 support is enabled by updating OES 2 SP3 servers with the *move-to-sles10-sp4* patch. Novell encourages customers to update to this latest set of patches. For more information, see "Updating (Patching) an OES 2 SP3 Server" in the *OES 2 SP3: Installation Guide*.

SLES 10 SP4 is considered a lower-risk update that contains a set of consolidated bug fixes and support for newer hardware. It does not impact the kernel ABI or third-party certifications.

With the release of the September 2011 patches, OES 2 SP2 customers who upgrade to OES 2 SP3 via the *move-to* patch will receive the SLES 10 SP4 updates. New installations of OES 2 SP3, migrations to OES 2 SP3, and down-server upgrades to OES 2 SP3, should all be performed using SLES 10 SP4 media.

1.4 New or Changed in OES 2 SP3

To see what is new or changed in a component or service, click the respective link below. Services without new features or changes are not listed.

- Common Proxy
- DHCP
- Distributed File Services
- DNS
- Domain Services for Windows
- Dynamic Storage Technology
- eDirectory 8.8.6
- File System Management
- FTP (Pure-FTPd)

- Identity Manager 3.6 (http://www.novell.com/documentation/idm36/idm_install/data/be1l5dw.html)
- iManager 2.7
- Installation
- iPrint
- Linux User Management
- Log File Location - all OES-related log files are now in `/var/opt/novell/log/oes`.
- Migration Tool
- NCP Server
- NetStorage
- Novell AFP
- Novell CIFS
- Novell Cluster Services (High Availability)
- Novell iFolder 3.8 - Clients
- Novell iFolder 3.8 - Servers
- NSS Auditing Client (VLOG)
- QuickFinder
- SLP (OpenSLP)
- Storage Management Services (SMS)

1.5 New or Changed in OES 2 SP2

This section summarizes the new features introduced in Novell Open Enterprise Server (OES) 2 SP2 that either involve multiple services or are not covered in service-specific documentation. For information on service-specific new features, see Section 1.8, “Links to What's New Sections,” on page 23.

- Section 1.5.1, “Auditing,” on page 18
- Section 1.5.2, “Base Platform Is SLES 10 SP3,” on page 19
- Section 1.5.3, “CIFS DFS Support,” on page 19
- Section 1.5.4, “Create EVMS Proposal Option,” on page 19
- Section 1.5.5, “Cross-Protocol File Locking Change,” on page 19
- Section 1.5.6, “Domain Services for Windows Installation,” on page 19
- Section 1.5.7, “Java Console for DNS/DHCP,” on page 19
- Section 1.5.8, “Performance Increases,” on page 20
- Section 1.5.9, “Pure-FTPd,” on page 20
- Section 1.5.10, “Upgrading Online,” on page 20
- Section 1.5.11, “Windows 7 Client Support,” on page 20

1.5.1 Auditing

OES 2 SP2 includes support for third-party developers to create auditing products. For more information, see Section 22.1.2, “NSS Auditing Engine,” on page 225.

1.5.2 Base Platform Is SLES 10 SP3

- With the release of OES 2 SP2, the Linux platform on which OES services run is changed from SUSE Linux Enterprise Server (SLES) 10 SP2 to SLES 10 SP3 and includes Tomcat 5.5.

1.5.3 CIFS DFS Support

This has been added in OES 2 SP2.

1.5.4 Create EVMS Proposal Option

The Partitioner in the YaST Install offers an option to "Create an EVMS Proposal."

For unpartitioned devices over 20 GB in size, this option creates a boot partition and a container for the `swap` and / (root) volumes in up to the first 20 GB, and leaves the remainder of the space on the device as unpartitioned free space. The default / partition size is 10 GB. The swap size is 1 GB or larger, depending on the amount of RAM the server has.

IMPORTANT: This option applies only if you are installing an NSS volume on the same disk as your Linux root (/) partition.

1.5.5 Cross-Protocol File Locking Change

Starting with OES 2 SP2, cross-protocol file locking (CPL) is enabled by default as follows:

- All new servers with NCP installed have CPL turned on.
- If an upgraded server was not configured for CPL prior to the upgrade, CPL will be turned on.
- If an upgraded server was configured for CPL prior to the upgrade, the CPL setting immediately preceding the upgrade is retained.

If a server is only accessed through NCP (AFP and CIFS are not installed), you can achieve an NCP performance gain of about 10%. However, there is a critical caveat. If you later install AFP or CIFS and you forget to re-enable CPL, data corruption can occur.

There are also obvious implications for clustering because the CPL settings for clustered nodes must match. For example, if an unmodified OES 2 SP1 node is clustered with an unmodified OES 2 SP2 node, their CPL settings will conflict and one of the nodes must be modified.

For more information about cross-protocol locking, see "Configuring Cross-Protocol File Locks for NCP Server" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.

1.5.6 Domain Services for Windows Installation

The DSfW installation has been rearchitected with a focus on usability and simplicity.

1.5.7 Java Console for DNS/DHCP

The Java Console for DNS/DHCP management is now available for Linux.

1.5.8 Performance Increases

AFP, NCP, and Samba all have improved performance in OES 2 SP2.

1.5.9 Pure-FTPd

Gateway parity with NetWare.

1.5.10 Upgrading Online

Support for upgrading through the SP Channel is included. For more information, see "Using the Patch Channel to Upgrade (Online)" in the *OES 2 SP3: Installation Guide*.

1.5.11 Windows 7 Client Support

OES 2 SP2 service clients are supported on Windows 7.

1.6 New in OES 2 SP1

- Section 1.6.1, "YaST Install Changes," on page 20
- Section 1.6.2, "Novell AFP," on page 20
- Section 1.6.3, "Novell CIFS," on page 21
- Section 1.6.4, "Novell Domain Services for Windows," on page 21
- Section 1.6.5, "Migration Tool," on page 22

1.6.1 YaST Install Changes

The default behavior of the option to use eDirectory certificates for HTTPS services changed in OES 2 SP1.

In OES 2, eDirectory certificates were only used by default if you were installing a new server.

In OES 2 SP1, eDirectory certificates are used by default in all installation and upgrade scenarios, except when you are upgrading to SP1 from OES 2. For an upgrade, the option that you selected for the initial installation is retained.

For a brief summary of what happens in each scenario, see Table 23-2 on page 244.

1.6.2 Novell AFP

Novell AFP is now available on the Linux platform to provide feature parity with NetWare®.

- Support for AFP v3.1 and AFP v3.2, providing network file services for Mac OS X and classic Mac OS workstations
- Support for Universal Password greater than 8 characters
- Integration with Novell eDirectory
- Integration with the Novell Storage Services (NSS) file system
- Support for Unicode filenames

- Integration with the Novell Trustee Model for file access
- Support for regular eDirectory users (no LUM required)
- Cross-protocol file locking with NCP

Novell AFP also offers the following features not available for NetWare:

- **DHX authentication mechanism:** Provides a secure way to transport passwords of up to 64 characters to the server.
- **Management:** You can use iManager to administer and configure the AFP server on OES 2. iManager support for AFP on NetWare is unchanged and includes only starting and stopping the server.
- **Auditing:** You can audit the AFP server to check on the authentication process and any changes that occur to the configuration parameters of the server.

For more information, see the *OES 2 SP3: Novell AFP For Linux Administration Guide*.

1.6.3 Novell CIFS

Novell CIFS is now available on Linux to provide feature parity with the existing NetWare release. It offers the following features:

- Support for Windows 2000, XP, 2003, and Windows Vista 32-bit
- Support for Universal Password greater than 8 characters
- Support for NTLMv1 authentication mode
- Integration with Novell eDirectory
- Integration with the Novell Storage Services (NSS) file system
- Support for Unicode filenames
- Integration with the Novell Trustee Model for file access
- Support for regular eDirectory users (no LUM required)
- Cross-protocol file locking is planned for a future release

For more information, see the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

1.6.4 Novell Domain Services for Windows

This service creates seamless cross-authentication capabilities between Microsoft Active Directory on Windows servers and Novell eDirectory on OES 2 SP2 servers, and offers the following functionality:

- Administrators with Windows networking environments can set up one or more “virtual” Active Directory domains in an eDirectory tree.
- Administrators can manage users and groups through MMC or iManager.
- eDirectory users can authenticate to the virtual domain from a Windows workstation without the Novell Client™ for Windows being installed.
- eDirectory users can also access file services on
    - Novell Storage Services (NSS) volumes on Linux servers by using Samba shares.
    - NTFS files on Windows servers that use CIFS shares.
    - Shares in trusted Active Directory forests.

For more information, see the *OES 2 SP3: Domain Services for Windows Administration Guide*.

1.6.5 Migration Tool

The new OES 2 SP2 Migration Tool uses a plug-in architecture and comprises multiple Linux command line utilities and a GUI wrapper.

The Migration Tool supports:

- A single, enhanced GUI interface for migrating all OES services
- Service migrations from either a single source server or multiple source servers (consolidation) to a target server.
- Transfer ID (server ID swap) migrations—transferring the services and identity from one server to another server.

For more information, see the *OES 2 SP3: Migration Tool Administration Guide*.

1.7 New in OES 2 (Initial Release)

Novell Open Enterprise Server 2 included the following major features and enhancements that were not included in OES 1. All features are retained in SP1 unless otherwise noted in Section 1.6, "New in OES 2 SP1," on page 20.

- Section 1.7.1, "Dynamic Storage Technology," on page 22
- Section 1.7.2, "OES 2 Migration Tools," on page 22
- Section 1.7.3, "Xen Virtualization Technology," on page 22

1.7.1 Dynamic Storage Technology

OES 2 introduces Novell Dynamic Storage Technology, a unique storage solution that lets you combine a primary file tree and a shadow file tree so that they appear to NCP and Samba/CIFS users as one file tree. The primary and shadow trees can be located on NSS volumes on the same server or on different servers.

This lets you manage storage costs in new and efficient ways that were not previously possible.

For more information, see the related sections in Chapter 14, "Storage and File Systems," on page 127 and the *OES 2 SP3: Dynamic Storage Technology Administration Guide*.

1.7.2 OES 2 Migration Tools

In addition to the legacy Server Consolidation and Migration Toolkit, OES 2 includes new migration tools for migrating data and services from NetWare to OES 2.

For more information, see Chapter 9, "Migrating and Consolidating Existing Servers and Data," on page 77.

1.7.3 Xen Virtualization Technology

Both OES 2 and NetWare 6.5 SP8 can run in virtual machines on either an OES 2 or a SUSE® Linux Enterprise Server 10 SP1 or later server. This is especially valuable to those organizations that are deploying new hardware that doesn't run NetWare as a physical installation.

For more information, see Chapter 10, "Virtualization in OES 2," on page 79.

1.8 Links to What's New Sections

The following table provides links to the What's New sections in the documentation for all OES 2 products.

Table 1-1 *What's New*

Product	Link to What's New Section
Archive and Version Services 2.1	Linux Administration Guide User Guide
DHCP	Administration Guide
Distributed File Services	Administration Guide
DNS	Administration Guide
Domain Services for Windows	Administration Guide
Dynamic Storage Technology	Administration Guide
File System Management	Management Guide
FTP (Pure-FTPd)	Section 18.5, "Novell FTP (Pure-FTPd) and OES 2," on page 202
Identity Manager 3.6	Getting Started Guide (http://www.novell.com/documentation/idm36/idm_install/data/be1l5dw.html)
iManager 2.7	Administration Guide
Installation	Installation Guide
iPrint	Administration Guide
Linux User Management	Technology Guide
Migration Tool	Administration Guide
NCP Server for OES 2	Administration Guide
NetStorage	Administration Guide
Novell AFP	Administration Guide
Novell CIFS	Administration Guide
Novell Client	Linux Windows XP/2003 Administration Guide Windows 7/2008 Administration Guide
Novell Cluster Services (High Availability)	Administration Guide
Novell FTP (Pure-FTPd)	Section 18.5, "Novell FTP (Pure-FTPd) and OES 2," on page 202
Novell iFolder 3.8	Administration Guide User Guide
Novell Remote Manager	Administration Guide

Product	Link to What's New Section
Novell Storage Services (NSS)	Administration Guide
NSS Auditing Client	What's New for VLOG
OES 2	Installation Guide
OpenWBEM	Administration Guide
QuickFinder 5	Administration Guide
Samba (Linux)	Administration Guide
Server Health Monitoring	This is now available in various Novell Remote Manager dialog boxes on both platforms. For more information, see "Health Monitoring Services" on page 88.
Shadow Volumes	See "Overview of Dynamic Storage Technology" in the *OES 2 SP3: Dynamic Storage Technology Administration Guide*.
SLP (OpenSLP)	Section 13.5.1, "Overview," on page 116
Storage Management Services (SMS)	Administration Guide

1.9 Where's NetWare?

Novell Open Enterprise Server SP3 does not include NetWare. Anyone who wants to deploy NetWare in an OES 2 SP3 environment should download NetWare 6.5 SP8 from the Novell download site (http://download.novell.com/Download?buildid=dpIR3H1ymhk~).

1.9.1 NetWare References in This Guide and Elsewhere

Because many organizations are transitioning their network services from NetWare to OES, information to assist with upgrading from NetWare to OES 2 is included in this guide and in the OES 2 SP3 documentation set—especially in the *OES 2 SP3: Upgrading to OES—Best Practices Guide*.

1.9.2 NetWare Documentation

For NetWare documentation, including installation and configuration instructions, see the NetWare 6.5 SP8 Online Documentation Web site (http://www.novell.com/documentation/nw65).

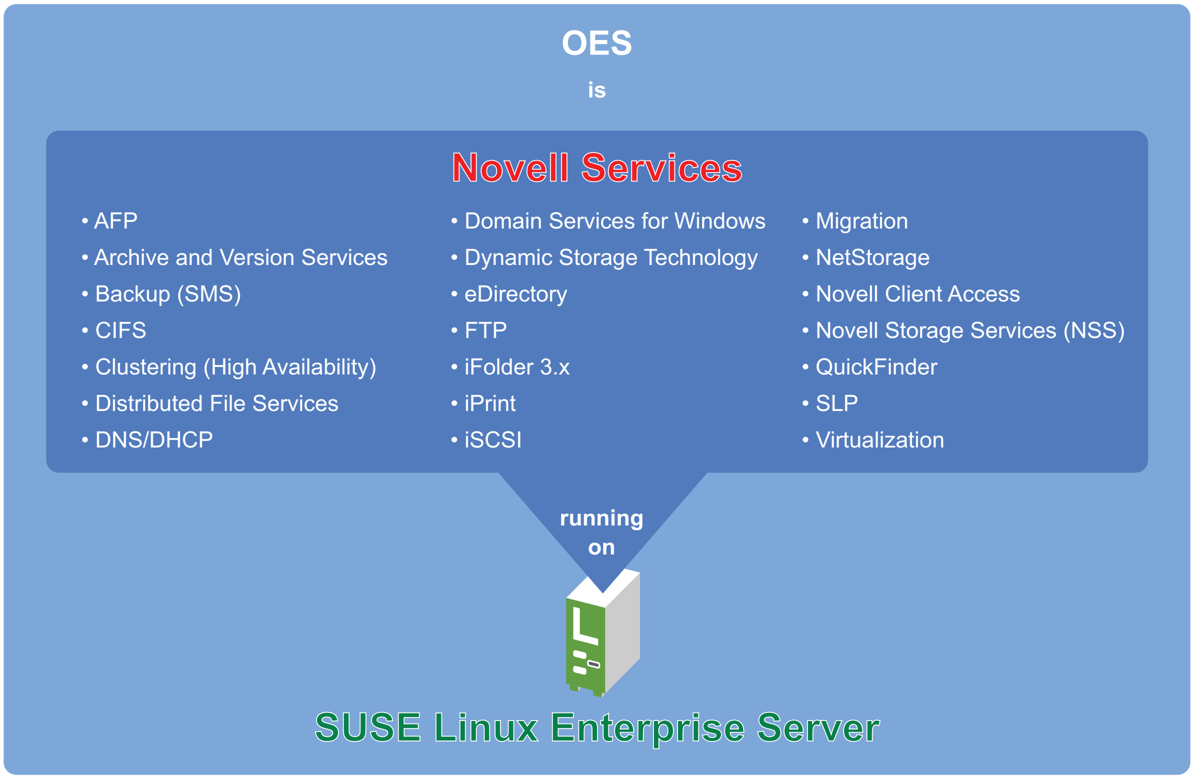
2 What About SLES 10 SP4?

Beginning with the release of the September patch, the supported base for OES 2 SP3 is SLES 10 SP4. The OES 2 SP3 documentation has been updated accordingly.

3 Welcome to Open Enterprise Server 2

Novell Open Enterprise Server 2 (OES 2) includes all the network services that organizations traditionally expect from Novell.

Figure 3-1 *OES 2 Overview*


OES
is
Novell Services
• AFP
• Archive and Version Services
• Backup (SMS)
• CIFS
• Clustering (High Availability)
• Distributed File Services
• DNS/DHCP
• Domain Services for Windows
• Dynamic Storage Technology
• eDirectory
• FTP
• iFolder 3.x
• iPrint
• iSCSI
• Migration
• NetStorage
• Novell Client Access
• Novell Storage Services (NSS)
• QuickFinder
• SLP
• Virtualization
running
on
SUSE Linux Enterprise Server

NOTE: For a list of OES 2 services, see Table 4-1, "Service Comparison Between NetWare 6.5 SP8 and OES 2 SP3 Linux," on page 29.

4 Planning Your OES 2 Implementation

As you plan which OES services to install, you probably have a number of questions. The following sections are designed to help answer your questions and alert you to the steps you should follow for a successful OES implementation.

4.1 What Services Are Included in OES 2?

Table 4-1 summarizes OES services and the differences in the way these services are provided.

Although extensive, this list is not exhaustive. If you are interested in a service or technology not listed, or for documentation for listed services, see the OES Documentation Web site (http://www.novell.com/documentation/oes2).

Table 4-1 *Service Comparison Between NetWare 6.5 SP8 and OES 2 SP3 Linux*

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Access Control Lists	Yes	Yes	In combination with NCP Server, Linux supports the Novell trustee model for file access on NSS volumes and NCP volumes on Linux.
AFP (Apple* File Protocol)	Yes - NFAP	Yes - Novell AFP	AFP services on NetWare and OES are proprietary and tightly integrated with eDirectory and Novell Storage Services (NSS).

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Apache Web Server	Yes - NetWare port of open source product	Yes - Standard Linux	Administration Instance vs. Public Instance on NetWare (http://www.novell.com/documentation/nw65/web_apache_nw/data/aipcu6x.html#aipcu6x). What's Different about Apache on NetWare (http://www.novell.com/documentation/nw65/web_apache_nw/data/ail8hvj.html).
Archive and Version Services (Novell)	Yes	Yes	Setup varies slightly, but there are no functional differences.
Backup (SMS) ◆ SMS ◆ NSS-Xattr	Yes	Yes	SMS provides backup applications with a framework to develop complete backup and restore solutions. For information, see the *OES 2 SP3: Storage Management Services Administration Guide for Linux*. NSS provides extended attribute handling options for NSS on Linux. For information, see "Using Extended Attributes (xAttr) Commands" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
CIFS (Windows File Services)	Yes - NFAP	Yes - Novell CIFS and Novell Samba	Both NFAP and Novell CIFS are Novell proprietary and tightly integrated with eDirectory and Novell Storage Services (NSS). Samba is an open source product distributed with SUSE Linux Enterprise Server (SLES). Novell Samba is enhanced by Novell with configuration settings for eDirectory LDAP authentication via Linux User Management (LUM). Novell Samba is not tightly integrated with NSS on Linux and works with any of the supported file systems.
Clustering	Yes	Yes	"Product Features" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*. "Product Features" in the *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide*.
DFS (Novell Distributed File Services)	Yes	Yes	In combination with NCP Server, DFS supports junctions and junction targets for NSS volumes on Linux and NetWare. DFS also supports junction targets for NCP volumes on non-NSS file systems, such as Reiser, Ext3, and XFS. The VLDB command offers additional options to manage entries in the VLDB for NCP volumes.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
DHCP	Yes	Yes	For a comparison between what is available on OES 2 and NetWare, see Section 13.2.2, “DHCP Differences Between NetWare and OES 2,” on page 103. To plan your DHCP implementations, see “Planning a DHCP Strategy” in the *OES 2 SP3: Novell DNS/DHCP Administration Guide* and “Planning a DHCP Strategy” in the *NW 6.5 SP8: Novell DNS/DHCP Services Administration Guide*.
DNS	Yes	Yes	For a comparison between what is available on OES 2 and NetWare, see Section 13.2.1, “DNS Differences Between NetWare and OES 2,” on page 102. See “Planning a DNS Strategy” in the *OES 2 SP3: Novell DNS/DHCP Administration Guide* and “Planning a DNS Strategy” in the *NW 6.5 SP8: Novell DNS/DHCP Services Administration Guide*.
Dynamic Storage Technology	No	Yes	DST runs on OES 2. An NSS volume on NetWare is supported only as the secondary volume in a shadow pair. When using DST in a cluster, each of the NSS volumes in a shadow pair must reside on OES 2.
eDirectory 8.8	Yes	Yes	No functional differences.
eDirectory Certificate Server	Yes	Yes	No functional differences.
eGuide (White Pages)	Yes	No	This functionality is now part of the Identity Manager 3.6 User Application. For more information, see the Identity Manager 3.6 Documentation Web Site. (http://www.novell.com/documentation/idm36/index.html).
FTP Server	Yes	Yes	FTP file services on OES 2 servers are provided by Pure-FTPd, a free (BSD), secure, production-quality and standard-conformant FTP server. The OES implementation includes support for eDirectory LDAP authentication and the same FTP/SFTP gateway functionality as on NetWare. See Section 18.1.2, “FTP Services,” on page 184.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Health Monitoring Services	Yes	Yes	The Health Monitoring Server, which was included in OES 1, has been removed in OES 2. This is now available in various Novell Remote Manager dialog boxes on both platforms. For more information, see "Health Monitoring Services" on page 88.
Identity Manager 3.6.1 Bundle Edition	No	Yes	IDM 3.6.1 is not available on NetWare.
iPrint	Yes	Yes	See "Overview" in the *OES 2 SP3: iPrint for Linux Administration Guide*, and "Overview" in the *NW 6.5 SP8: iPrint Administration Guide*.
IPX (Internetwork Packet Exchange) from Novell	Yes	No	Novell has no plans to port IPX to OES.
iSCSI	Yes	Yes	The iSCSI target for Linux does not support eDirectory access controls like the NetWare target does. Nor is the iSCSI initiator or target in OES 2 integrated with NetWare Remote Manager management. You use YaST management tools instead. On the other hand, the iSCSI implementation for Linux is newer and performs better. See Linux-iSCSI Project on the Web (http://linux-iscsi.sourceforge.net). See "Overview" in the *NW 6.5 SP8: iSCSI 1.1.3 Administration Guide*.
LDAP Server for eDirectory	Yes	Yes	No functional differences.
Multipath Device Management	Yes	Yes	NetWare uses NSS multipath I/O. Linux uses Device Mapper - Multipath that runs underneath other device management services.
MySQL	Yes - NetWare port of open source product	Yes - Standard Linux	See MySQL.com on the Web (http://www.mysql.com). See "Overview: MySQL" in the *NW 6.5 SP8: Novell MySQL Administration Guide*.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
NCP Volumes	No	Yes	NCP Server on Linux supports creating NCP volumes on Linux POSIX file systems such as Reiser, Ext3, and XFS. For information, see "Managing NCP Volumes" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.
NCP Server	Yes	Yes	NCP services are native to NetWare 6.5 and NSS volumes; to have NCP services on OES, the NCP Server must be installed. See "Benefits of NCP Server" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.
NetStorage	Yes	Yes	NetStorage on Linux offers connectivity to storage locations through the CIFS, NCP, and SSH protocols. NetWare uses only NCP. These and other differences are summarized in "NetStorage" on page 185.
NetWare Traditional File System	Yes	No	Novell has no plans to port the NetWare Traditional File System to Linux.
NetWare Traditional Volumes	Yes	N/A	
NFS	Yes - NFAP	Yes - native to Linux	For NetWare, see "Working with UNIX Machines" in the *NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide*.
NICI (Novell International Cryptography Infrastructure)	Yes	Yes	No functional differences.
NMAS (Novell Modular Authentication Services)	Yes	Yes	No functional differences.
Novell Audit	Yes	Yes	See *OES 2 SP3: NSS Auditing Client Logger (VLOG) Utility Reference*.
Novell Client for Windows and Linux support	Yes	Yes	Novell Client connectivity to OES 2 requires that the NCP Server be installed.
Novell Cluster Services	Yes	Yes	See "Product Features" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*. See "Product Features" in the *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide*.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Novell iFolder 2.*x*	Yes	No	For migration information, see "Migrating iFolder 2.x" in the *OES 2 SP3: Migration Tool Administration Guide*
Novell iFolder 3.8	No	Yes	OES 2 SP3 includes Linux, Macintosh, and Windows clients.
Novell Licensing Services	Yes	No	See Section 5.5.3, "OES 2 Doesn't Support NLS," on page 60.
NSS (Novell Storage Services)	Yes	Yes	Most NSS services are available on both platforms. For a list of NSS features that are not used on Linux, see "Cross-Platform Issues for NSS" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
NTPv3	Yes	Yes	The `ntpd.conf` file on NetWare can replace an OES server's NTP configuration file without modification.
OpenSSH	Yes	Yes	Netware includes a port of the open source product. Linux includes the open source product itself. See "Functions Unique to the NetWare Platform" in the *NW 6.5 SP8: OpenSSH Administration Guide*.
PAM (Pluggable Authentication Modules)	No	Yes	PAM is a Linux service that Novell leverages to provide eDirectory authentication. eDirectory authentication is native on NetWare.
Pervasive.SQL	Yes	No	Pervasive.SQL is available for Linux from the Web (http://www.pervasive.com/support/technical/online_manuals.asp).
PKI (Public Key Infrastructure)	Yes	Yes	No functional differences.
Printing	Yes	Yes	See iPrint.
QuickFinder	Yes	Yes	See Search.
RADIUS	Yes	Yes	See the information on forge.novell.com (http://forge.novell.com/modules/xfmod/project/?edirfreeradius).
Samba	No	Yes	Samba is an open source technology available on OES. Novell provides automatic configuration for authentication through eDirectory. For more information, see the *OES2 SP3: Samba Administration Guide*.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Search (QuickFinder)	Yes	Yes	When indexing a file system, the QuickFinder engine indexes only what it has rights to see. On NetWare, it has full access to all mounted volumes. On Linux, it has rights to only the files that the novlwww user in the www group has rights to see. For more information, see "Security Characteristics" and "Generating an Index For a Linux-Mounted NSS Volume" in the *OES 2 SP3: Novell QuickFinder Server 5.0 Administration Guide*.
SLP	Yes - Novell SLP	Yes - OpenSLP	For OES 2, see Section 13.5, "SLP," on page 116. NetWare uses Novell SLP, which provides caching of Directory Agent scope information in eDirectory. This provides for sharing of scope information among DAs. Starting with SP3, OpenSLP on Linux is customized to provide DA synchronization as well.
Software RAIDS (NSS volumes)	Yes (0, 1, 5, 10, 15)	Yes (0, 1, 5, 10, 15)	See "Understanding Software RAID Devices" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
Storage Management Services (SMS)	Yes	Yes	No functional differences, except that the SBCON backup engine is not supported on Linux. The nbackup engine is available for exploring SMS capabilities, but in a production environment, you should use a third-party, full-featured backup engine.
TCP/IP	Yes	Yes	No functional differences.
Timesync NLM	Yes	No	Timesync will not be ported to Linux. However, NTPv3 is available on both Linux and NetWare. See "Time Services" on page 104.
Tomcat	Yes	Yes	NetWare includes Tomcat 4 and a Tomcat 5 servlet container for iManager 2.7. OES 2 includes Tomcat 5. There is no impact to any of the OES 2 administration tools, which are tested and supported on both platforms. See "Administration Instance vs. Public Instance on NetWare" (http://www.novell.com/documentation/oes2/web_tomcat_nw/data/ahdyran.html#ahdyran)

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Virtual Office (Collaboration)	Yes	No	Virtual Office has been replaced by Novell Teaming + Conferencing. A separate purchase is required. For more information, see the Novell Teaming + Conferencing Web Site (http://www.novell.com/products/teaming/index.html).
WAN Traffic Manager	Yes	No	
Xen Virtualization Guest	Yes	Yes	NetWare 6.5 SP8 (and NetWare 6.5 SP 7) can run on a paravirtualized machine. OES 2 can run on a paravirtualized machine or fully virtualized machine.
Xen Virtualization Host Server	N/A	Yes	

4.2 Which Services Do I Need?

We recommend that you review the brief overviews included at the beginning of each service section in this guide to get a full picture of the solutions that OES 2 offers. It is not uncommon that administrators discover capabilities in OES that they didn't know existed.

4.3 Exploring OES 2 services

We also recommend that you explore commonly used OES services by following the step-by-step instructions provided in the *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare*.

4.4 Plan for eDirectory

eDirectory is the heart of OES network services and security.

If you are installing into an existing tree, be sure you understand the information in Section 15.2.3, "eDirectory Coexistence and Migration," on page 145.

If you are creating a new eDirectory tree on your network, you must do some additional planning before you install the first server into the tree. The first server is important for two reasons:

- You create the basic eDirectory tree structure during the first installation
- The first server permanently hosts the Certificate Authority for your organization

To ensure that your eDirectory tree meets your needs, take time to plan the following:

- **Structure of the eDirectory tree:** A well-designed tree provides containers for servers, users, printers, etc. It is also optimized for efficient data transfer between geographically dispersed locations. For more information, see "Designing Your Novell eDirectory Network" in the *Novell eDirectory 8.8 SP7 Administration Guide*.
- **Time synchronization:** eDirectory requires that all OES 2 servers, both NetWare and Linux, be time synchronized. For more information, see Chapter 13.3, "Time Services," on page 104.

- **Partitions and replicas:** eDirectory allows the tree to be partitioned for scalability. Replicas (copies) of the partitions provide fault tolerance within the tree. The first three servers installed into an eDirectory tree automatically receive replicas of the tree's root partition. You might want to create additional partitions and replicas. For more information, see "Managing Partitions and Replicas" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

For information on these and other eDirectory planning tasks, see the *Novell eDirectory 8.8 SP7 Administration Guide*.

The *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare* provides a basic introduction to creating container objects as well as Group and User objects in eDirectory.

4.5 Prepare Your Existing eDirectory Tree for OES 2

If you are installing OES 2 into an existing tree, you must use Deployment Manager (located on the NetWare 6.5 SP8 DVD) to see whether your tree requires any updates.

For instructions on running Deployment Manager, see "Preparing to Install NetWare 6.5 SP8" in the *NW65 SP8: Installation Guide*.

4.6 Identify a Purpose for Each Server

Large networks usually have one or more servers dedicated to providing a single network service. For example, one or more servers might be designated to provide Novell iFolder file services to network users while other servers provide iPrint printing services for the same users.

For smaller organizations, it is often not practical or cost effective to dedicate servers to providing a single service. For example, the same server might provide both file and print services to network users.

Prior to installing a new server on your network, you should identify the service or services that it will provide and see how it will integrate into your overall network service infrastructure.

4.7 Understand Server Requirements

OES 2 and NetWare 6.5 SP8 both have specific hardware and software requirements.

Prior to installing OES, make sure your server machine and network environment meet the requirements outlined in the following sections:

- **OES 2 Server (Physical):** "Preparing to Install OES 2 SP3" in the *OES 2 SP3: Installation Guide*.
- **OES 2 Server (Virtual):** "System Requirements" in the *OES 2 SP3: Installation Guide*.
- **NetWare 6.5 SP8 Server (Physical):** "Meeting System Requirements" in the *NW65 SP8: Installation Guide*.
- **NetWare 6.5 SP8 Server (Virtual):** "Planning for NetWare VM Guest Servers" in the *OES 2 SP3: Installation Guide*.

4.8 Understand User Restrictions and Linux User Management

If you plan to use Linux User Management, be sure you understand the security implications before you accept the default PAM-enabled service settings. The implications are explained in Section 22.2.2, "User Restrictions: Some OES 2 Limitations," on page 229.

4.9 Caveats to Consider Before You Install

IMPORTANT: As support packs are released, there are sometimes new caveats identified. Be sure to always check the OES Readme (http://www.novell.com/documentation/oes2/oes_readme/data/readme.html) for items specific to each support pack.

This section discusses the following installation/migration caveats:

- Section 4.9.1, "Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes," on page 38
- Section 4.9.2, "Always Double-Check Service Configurations Before Installing," on page 39
- Section 4.9.3, "Back Button Doesn't Reset Configuration Settings," on page 39
- Section 4.9.4, "Cluster Upgrades Must Be Planned Before Installing OES 2," on page 39
- Section 4.9.5, "Cross-Protocol File Locking Has Changed," on page 40
- Section 4.9.6, "Do Not Create Local (POSIX) Users," on page 40
- Section 4.9.7, "Do Not Upgrade to eDirectory 8.8 Separately," on page 40
- Section 4.9.8, "Follow the Instructions for Your Chosen Platforms," on page 40
- Section 4.9.9, "If You've Ever Had OES 1 Linux Servers with LUM and NSS Installed," on page 41
- Section 4.9.10, "iFolder 3.8 Considerations," on page 44
- Section 4.9.11, "Incompatible TLS Configurations Give No Warning," on page 44
- Section 4.9.12, "Installing into an Existing eDirectory Tree," on page 44
- Section 4.9.13, "NetWare Caveats," on page 45
- Section 4.9.14, "Novell Distributed Print Services Cannot Migrate to Linux," on page 46
- Section 4.9.15, "NSS Caveats," on page 46
- Section 4.9.16, "Plan eDirectory Before You Install," on page 47
- Section 4.9.17, "Samba Enabling Disables SSH Access," on page 47
- Section 4.9.18, "Unsupported Service Combinations," on page 47
- Section 4.9.19, "VNC Install Fails to Set the IP Address in /etc/hosts," on page 49

4.9.1 Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes

After you add a Linux node to a cluster, you cannot add more NetWare nodes. For more information, see the *OES 2 SP3: Novell Cluster Services NetWare to Linux Conversion Guide*.

4.9.2 Always Double-Check Service Configurations Before Installing

It is critical and you double-check your service configurations on the Novell Open Enterprise Server Configuration summary page before proceeding with an installation. One reason for this is explained in Section 4.9.3, “Back Button Doesn’t Reset Configuration Settings,” on page 39.

4.9.3 Back Button Doesn’t Reset Configuration Settings

During an installation, after you configure eDirectory and reach the Novell Open Enterprise Server Configuration summary screen, service configuration settings have been “seeded” from the eDirectory configuration.

If you discover at that point that something in the eDirectory configuration needs to change, you can change the settings by clicking the *eDirectory* link on the summary page or by clicking the Back button.

In both cases when you return to the summary page, the eDirectory configuration has changed, but the individual service configurations have the same eDirectory settings you originally entered. These must each be changed manually.

For example, if you specified the wrong server context while initially configuring eDirectory, the NSS and LUM configurations still have the wrong context. You must select each service individually and change the server context in them.

Unless you manually change the services affected by changes to eDirectory, your services will at best not work as expected and at worst completely fail.

4.9.4 Cluster Upgrades Must Be Planned Before Installing OES 2

Because of differences between Novell Cluster Services on NetWare 6.5 SP8 and OES 2, there are important issues to consider before combining them into a mixed node cluster, as explained in the following sections.

- “Service Failover in a Mixed Cluster” on page 39
- “Working with Mixed Node Clusters” on page 39

Service Failover in a Mixed Cluster

The only cluster-enabled service that can fail over cross-platform (run on either OES 2 or NetWare 6.5 SP8) is cluster-enabled NSS pools. All other services (iPrint, iFolder, etc.) can only fail over between servers that are the same platform. For example, an iPrint service that is running on an OES 2 server can fail over to another OES 2 server in the cluster, but the service cannot fail over to an NetWare 6.5 SP8 server.

Working with Mixed Node Clusters

The following points apply to working with mixed NetWare and OES clusters:

- You cannot uses EVMSGUI to create a Linux POSIX file system as a cluster resource until the entire cluster is migrated to Linux.
- You cannot migrate or fail over a Linux POSIX file system cluster resource to a NetWare cluster node.

- Only NSS pool cluster resources that are created on a NetWare cluster node can be failed over between Linux and NetWare nodes.
- NetWare NSS to Linux NSS failover requires that the Linux node be configured for NSS and that the version of NSS supports the NSS media format and features being used by the NSS pool cluster resource.
- The new NSS media format in OES 2 is not available for OES 1 SP2 Linux and earlier. After a volume has been upgraded to the new media format, you cannot fail it over to a node that is running OES 1 SP2 Linux or earlier.

4.9.5 Cross-Protocol File Locking Has Changed

If you plan to use Novell CIFS, Novell AFP and/or NCP file services in combination with each other, be sure to read Section 1.5.5, "Cross-Protocol File Locking Change," on page 19.

4.9.6 Do Not Create Local (POSIX) Users

During the OES 2 install you are prompted by the SLES portion of the install to create at least one user besides `root` and you are warned if you bypass the prompt.

Creating local users is not recommended on OES 2 servers because user management in OES 2 is managed entirely in eDirectory. The only local user you need on the server is the `root` user. Creating other local users can, in fact, cause unnecessary confusion and result in service-access problems that are difficult to troubleshoot.

eDirectory users are enabled for POSIX access through the Linux User Management (LUM) technology installed by default on every OES 2 server.

Also be aware that not all OES services require that users are LUM-enabled. Novell Client users, for example, can access NCP and NSS volumes on OES 2 servers just as they do on NetWare without any additional configuration.

For more information about this topic, see Section 16.2, "Linux User Management: Access to Linux for eDirectory Users," on page 153.

4.9.7 Do Not Upgrade to eDirectory 8.8 Separately

If you are running OES 1 SP2, do not upgrade to eDirectory 8.8 independently of upgrading to OES 2 SP3.

For example, do not upgrade from eDirectory 8.7.3 to eDirectory 8.8.2 through the oes-edir88 patch channel prior to upgrading to OES 2 SP3. Doing so causes configuration problems that the OES 2 SP3 install is not designed to handle.

4.9.8 Follow the Instructions for Your Chosen Platforms

Although installing OES 2 services on Linux or NetWare is a straightforward process, the installation processes are platform-specific, requiring different sets of media and different installation programs.

4.9.9 If You’ve Ever Had OES 1 Linux Servers with LUM and NSS Installed

Having NSS volumes on OES servers requires certain system-level modifications, most of which are automatic. For more information, see Appendix I, “System User and Group Management in OES 2 SP3,” on page 269.

However, as OES has evolved, some initially defined conventions regarding system Users have needed adjustment. Be sure to read the information and follow the instructions in this section if your network has ever included an OES 1 Linux server with both LUM and NSS installed.

- “NetStorage, XTier, and Their System Users” on page 41
- “An NSS Complication” on page 41
- “eDirectory Solves the Basic Problem” on page 41
- “ID Mismatches on OES 1” on page 42
- “The OES 1 Solution: The nssid.sh Script” on page 42
- “OES 2 SP1 or Later Requires a New Approach” on page 42
- “The OES 2 Solution: Standardizing the UIDs on all OES servers” on page 42

NetStorage, XTier, and Their System Users

By default, certain OES services, such as NetStorage, rely on a background Novell service named XTier.

To run on an OES server, XTier requires two system-created users (named `novlxsrvd` and `novlxregd`) and one system-created group that the users belong to (named `novlxtier`).

An NSS Complication

The two system users and their group are created on the local system when XTier is installed. For example, they are created when you install NetStorage, and their respective UIDs and GID are used to establish ownership of the service’s directories and files.

For NetStorage to run, these XTier users and group must be able to read data on all volume types that exist on the OES server.

As long as the server only has Linux traditional file systems, such as Ext3, Reiser, or XFS, NetStorage runs without difficulties.

However, if the server has NSS volumes, an additional requirement is introduced. NSS data can only be accessed by eDirectory users. Consequently, the local XTier users can’t access NSS data, and NetStorage can’t run properly.

eDirectory Solves the Basic Problem

Therefore, when NSS volumes are created on the server, the XTier users are moved to eDirectory and enabled for Linux User Management (LUM). See Section 16.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 153.

After the move to eDirectory, they can function as both eDirectory and POSIX users, and they no longer exist on the local system.

ID Mismatches on OES 1

Problems with OES 1 occurred when additional OES NetStorage servers with NSS volumes were installed in the same eDirectory container. Because the UIDs and GID were assigned by the Linux system, unless the installation process was exactly the same for each OES 1 Linux server, the UIDs and GID didn't match server-to-server.

When the local XTier UIDs and GID on subsequently installed servers didn't match the XTier UIDs and GID in eDirectory, NetStorage couldn't access the NSS volumes on the server.

The OES 1 Solution: The nssid.sh Script

To solve this problem, the OES 1 installation program looked for XTier ID conflicts, and if the IDs on a newly installed server didn't match the IDs in eDirectory, the program generated a script file named `nssid.sh`. The documentation instructed installers to always check for an `nssid.sh` file on a newly installed server, and if the file was found, to run it. The `nssid.sh` script synchronized all of the XTier IDs with those that had already been stored in eDirectory.

This solution remained viable through the first release of OES 2.

OES 2 SP1 or Later Requires a New Approach

Unfortunately, system-level changes in SUSE Linux Enterprise Server 10 SP2 invalidated the `nssid.sh` script solution for OES 2 SP1. Synchronizing the XTier IDs with an OES 1 installation can now cause instability in other non-OES components. Therefore, starting with OES 2 SP1, you should standardize all XTier IDs on existing servers before installing a new OES 2 server with XTier-dependent services.

The OES 2 Solution: Standardizing the UIDs on all OES servers

If your eDirectory tree has ever contained an OES 1 Linux server with NSS and LUM installed, do the following on each server (including OES 2) that has NSS and LUM installed:

1 Log in as `root` and open a terminal prompt. Then enter the following commands:

```
id novlxregd
```

```
id novlxsrvd
```

The standardized XTier IDs are UID 81 for `novlxregd`, UID 82 for `novlxsrvd`, and GID 81 for `novlxtier`.

2 (Conditional) If you see the following ID information, the XTier IDs are standardized and you can start over with Step 1 for the next server:

```
uid=81(novlxregd) gid=81(novlxtier) groups=81(novlxtier)
uid=82(novlxsrvd) gid=81(novlxtier) groups=81(novlxtier),8(www)
```

3 (Conditional) If you see different IDs than those listed above, such as 101, 102, 103, etc., record the numbers for both XTier users and the novlxtier group, then continue with Step 4.

You need these numbers to standardize the IDs on the server.

4 Download the following script file:

- `fix_xtier_ids.sh` (http://www.novell.com/documentation/oes2/scripts/fix_xtier_ids.sh)

5 Customize the template file by replacing the variables marked with angle brackets (<>) as follows:

- **<server_name>:** The name of the server object in eDirectory.

  This variable is listed on line 38 in the file. Replace it with the server name.

  For example, if the server name is myserver, replace *<server_name>* with *myserver* so that the line in the settings section of the script reads

  ```
  server=myserver
  ```

- **<context>:** This is the context of the XTier user and group objects.

  Replace this variable with the fully distinguished name of the context where the objects reside.

  For example, if the objects are an Organizational Unit object named servers, replace ou=servers,o=company with the fully distinguished name.

- **<admin fdn>:** The full context of an eDirectory admin user, such as the Tree Admin, who has rights to modify the XTier user and group objects.

  Replace this variable with the admin name and context, specified with comma-delimited syntax.

  For example, if the tree admin is in an Organization container named company, the full context is cn=admin,o=company and the line in the settings section of the script reads

  ```
  admin_fdn="cn=admin,o=company"
  ```

- **<novlxregd_uid>:** This is the UID that the system assigned to the local `novlxregd` user. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

  Replace this variable with the UID reported for the novlxregd user on this server as listed in Step 1 on page 42.

  For example, if the UID for the novlxregd user is 101, change the line to read

  ```
  novlxregd_uid=101
  ```

- **<novlxsrvd_uid>:** This is the UID that the system assigned to the local novlxsrvd user. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

  Replace this variable with the UID reported for the novlxsrvd user on this server as listed when you ran the commands in Step 1 on page 42.

  For example, if the UID for novlxsrvd_uid is 102, change the line to read

  ```
  novlxsrvd_uid=102
  ```

- **<novlxtier_gid>:** This is the GID that the system assigned to the local novlxtier group. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

  Replace this variable with the GID reported for the novlxtier group on this server as listed when you ran the commands in Step 1 on page 42.

  For example, if the GID for novlxtier_gid is 101, change the line to read

  ```
  novlxtier_gid=101
  ```

6 Make the script executable and then run it on the server.

IMPORTANT: Changes to the XTier files are not reported on the terminal.

Error messages are reported, but you can safely ignore them. The script the entire file system, and some files are locked because the system is running.

7 Repeat from Step 1 for each of the other servers in the same context.

4.9.10 iFolder 3.8 Considerations

For best results, be sure you read and carefully follow the instructions in the *Novell iFolder 3.8.4 Administration Guide*, and especially "Deploying iFolder Server ." This is especially critical if you plan to use NSS for your iFolder 3.8 data volume.

4.9.11 Incompatible TLS Configurations Give No Warning

When you install a new eDirectory tree, the eDirectory Configuration - New or Existing Tree screen has the *Require TLS for Simple Binds with Password* option selected by default. If you keep this configuration setting, the eDirectory LDAP server requires that all communications come through the secure LDAP port that you specified on the eDirectory Configuration - Local Server Configuration screen. By default, this is port 636.

Unfortunately, the OES install doesn't display a warning if you subsequently configure OES services to use non-TLS (non-secure) LDAP communications (port 389). The installation proceeds normally but the service configuration fails.

For example, if you accept the TLS default, then configure Novell DHCP to use non-secure communications (by deselecting the *Use secure channel for configuration* option), the OES install doesn't warn that you have created an incompatible configuration.

After eDirectory and the iManager plug-ins install successfully, the Novell DHCP configuration fails. You must then use iManager to change either the LDAP server configuration or the Novell DHCP configuration to support your preferred communication protocol.

Simply enabling non-TLS LDAP communications doesn't disable TLS. It merely adds support for non-secure communications with the LDAP server.

4.9.12 Installing into an Existing eDirectory Tree

Novell Support has reported a significant number of installation incidents related to eDirectory health and time synchronization. To avoid such problems, do the following prior to installing OES:

- "Consider Coexistence and Migration Issues" on page 44
- "Do Not Add OES to a Server That Is Already Running eDirectory" on page 45
- "Be Sure That eDirectory Is Healthy" on page 45
- "Be Sure That Network Time Is Synchronized" on page 45
- "Be Sure that OpenSLP on OES 2 Is Configured Properly" on page 45

Consider Coexistence and Migration Issues

If you are installing a new OES 2 server into an existing eDirectory tree, be sure to read and follow the instructions in "Preparing eDirectory for OES 2 SP3" in the *OES 2 SP3: Installation Guide*.

Do Not Add OES to a Server That Is Already Running eDirectory

Although you can add OES to an existing SLES 10 server if needed, you cannot install OES on a SLES 10 server that is already running eDirectory.

eDirectory must be installed in conjunction with the installation of OES services.

Be Sure That eDirectory Is Healthy

Review and follow the guidelines in "Keeping eDirectory Healthy" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

Be Sure That Network Time Is Synchronized

OES2 Linux and NetWare 6.5 SP8 servers can receive network time from either an existing eDirectory server or from an NTP time source. The critical point is that the entire tree must be synchronized to the same time source. For example, do not set your new OES 2 server to receive time from an NTP source unless the whole tree is synchronized to the same NTP source.

For an in-depth explanation of OES time synchronization, see Chapter 13.3, "Time Services," on page 104.

Be Sure that OpenSLP on OES 2 Is Configured Properly

Novell SLP (NetWare) and OpenSLP (Linux) can coexist, but there are differences between the services that you should understand before deciding which to use or before changing your existing SLP service configuration. For more information, see Section 13.5, "SLP," on page 116.

4.9.13 NetWare Caveats

- "NetWare Licenses and OES 2 Trees" on page 45
- "NetWare 6.5 Servers Must Be Running SP3 or Later" on page 46

NetWare Licenses and OES 2 Trees

OES doesn't use Novell Licensing Services (Section 5.5, "Licensing," on page 59). As a result, OES servers don't need a license container in eDirectory as part of the server installation.

In a mixed OES 2 and NetWare eDirectory tree, at least one NetWare server must hold a replica for each partition where there is a NetWare server object. Without this configuration, It is impossible to install licenses or to service requests from NetWare servers to consume those licenses.

If you need to install a NetWare server in an OES tree, you must do the following after installing the first NetWare server in a partition:

1. Install iManager on the NetWare server, or use iManager Workstation.

   You can do this during initial installation or later as described in "Installing iManager" in the *Novell iManager 2.7.6 Installation Guide*.
2. Add a Read/Write replica to the server as described in "Adding a Replica" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

3 Install the NetWare license as described in "Installing and Removing License Certificates" in the *NW 6.5 SP8: Licensing Services Administration Guide*.

The iManager Licensing plug-in is not installed on OES servers. If you have configured Role-Based Services, you need to make sure the licensing plug-in is installed and added to the RBS collection. For more information, see "Upgrading iManager" in the *Novell iManager 2.7.6 Installation Guide*.

NetWare 6.5 Servers Must Be Running SP3 or Later

If you are installing OES 2 servers into a tree containing NetWare 6.5 servers, be sure that the following server types have been updated to SP3 or later prior to installing OES 2:

- **SLP Directory Agents:** If the SLP Directory Agents on your network are not running NetWare 6.5 SP3 or later, installing an OES 2 server into the tree can cause the DA servers to abend.
- **LDAP Servers:** If the LDAP servers referenced in your installation are not running NetWare 6.5 SP3 or later, the servers might abend during a schema extension operation.

4.9.14 Novell Distributed Print Services Cannot Migrate to Linux

NDPS clients are not supported on OES. You must therefore migrate any NDPS clients to iPrint before you migrate your print services to OES. For more information, see "Migrating NDPS Printers to iPrint" in the *NW 6.5 SP8: iPrint Administration Guide*.

4.9.15 NSS Caveats

- "About New Media Support and Clusters" on page 46
- "Removable Media Cannot Be Mounted on OES 2" on page 46

About New Media Support and Clusters

The new media support for hard links on OES 2 NSS volumes was not available for OES 1 SP2 Linux and earlier, but it was available for NetWare 6.5 SP4 and later.

If you've already upgraded the media format of the volume, you cannot fail over to a node that is running OES 1 SP2 until you have upgraded the node to OES 2.

Removable Media Cannot Be Mounted on OES 2

CD and DVD media and image files cannot be mounted as NSS volumes on OES; instead, they are mounted as Linux POSIX file systems.

For more details about NSS compatibility, see "Cross-Platform Issues for NSS Volumes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

4.9.16 Plan eDirectory Before You Install

Although the default eDirectory settings work for simple trees, they are not usually practical for a production implementation. For example, by default the tree Admin user and the server are installed in the same context.

Some administrators, when they discover that the tree structure doesn't meet their needs, assume they can rectify the situation by uninstalling and then reinstalling eDirectory. This simply cannot be done.

In fact, OES services cannot be uninstalled. For more information, see "Disabling OES 2 Services" in the *OES 2 SP3: Installation Guide*.

4.9.17 Samba Enabling Disables SSH Access

Enabling users for Samba automatically disables SSH access for them. However, this default configuration can be changed. For more information, see Section 12.4, "SSH Services on OES 2," on page 95.

4.9.18 Unsupported Service Combinations

Do not install any of the following service combinations on the same server. Although not all of the combinations shown in Table 4-2 cause pattern conflict warnings, Novell does not support any of them.

Table 4-2 *Unsupported Service Combinations*

Service	Unsupported on the Same Server
Novell AFP	◆ File Server (Samba) ◆ Netatalk ◆ Novell Domain Services for Windows ◆ Novell Samba ◆ Xen Virtual Machine Host Server
Novell Archive and Version Services	◆ Novell Domain Services for Windows (DSfW) ◆ Xen Virtual Machine Host Server
Novell Backup / Storage Management Services	No restrictions
Novell CIFS	◆ File Server (Samba) ◆ Novell Domain Services for Windows ◆ Novell Samba ◆ Xen Virtual Machine Host Server
Novell Cluster Services (NCS)	◆ High Availability ◆ Novell Domain Services for Windows DSfW can actually be installed and run on the same server as NCS, but DSfW cannot run as a clustered service.
Novell DHCP	◆ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell DNS	◆ Xen Virtual Machine Host Server
Novell Domain Services for Windows	◆ File Server (Samba) ◆ Novell AFP ◆ Novell Archive and Version Services ◆ Novell CIFS ◆ Novell Cluster Services (NCS) NCS can actually be installed and run on the server, but DSfW cannot run as a clustered service. ◆ Novell FTP ◆ Novell iFolder ◆ Novell NetStorage ◆ Novell Pre-Migration Server ◆ Novell QuickFinder ◆ Novell Samba ◆ Xen Virtual Machine Host Server
Novell eDirectory	◆ Directory Server (LDAP) ◆ Xen Virtual Machine Host Server
Novell FTP	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell iFolder	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell iManager	◆ Xen Virtual Machine Host Server
Novell iPrint	◆ Print Server (CUPS) CUPS components are actually installed, but CUPS printing is disabled. For more information, see Section 7.9.6, “iPrint Disables CUPS Printing on the OES 2 Server,” on page 70. ◆ Xen Virtual Machine Host Server
Novell Linux User Management (LUM)	No restrictions
Novell NCP Server / Dynamic Storage Technology	◆ Xen Virtual Machine Host Server
Novell NetStorage	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell Pre-Migration Server	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell QuickFinder	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell Remote Manager (NRM)	◆ Xen Virtual Machine Host Server
Novell Samba	◆ File Server (Samba) ◆ Novell CIFS ◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell Storage Services (NSS)	◆ Xen Virtual Machine Host Server
Xen Virtual Machine Host Server	◆ File Server (Samba) ◆ Novell AFP ◆ Novell Archive and Version Services ◆ Novell CIFS ◆ Novell DHCP ◆ Novell DNS ◆ Novell Domain Services for Windows ◆ Novell eDirectory ◆ Novell FTP ◆ Novell iFolder ◆ Novell iManager ◆ Novell iPrint ◆ Novell NCP Server / Dynamic Storage Technology ◆ Novell NetStorage ◆ Novell Pre-Migration Server ◆ Novell QuickFinder ◆ Novell Remote Manager (NRM) ◆ Novell Samba ◆ Novell Storage Services ◆ Print Server (CUPS)

4.9.19 VNC Install Fails to Set the IP Address in /etc/hosts

If you install through a VNC connection, the `/etc/hosts` file is configured with a loop back address assigned to the hostname. This can cause problems with services.

Using a text editor, modify `/etc/hosts` so that the hostname is associated with its actual IP address.

4.10 Consider Coexistence and Migration Issues

You probably have a network that is already providing services to network users. In many cases, the services you are currently running will influence your approach to implementing OES 2. In some cases, there are specific paths to follow so that the OES 2 integration process is as smooth as possible.

Novell has invested considerable effort in identifying service coexistence and migration issues you might face. We understand, however, that we can't anticipate every combination of services that you might have. Therefore, we intend to continue developing coexistence and migration information.

For information about coexistence of OES 2 servers with existing NetWare and Linux networks, see Chapter 9, "Migrating and Consolidating Existing Servers and Data," on page 77.

4.11 Understand Your Installation Options

Before installing OES, you should be aware of the information in the following sections:

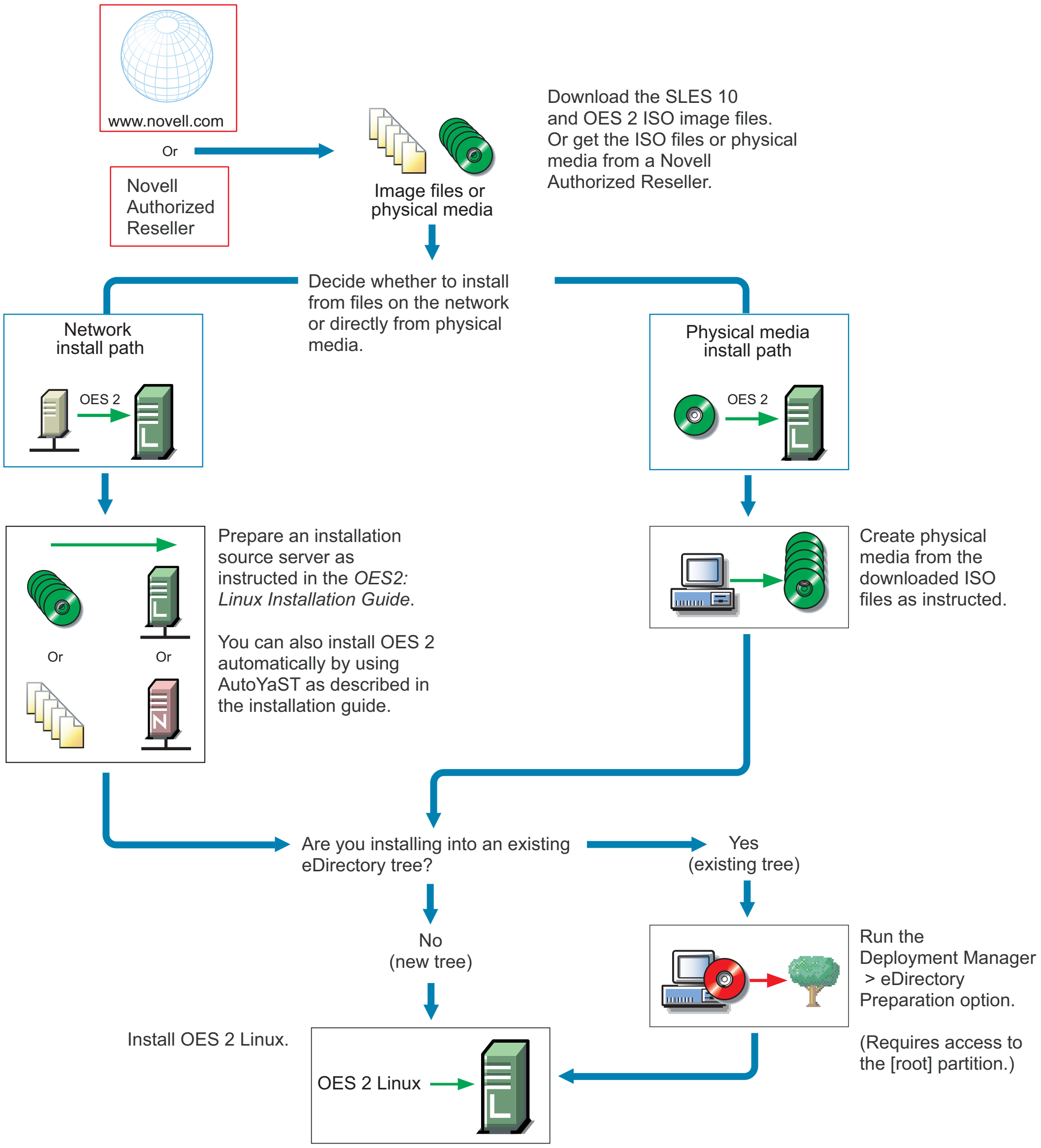
- Section 4.11.1, "OES 2 Installation Overview," on page 50
- Section 4.11.2, "About Your Installation Options," on page 51
- Section 4.11.3, "Use Predefined Server Types (Patterns) When Possible," on page 52
- Section 4.11.4, "If You Want to Install in a Lab First," on page 52
- Section 4.11.5, "If You Want to Install NSS on a Single-Drive Linux Server," on page 53

4.11.1 OES 2 Installation Overview

The software and network preparation processes required to install OES 2 are outlined in Figure 4-1.

NOTE: Chapter 5, "Getting and Preparing OES 2 Software," on page 55 contains instructions for obtaining the ISO image files referred to in the following illustration.

Figure 4-1 *OES 2 Install Preparation*


www.novell.com
Or
Novell Authorized Reseller
Image files or physical media
Download the SLES 10 and OES 2 ISO image files. Or get the ISO files or physical media from a Novell Authorized Reseller.
Decide whether to install from files on the network or directly from physical media.
Network install path
OES 2
Physical media install path
OES 2
Or
Or
Prepare an installation source server as instructed in the OES2: Linux Installation Guide.
You can also install OES 2 automatically by using AutoYaST as described in the installation guide.
Create physical media from the downloaded ISO files as instructed.
Are you installing into an existing eDirectory tree?
Yes (existing tree)
No (new tree)
Run the Deployment Manager > eDirectory Preparation option.
(Requires access to the [root] partition.)
Install OES 2 Linux.
OES 2 Linux

For detailed instructions, see "Setting Up a Network Installation Source" in the *OES 2 SP3: Installation Guide*.

4.11.2 About Your Installation Options

As illustrated in the previous section, OES 2 lets you install from either physical media or from files on the network.

- "OES 2 Options" on page 52
- "Virtual Machine Installation Options" on page 52

OES 2 Options

OES 2 includes numerous installation options as documented in the *OES 2 SP3: Installation Guide*.

- **CD/DVD Install:** You can install SLES 10 by using CDs or a DVD and then install OES 2 from a CD, all of which can be either obtained from a Novell Authorized Reseller or created from downloaded ISO image files.

  See "Preparing Physical Media for a New Server Installation or an Upgrade " in the *OES 2 SP3: Installation Guide*.
- **Network Install:** You can install from the network by using the NFS, FTP, or HTTP protocol.

  Installing from the network saves you from swapping CDs on the server during the installation.

  See "Setting Up a Network Installation Source" in the *OES 2 SP3: Installation Guide*.
- **Automated Install:** You can install from the network by using an AutoYaST file.

  This lets you install without providing input during the installation process. It is especially useful for installing multiple servers with similar configurations.

  See "Using AutoYaST to Install and Configure Multiple OES Servers" in the *OES 2 SP3: Installation Guide*.

Virtual Machine Installation Options

Virtual machine installations offer additional options. For more information, see

- "Installing, Upgrading, or Updating OES on a Xen-based VM" in the *OES 2 SP3: Installation Guide*
- "Installing and Managing NetWare on a Xen-based VM" in the *OES 2 SP3: Installation Guide*

4.11.3 Use Predefined Server Types (Patterns) When Possible

Both OES 2 and NetWare 6.5 SP8 include predefined server installation options that install only the components required to provide a specific set of network services. In the OES 2, these server types are called *patterns*.

For example, if you want to install an OES 2 server that provides enterprise level print services, you should select the *Novell iPrint Server* pattern during the installation.

You should always choose a predefined server type if one fits the intended purpose of your server. If not, you can choose to install a customized OES 2 server with only the service components you need.

More information about server patterns is available in the installation guides:

- **OES 2:** "OES Services Pattern Descriptions" in the *OES 2 SP3: Installation Guide*
- **NetWare 6.5 SP8:** "Choosing a Server Pattern" in the *NW65 SP8: Installation Guide*

4.11.4 If You Want to Install in a Lab First

Many organizations prefer to install products on smaller servers for testing in a lab prior to full deployment. The *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare* walks you through installing and exploring all the basic OES 2 services.

4.11.5 If You Want to Install NSS on a Single-Drive Linux Server

Many are interested in Novell Storage Services (NSS) running on Linux. If you plan to experiment with NSS on a single-drive server, be sure to follow the instructions in "Installing with EVMS as the Volume Manager of the System Device" in the *OES 2 SP3: Installation Guide*.

5 Getting and Preparing OES 2 Software

This section contains instructions for getting and preparing Open Enterprise Server 2 software and discusses the following topics:

If you have not already done so, we recommend that you review the information in Section 4.11, “Understand Your Installation Options,” on page 50.

5.1 Do You Have Upgrade Protection?

If you have Novell Upgrade Protection, you can upgrade to OES 2 and the associated support packs, free of charge until your upgrade protection expires. After your protection expires, the OES 2 upgrade link disappears from your account page.

For more information and to start the upgrade process, do the following:

1. Using your Novell account information, log in to the Novell Web Site (http://www.novell.com/nps).
2. Click *Customer Center* and log in, using your Novell account username and password to access the Novell Customer Center home page.
3. Follow the instructions on the page to obtain the upgrade to Open Enterprise Server 2.

5.2 Do You Want 32-Bit or 64-Bit OES?

Compatibility is the first thing to consider as you start planning which software to download and install.

OES 2 is a set of services or an “add-on product” that runs on SUSE Linux Enterprise Server (SLES 10) and is available in both 32-bit and 64-bit versions. These two versions are required for compatibility with SLES 10 and the server hardware that it runs on. Having two versions of OES introduces a little more complexity into your planning, as illustrated in Table 5-1.

Table 5-1 *OES 2, SLES 10, and Server Hardware Compatibility Matrix*

OES 2 SP3 Version	SLES 10 SP4	Server Hardware	Notes
32-bit (i386)	32-bit (i386)	32-bit 64-bit	The 32-bit version of OES 2 SP3 requires the 32-bit version of SLES 10 SP4. If you plan to install 64-big SLES, you should also install 64-bit OES. Attempting to install the 32-bit version of OES as an add-on product to the 64-bit version of SLES 10 generates numerous dependency errors and is not supported. 32-bit software (OES and SLES) can be installed on either 32-bit or 64-bit hardware.
64-bit (x86_64)	64-bit (x86_64)	64-bit	The 64-bit version of OES 2 SP3 requires the 64-bit version of SLES 10 SP4, and they can only be installed on 64-bit hardware.

5.3 Do You Want to Purchase OES 2 or Evaluate It?

If you want to evaluate OES prior to purchasing it, skip to the next section, Evaluating OES 2 Software.

If you have decided to purchase OES 2, visit the Novell How to Buy OES 2 Web page (http://www.novell.com/products/openenterpriseserver/howtobuy.html).

When you purchase OES 2, you receive two activation codes for OES 2 (one for OES 2 services and one for SUSE Linux Enterprise Server 10). Both codes are required for registering an OES 2 system in the Novell Customer Center. After it is registered, your server can receive online updates, including the latest support pack.

As part of the purchase process, it is important that you understand the OES 2 licensing model. For a brief description, see Section 5.5, "Licensing," on page 59.

After completing your purchase, the installation process goes more smoothly if you understand your installation options. If you haven't already done so, be sure to review the information in Section 4.11, "Understand Your Installation Options," on page 50 and then skip to Chapter 6, "Installing OES 2," on page 61.

5.4 Evaluating OES 2 Software

This section walks you through the OES 2 software evaluation process and discusses the following topics:

- Section 5.4.1, "Understanding OES 2 Software Evaluation Basics," on page 57
- Section 5.4.2, "Downloading OES 2 SP3 Software from the Novell Web Site," on page 57
- Section 5.4.3, "Preparing the Installation Media," on page 58
- Section 5.4.4, "Installing OES 2 for Evaluation Purposes," on page 58
- Section 5.4.5, "Evaluating OES 2," on page 59
- Section 5.4.6, "Installing Purchased Activation Codes after the Evaluation Period Expires," on page 59

5.4.1 Understanding OES 2 Software Evaluation Basics

You can evaluate the full OES 2 product. The evaluation software is the complete, fully functional OES 2 product.

As you install each server, you are required to accept an end user license agreement (EULA). Your rights to evaluate and use the OES 2 product are limited to the rights set forth in the EULA.

Briefly, the evaluation period for OES 2 servers is 60 days. To receive software updates during this time, you must have or create an account with the Customer Center, receive evaluation codes for OES 2 and SLES 10 while downloading the software, and use these codes to register your server. No software updates can be downloaded after the 60-day evaluation period expires until you purchase the product.

5.4.2 Downloading OES 2 SP3 Software from the Novell Web Site

If you already have OES 2 SP3 ISO image files, skip to Section 5.4.3, "Preparing the Installation Media," on page 58.

If you have OES 2 SP3 product media (CDs and DVDs), skip to Section 5.4.4, "Installing OES 2 for Evaluation Purposes," on page 58.

To download ISO image files from the Web:

1. If you don't already have a Novell account, register for one on the Web (https://secure-www.novell.com/selfreg/jsp/createAccount.jsp?).
2. Access the Novell Downloads Web page (http://download.novell.com).
3. Do a keyword search for *Open Enterprise Server SP3*, then click the *Open Enterprise Server SP3 e-Media Kit* link.
4. Click the *proceed to download* button (upper right corner of the first table).
5. If you are prompted to log in, type your *Novell Account* > *username* and *password*, then click *login*.
6. Accept the *Export Agreement* (required for first downloads only) and answer the survey questions about your download (optional).
7. Print the download page. You need the listed MD5 verification numbers to verify your downloads.
8. Scroll down to the *Download Instructions* section and click the *Download Instructions* link.
9. Print the Download Instructions page for future reference.
10. Use the information on the Download Instructions page to decide which files you need to download for the platforms you plan to evaluate, then mark them on the MD5 verification list on the page you printed in Step 7.
11. On the download page, start downloading the files you need by clicking the *download* button for each file.
12. If you have purchased OES 2 previously and received purchased OES 2 and SLES 10 activation codes, skip to Step 15.

    Otherwise, in the *Evaluating Open Enterprise Server 2* section, click the *Get Activation Codes* link in the *Novell Open Enterprise Server 2—Linux* paragraph.

    60-day evaluation codes are sent in separate e-mail messages to the e-mail address associated with your Novell account.
13. Access your e-mail account and print the messages or write down the activation codes.

Both the OES 2 and the SLES codes are required for product registration and downloading software updates.

14 Click *Back* to return to the download page.

15 In the download table at the top of the page, click the *Install Instructions* > *View* link at the end of the list of files to download.

Although you might have printed this file earlier, the online version is required for the steps that follow.

16 Scroll past the download decision tables; while you wait for the downloads, read through the brief installation instructions, clicking the links for more information.

17 Verify the integrity of each downloaded file by running an MD5-based checksum utility on it and comparing the values against the list you printed in Step 15.

For example, on a Linux system you can enter the following command:

```
md5sum filename
```

where *filename* is the name of the `.iso` file you are verifying.

For a Windows system, you need to obtain a Windows-compatible MD5-based checksum utility from the Web and follow its usage instructions.

18 (Optional) If you plan to install OES 2 from files on your network, see the instructions in "Setting Up a Network Installation Source" in the *OES 2 SP3: Installation Guide*.

5.4.3 Preparing the Installation Media

IMPORTANT: If you have downloaded `.iso` image files from the Web, it is critical that you verify the integrity of each file as explained in Step 17 on page 58. Failure to verify file integrity can result in failed installations, especially in errors that report missing files.

Instructions for preparing installation media are located in "Setting Up a Network Installation Source" in the *OES 2 SP3: Installation Guide*.

5.4.4 Installing OES 2 for Evaluation Purposes

If you followed the instructions in Section 5.4.2, "Downloading OES 2 SP3 Software from the Novell Web Site," on page 57, you now have two activation/evaluation codes: one for OES 2 and another for SLES 10. As you install OES 2, you should register with the Novell Customer Center and use these codes to enable your server for online updates from the OES 2 and SLES 10 patch channels.

IMPORTANT: Always download the current patches during an installation.

Instructions for using the activation codes during an installation are found in "On the Novell Customer Center Configuration configuration page, select all of the following options, then click Next." in the *OES 2 SP3: Installation Guide*.

The evaluation period begins when the codes are issued. Use the same activation codes for each OES 2 server you install during the evaluation period.

5.4.5 Evaluating OES 2

During the evaluation period, we recommend that you fully explore the many services available in OES 2.

To help you get started with the process, we have prepared a lab guide for OES 2 that explores both OES 2 and virtualized NetWare on a second OES 2 virtual machine host server. The sections in this guide introduce eDirectory, walk you through server installations, and provide brief exercises you can complete to get started using OES 2 Services. After completing the exercises in the guide, you can use the lab setup to further explore OES 2 and learn about its many powerful services.

For more information, see the *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare*.

After working through the lab guide, we recommend that you review all of the information in this guide to gain a comprehensive overview of OES 2 and the planning and implementation processes you will follow to fully leverage its network services.

5.4.6 Installing Purchased Activation Codes after the Evaluation Period Expires

After purchasing Open Enterprise Server, use the instructions in "Registering the Server in the Novell Customer Center (Command Line)" in the *OES 2 SP3: Installation Guide* to enter the purchased activation codes that you received with your purchase. After logging in as `root`, complete the step where you enter the activation codes, replacing the evaluation codes with the purchased codes.

5.5 Licensing

This section explains the following:

- Section 5.5.1, "The OES 2 Licensing Model," on page 59
- Section 5.5.2, "SLES Licensing Entitlements in OES 2," on page 60
- Section 5.5.3, "OES 2 Doesn't Support NLS," on page 60

5.5.1 The OES 2 Licensing Model

The only OES 2 licensing restriction is the number of user connections allowed to use OES 2 services on your network. You are authorized to install as many OES 2 servers as you need to provide OES 2 services to those users.

For example, if your OES 2 license is for 100 user connections, you can install as many OES 2 servers as desired. Up to 100 users can then connect to and use the services provided by those OES 2 servers. When you install OES 2, you must accept an end user license agreement (EULA). Your rights to use the OES 2 product are limited to the rights set forth in the EULA. Violators of the Novell license agreements and intellectual property are prosecuted to the fullest extent of the law.

To report piracy and infringement violations, please call 1-800-PIRATES (800-747-2837) or send e-mail to pirates@novell.com.

For more information on OES 2 licensing, see the OES 2 Licensing page on the Novell Web site (http://www.novell.com/licensing/oes_licensing.html).

5.5.2 SLES Licensing Entitlements in OES 2

SUSE Linux Enterprise Server (SLES) entitlements in OES 2 have changed. For more information, refer to the EULA (http://www.novell.com/licensing/eula/oes/oes_2_english.pdf) on the Web.

After installing OES 2, you can use Novell iManager to install and manage license certificates in your eDirectory tree and to monitor NetWare usage. You can also monitor usage of Novell Licensing Services-enabled products.

5.5.3 OES 2 Doesn’t Support NLS

Novell Licensing Services (NLS) are not available on OES 2, nor does an OES 2 installation require a license/key file pair (`*.nlf` and `*.nfk`). Therefore, in a mixed OES 2 and NetWare eDirectory tree, at least one NetWare server must hold a replica for each partition where there is a NetWare server object. For more information about licensing for NetWare servers in OES trees, see “NetWare Licenses and OES 2 Trees” on page 45.

6 Installing OES 2

IMPORTANT: Before you install Open Enterprise Server 2, be sure to review the information in Chapter 4, “Planning Your OES 2 Implementation,” on page 29, especially Section 4.9, “Caveats to Consider Before You Install,” on page 38.

This section briefly covers the following:

- Section 6.1, “Installing OES 2,” on page 61
- Section 6.2, “Installing OES 2 Servers in a Xen VM,” on page 62

6.1 Installing OES 2

The OES 2 installation leverages the SUSE Linux YaST graphical user interface. You can install OES 2 services on an existing SUSE Linux Enterprise Server 10 server, or you can install both OES 2 and SLES 10 at the same time, making the installation of SLES 10 and OES 2 services a seamless process.

To ensure a successful installation:

1. Read and follow all instructions in the OES 2 Readme (http://www.novell.com/documentation/oes2/oes_readme/data/oes_readme.html#bsen7me).
2. Carefully follow the instructions in the *OES 2 SP3: Installation Guide*, especially those found in
   - “Preparing to Install OES 2 SP3”
   - “Installing OES 2 SP3 as a New Installation”
3. Make sure you always download the latest patches as part of the Customer Center configuration during the install. This ensures the most stable configuration and installation process and prevents some issues that are documented in the product Readme.
4. After updating the server, red text appears under the *CA Management* section, indicating that the CA must be configured before proceeding.

   This happens because the server reboots as part of the upgrade process and the `root` password is no longer in memory.

   Click *CA Management*, type and confirm the `root` password in the indicated fields, then click *Next*. The installation proceeds.
5. During the installation, you have the option to disable each service for later configuration. However, we recommend that you configure all services at install time simply because the process is more streamlined.

   For more information on configuring services later, see “Installing or Configuring OES 2 SP3 on an Existing Server” in the *OES 2 SP3: Installation Guide*.

6.1.1 What's Next

After installing OES 2 and before starting to use your new OES 2 server, be sure to review the information in Chapter 7, "Caveats for Implementing OES 2 Services," on page 63.

The various service sections in this guide contain information about completing your OES 2 services implementation. See the sections for the services you have installed, beginning with Chapter 12, "Managing OES 2," on page 85.

6.2 Installing OES 2 Servers in a Xen VM

Installing OES 2 servers on a Xen virtual machine involves installing an OES 2 SP3 or SUSE Linux Enterprise Server (SLES) 10 SP4 VM host server, creating a VM, and then installing an OES 2 server (NetWare or Linux) in the VM.

To get started with Xen virtualization in OES 2, see the following:

- "Introduction to Xen Virtualization (http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_basics.html)" in the *Virtualization with Xen (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html)*guide.
- "Installing OES as a Xen VM Host Server" in the *OES 2 SP3: Installation Guide*.
- "Installing, Upgrading, or Updating OES on a Xen-based VM" in the *OES 2 SP3: Installation Guide*.
- "Installing and Managing NetWare on a Xen-based VM" in the *OES 2 SP3: Installation Guide*.

7 Caveats for Implementing OES 2 Services

This section presents a few pointers for avoiding common Open Enterprise Server 2 implementation problems.

The list that follows is not comprehensive. Rather, it simply outlines some of the more common problems reported by network administrators. To ensure successful service implementations, you should always follow the instructions in the documentation for the services you are implementing.

7.1 AFP

- Section 7.1.1, "Anti-Virus Solutions and AFP," on page 64

7.1.1 Anti-Virus Solutions and AFP

The Apple Filing Protocol (AFP) support for NSS files on OES 2 SP3 is implemented via a technology that bypasses the real-time scanning employed by most anti-virus solutions for OES.

NSS files shared through an AFP connection can be protected by on-demand scanning on the OES 2 server or by real-time and on-demand scanning on the Apple client.

7.2 Avoiding POSIX and eDirectory Duplications

OES 2 servers can be accessed by

- Local (POSIX) users that are created on the server itself.
- eDirectory users that are given local access through Linux User Manager (LUM).

However, there are some issues you need to consider:

- Section 7.2.1, "The Problem," on page 64
- Section 7.2.2, "Three Examples," on page 64
- Section 7.2.3, "Avoiding Duplication," on page 65

7.2.1 The Problem

There is no cross-checking between POSIX and eDirectory to prevent the creation of users or groups with duplicate names.

When duplicate names occur, the resulting problems are very difficult to troubleshoot because everything on both the eDirectory side and the POSIX side appears to be configured correctly. The most common problem is that LUM-enabled users can't access data and services as expected but other errors could surface as well.

Unless you are aware of the users and groups in both systems, especially those that are system-created, you might easily create an invalid configuration on an OES 2 server.

7.2.2 Three Examples

The following examples illustrate the issue.

- "The shadow Group" on page 65
- "The users Group" on page 65
- "Other Non-System Groups" on page 65

The shadow Group

There is a default system-created group named shadow that is used by certain Web-related services, including the OES 2 QuickFinder server, but it has no relationship with Dynamic Storage Technology (DST) and shadow volumes.

Because shadow is a local POSIX group, there is nothing to prevent you from creating a LUM-enabled second group in eDirectory that is also named shadow. In fact, this could be a logical name choice for many administrators in conjunction with setting up shadow volume access for Samba/CIFS users.

However, using this group name results in LUM-enabled users being denied access by POSIX, which looks first to the local shadow group when determining access rights and only checks eDirectory for a group named shadow if no local group is found.

The users Group

There is another default system-created group named users that is not used by OES 2 services but is nevertheless created on all SLES 10 (and therefore, OES 2) servers.

Creating an eDirectory group named users would seem logical to many administrators. And as with the shadow group, nothing prevents you from using this name.

Unfortunately, having a LUM-enabled eDirectory group named users is not a viable configuration for services requiring POSIX access. The local users group is always checked first, and the LUM-enabled users group in eDirectory won't be seen by POSIX.

NOTE: Do not confuse eDirectory Group objects with Organizational Unit (OU) container objects.

Creating an OU container in eDirectory named users is a valid option and does not create conflicts with POSIX.

Other Non-System Groups

Conflicts between group and user names also occur when administrators create local and eDirectory groups with the same name.

For example, one administrator creates a group named myusers on the local system and another creates a LUM-enabled group in eDirectory with the same name. Again, the LUM-enabled users who are members of the eDirectory group won't have access through POSIX.

This is why we recommend that, as a general rule, administrators should not create local users or groups on OES 2 servers. You should only make exceptions when you have determined that using LUM-enabled users and groups is not a viable option and that objects with the same names as the POSIX users and groups will not be created in eDirectory in the future.

7.2.3 Avoiding Duplication

Having duplicate users and groups is easily avoided by following these guidelines:

- "Use YaST to List All System-Created Users and Groups" on page 66
- "Create Only eDirectory Users and Groups" on page 66

Use YaST to List All System-Created Users and Groups

We recommend that you use the YaST Group Management/User Management module to check for names you might duplicate by mistake.

1. Open the YaST Control Center.
2. Click either *Group Management* or *User Management*.
3. Click *Set Filter* > *Customize Filter*.
4. Select both options (*Local* and *System*), then click *OK*.

   All users or groups as displayed, including those that exist only in eDirectory and are LUM-enabled.
5. To avoid duplication, keep this list in mind as you create eDirectory users and groups.

NOTE: The list of users and groups in Appendix I, "System User and Group Management in OES 2 SP3," on page 269 is not exhaustive. For example, the users group is not listed.

Create Only eDirectory Users and Groups

For OES 2 services, the LUM technology eliminates the need for local users and groups. We recommend, therefore, that you avoid the problems discussed in this section by not creating local users and groups.

7.3 CIFS

- Section 7.3.1, "Changing the Server IP Address," on page 66

7.3.1 Changing the Server IP Address

Reconfiguring CIFS in YaST might not take effect if the server IP address was changed on the server but not in the OES LDAP server configuration.

To work around this:

1. Reconfigure the LDAP server IP address with the IP address changes.
2. Then change the CIFS IP address configuration.

7.4 ConsoleOne Can Cause JClient Errors

ConsoleOne support is now limited to management of GroupWise and ZENworks for Desktops 7.

If you need to use ConsoleOne to manage either of these supported products on OES 2, make sure you have installed version 1.3.6h or later.

Earlier versions of ConsoleOne cause JClient errors in iManager.

7.5 CUPS on OES 2

iPrint is the print solution for OES 2 and offers more robust and scalable print services than a CUPS installation can. iPrint actually uses CUPS to render print jobs prior to sending them to the printer, but for scalability and performance, printing from the server itself is disabled during iPrint installation.

If you plan to use iPrint, deselect *Print Server* in the *Primary Functions* category during the install and don't configure CUPS on the OES 2 server.

7.6 DSfW: MMC Password Management Limitation

After creating a user, you cannot then force a password change through the Microsoft Management Console (MMC) because the *User must change password at next logon* option is disabled. You can work around this issue while creating the user by selecting the option as part of the creation task. For existing users, you can reset the password and select the same option as part of the reset task.

7.7 eDirectory

- Section 7.7.1, "Avoid Uninstalling eDirectory," on page 67
- Section 7.7.2, "Avoid Renaming Trees and Containers," on page 67
- Section 7.7.3, "Default Static Cache Limit Might Be Inadequate," on page 68
- Section 7.7.4, "eDirectory Not Restarting Automatically," on page 68
- Section 7.7.5, "One Instance Only," on page 68
- Section 7.7.6, "Special Characters in Usernames and Passwords," on page 68

7.7.1 Avoid Uninstalling eDirectory

OES services are tightly integrated with eDirectory and do not function without it.

Although the eDirectory 8.8 documentation describes how to remove and reinstall eDirectory, the processes described do not cleanly decouple OES services, nor do they restore service connections. As a result, not only does uninstalling eDirectory break OES services, reinstalling eDirectory does not restore them.

If you have an issue that you believe can only be resolved by uninstalling eDirectory, make sure you consult with Novell Technical Services before you attempt to do so.

7.7.2 Avoid Renaming Trees and Containers

The configuration files for many OES services point to configuration data stored within eDirectory.

Although eDirectory tracks all changes internally, OES services do not. Therefore, if you rename your eDirectory tree or one of the containers below [Root], you should expect that one or more of your OES services will break.

If you need to rename a container or tree, make sure that you

1. Identify all of the configuration files for your OES services.

2. Assess whether the changes that you are planning impact any of your service configurations.
3. Understand and articulate the changes that are required to restore your services after renaming.

There are no automated tools in OES for resolving the configuration errors and other problems that are caused by renaming a tree or its containers.

7.7.3 Default Static Cache Limit Might Be Inadequate

The eDirectory install in OES 2 SP3 sets a default static cache of 200 MB if an `_ndsdb.ini` file is not present in the `dib` directory.

To improve performance, you can adjust the cache parameter in the `_ndsdb.ini` file after the install to meet your eDirectory performance requirements, depending on the database size and available system RAM. We recommend setting the cache to 200 MB on a 2 GB RAM system and 512 MB on 4 GB RAM system.

7.7.4 eDirectory Not Restarting Automatically

After a system crash or power failure, eDirectory services (ndsd) might not automatically restart in some situations. To start eDirectory again, do the following:

1. Delete the `/var/opt/novell/eDirectory/data/ndsd.pid` file.
2. At a terminal prompt, enter `/etc/init.d/ndsd start`.

7.7.5 One Instance Only

OES 2 supports only one instance of eDirectory (meaning one tree instance) per server.

If you need two or more instances running on a single server, you must install them on a non-OES server, such as SLES 10.

7.7.6 Special Characters in Usernames and Passwords

Using special characters in usernames and passwords can create problems when the values are passed during an eDirectory installation or schema extension.

If the username or password contains special characters, such as $, #, and so on, escape the character by preceding it with a backslash (\). For example, an administrator username of

```
cn=admin$name.o=container
```

must be passed as

```
cn=admin\$name.o=container
```

When entering parameter values at the command line, you can either escape the character or place single quotes around the value. For example:

```
cn=admin\$name.o=container
```

or

```
'cn=admin$name.o=container'
```

7.8 iFolder 3.8

Implementation caveats for iFolder 3.8 are documented in "Caveats for Implementing iFolder Services" in the *Novell iFolder 3.8.4 Administration Guide*.

7.9 iPrint

iPrint has the following implementation caveats:

- Section 7.9.1, "Cluster Failover Between Mixed Platforms Not Supported," on page 69
- Section 7.9.2, "Printer Driver Uploading on OES 2 Might Require a CUPS Administrator Credential," on page 69
- Section 7.9.3, "Printer Driver Uploading Support," on page 69
- Section 7.9.4, "iManager Plug-Ins Are Platform-Specific," on page 69
- Section 7.9.5, "iPrint Client for Linux Doesn't Install Automatically," on page 70
- Section 7.9.6, "iPrint Disables CUPS Printing on the OES 2 Server," on page 70

7.9.1 Cluster Failover Between Mixed Platforms Not Supported

Clustered iPrint services can only fail over to the same platform, either OES 2 or NetWare.

7.9.2 Printer Driver Uploading on OES 2 Might Require a CUPS Administrator Credential

A PPD is the Linux equivalent of a printer driver on Windows.

There are two versions of the iPrint Client: high security and low security. By default, end users and administrators install the high-security client when using the iPrint Printer List Web page.

This means that administrators are prompted for a CUPS administrator credential when uploading PPDs. However, the prompt doesn't specify that a CUPS administrator credential is needed and the `root` user credential does not work.

7.9.3 Printer Driver Uploading Support

Uploading PPD printer drivers from a Linux workstation requires a Mozilla-based browser. Only the *Add From System* button works for uploading drivers. Non-Mozilla-based browsers, such as Konqueror, cannot be used to upload drivers.

Uploading PPD printer drivers from a Windows workstation requires Internet Explorer 5.5 or later. Other browsers running on Windows do not work for uploading drivers.

Windows printer drivers cannot be uploaded by using Mozilla-based or other browsers on any platform.

7.9.4 iManager Plug-Ins Are Platform-Specific

The iManager plug-ins are different for each server platform. Therefore, if you have both OES 2 and NetWare 6.5 SP8 servers running iPrint services, you need two instances of iManager to manage iPrint—one on each platform.

7.9.5 iPrint Client for Linux Doesn't Install Automatically

Users who are used to installing the Windows iPrint Client expect to choose an *Open* option and have the client install automatically. However, installing the client on Linux workstations requires you to save the RPM package and then install it manually if a package manager is not already installed and configured as it is in the Novell Linux Desktop. For more information, see "Linux: iPrint Client" in the *OES 2 SP3: iPrint for Linux Administration Guide*.

7.9.6 iPrint Disables CUPS Printing on the OES 2 Server

iPrint uses CUPS to render print jobs before sending the print job to the Print Manager. For performance and scalability, printing from the server itself is disabled during the OES installation of iPrint.

7.10 LDAP—Preventing "Bad XML" Errors

If you are using Novell eDirectory 8.7.3x, time outs are possible when you search from iManager for eDirectory objects, such as NCP Server objects, Volume objects, and Cluster objects. This is because the Object Class attribute is not indexed by default. The LDAP sub-tree search can take over 30 seconds, which causes the query to time out. For example, a Cluster objects search from the Cluster Options page returns the error:

```
Bad XML found during parsing when accessing cluster options
```

We recommend that you create a value index on the objects' Object Class attribute. (Object Class is considered an attribute for indexing purposes.) This helps to reduce the time needed for the subtree search from over 30 seconds to 10 to 50 milliseconds. For instructions, see "Creating an Index" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

Building indexes speeds up the subtree search, even if some partitions being searched do not contain these types of objects. For example, searching for a Cluster object in a context that contains only users is not expected to return results; however, the Object Class search is still performed, and benefits from having an index present.

The subtree search performance issue is resolved in the eDirectory 8.8.x release with the addition of the AncestorID feature.

7.11 LUM Cache Refresh No Longer Persistent

In reponse to customer requests for improved LDAP performance, persistent searching for new Linux-enabled users and groups has been disabled in OES 2 SP3. This means that when a user or group is enabled for Linux access, it is not immediately listed in some of the interfaces, such as the GUI file browser.

For most installations this is not an issue. However, persistent searching can be turned on by editing the `/etc/nam.conf` file and changing the `persistent-search` parameter from `no` to `yes`.

Alternatively, you can shorten the LUM cache refresh period (default is 8 hours). You can adjust the refresh period by editing the `persistent-cache-refresh-period` parameter in the `/etc/nam.conf` file and restarting LUM using the `rcnamcd restart` command.

You can also refresh the cache immediately by using the `namconfig cache_refresh` command.

For more information, see “What’s New” in the *OES 2 SP3: Novell Linux User Management Administration Guide*.

7.12 Management

- Section 7.12.1, “iManager RBS Configuration with OES 2,” on page 71
- Section 7.12.2, “Storage Error in iManager When Accessing a Virtual Server,” on page 72
- Section 7.12.3, “Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt,” on page 72

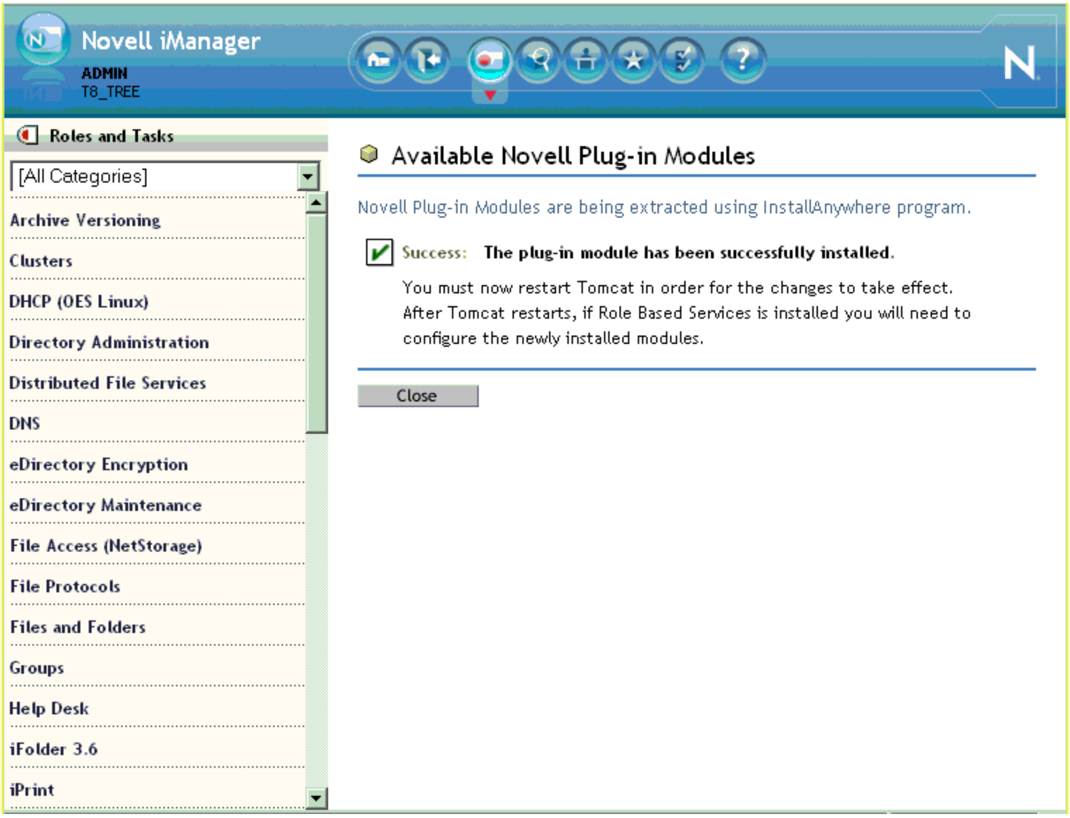
7.12.1 iManager RBS Configuration with OES 2

In “Installing RBS” in the *Novell iManager 2.7.6 Administration Guide*, you are instructed to run the iManager Configuration Wizard before using iManager.

When iManager is installed in connection with OES 2, various roles and tasks are configured, as shown in Figure 7-1.

These roles and tasks are available to all the users you create until you run the configuration wizard. After that, the roles and tasks are available only to the Admin user and other users or groups you specifically designate.

Figure 7-1 *iManager Roles and Tasks*



Available Novell Plug-in Modules

Novell Plug-in Modules are being extracted using InstallAnywhere program.

☑ Success: **The plug-in module has been successfully installed.**

You must now restart Tomcat in order for the changes to take effect. After Tomcat restarts, if Role Based Services is installed you will need to configure the newly installed modules.

For more information on iManager, see the *Novell iManager 2.7.6 Administration Guide*.

7.12.2 Storage Error in iManager When Accessing a Virtual Server

iManager returns a `Storage Error` when you access the Authentication tab for a virtual server object. This is working as designed.

7.12.3 Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt

Use the actual filenames instead of names such as `filena~1.txt` during file operations from the command prompt.

7.13 NCP Doesn’t Equal NSS File Attribute Support

NSS file attributes and NCP services tend to get mixed together in the minds of NetWare administrators. It is important to remember that file and directory attributes are supported and enforced by the file system that underlies an NCP volume, not by the NCP server.

For example, even though the Rename Inhibit attribute appears to be settable in the NCP client interface, if the underlying file system is Linux POSIX (Reiser, Ext3, or XFS) there is no support for the attribute and it cannot be set.

Salvage (undelete) and Purge are other features that are available only on NSS and only where the Salvage attribute has been set (the NSS default). They can be managed in the NCP client and through NetStorage, but they are not available on NCP volumes where the underlying file system is Linux POSIX.

Some administrators assume they can provide NSS attribute support by copying or migrating files, directories, and metadata from an NSS volume to a defined NCP volume on a Linux POSIX partition. However, this doesn’t work, because NSS file attributes are only supported on NSS volumes.

7.14 Novell-tomcat Is for OES Use Only

The `novell-tomcat` package is installed for Novell service use only. It is an embedded part of Novell services, not a generic application platform.

If you want to deploy a Web application on Tomcat on an OES server, install and use the Tomcat package that comes with SLES 10, not the `novell-tomcat` package.

7.15 NSS (OES 2)

- Section 7.15.1, “Understanding Name Space Support,” on page 73
- Section 7.15.2, “The Role of EVMS,” on page 73

7.15.1 Understanding Name Space Support

NSS stores LONG, UNIX, DOS, and AFP name spaces for all files. The default name space sets which name space will be exposed.

In OES 2 the LONG name space was made the default to help performance of NCP, CIFS, and Samba file services. If your primary use is for GroupWise, we recommend changing the default name space to UNIX.

7.15.2 The Role of EVMS

EVMS is the only supported volume manager for NSS volumes on OES 2.

Although some administrators have successfully created NSS volumes on hard disks managed by non-EVMS volume managers, there are serious management and configuration limitations associated with this unsupported implementation. For more information, see "Using NSS on Devices Managed by Non-EVMS Volume Managers " in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

NOTE: EVMS support is automatic and requires no manual configuration unless NSS is being installed on the device that contains the boot (`/boot`) and root (`/`) partitions (the system device). In that case only you must follow the instructions in "Installing with EVMS as the Volume Manager of the System Device" in the *OES 2 SP3: Installation Guide*.

7.16 OpenLDAP on OES 2

You cannot run OpenLDAP on an OES 2 server with eDirectory installed. eDirectory LDAP is required for OES 2 services and uses the same ports as OpenLDAP.

7.17 Samba

For Samba implementation caveats, see "Samba Caveats" in the *OES2 SP3: Samba Administration Guide*.

7.18 Virtualization Issues

The following are caveats for setting up OES 2 server in Xen VMs:

7.18.1 Always Close Virtual Machine Manager When Not in Use

You should always close Virtual Machine Manager (VMM) when you are not actively using it. Virtual Machines are not affected.

Leaving VMM open can affect the system resources available to the VMs.

7.18.2 Always Use Timesync Rather Than NTP

Time synchronization problems have been observed when virtualized NetWare servers are running the XNTPD NLM. Therefore, Novell strongly recommends using Timesync and also configuring the service to communicate through NTP.

7.18.3 Backing Up a Xen Virtual Machine

When backing up a Xen virtual machine running virtualized NetWare, we recommend using a remote backup source rather than a local tape device because of limitations in detecting a local tape device.

7.18.4 Time Synchronization and Virtualized OES 2

eDirectory relies on time being synchronized and connections with eDirectory are lost if the system time varies in the host operating system. Be sure you understand and follow the instructions in Virtual Machine Clock Settings (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/sec_guest_suse.html#sec_xen_time) in the "Virtual Machine Clock Settings" (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html) guide.

7.18.5 NSS Considerations

Make sure you follow these guidelines for using NSS volumes in connection with OES 2 servers running in Xen VMs:

- **Both Linux and NetWare Platforms:** NSS pools and volumes must be created on only SCSI or Fibre Channel devices. You cannot use a file-based disk image, LVM-based disk image, or an SATA/IDE disk for the virtual machine.
- **OES 2:** Data shredding is not supported.

8 Upgrading to OES 2

This section provides information and links for upgrading to Open Enterprise Server.

- Section 8.1, "Caveats to Consider Before Upgrading," on page 75
- Section 8.2, "OES 2 SP3 Upgrade Paths," on page 76
- Section 8.3, "NetWare 6.5 SP8 Upgrade Paths," on page 76

8.1 Caveats to Consider Before Upgrading

Be aware of the following caveats when upgrading an OES server:

- Section 8.1.1, "About Previously Installed Packages (RPMs)," on page 75
- Section 8.1.2, "iManager 2.5 Replaced by iManager 2.7 on NetWare," on page 75
- Section 8.1.3, "OES 1 Linux to OES 2 Service Differences," on page 75
- Section 8.1.4, "Only One eDirectory Instance Is Supported on OES Servers," on page 76

8.1.1 About Previously Installed Packages (RPMs)

Other Novell products, such as GroupWise, and third-party applications that you have installed are treated differently by default when you upgrade an OES server, depending on the version of the server you are upgrading:

- **OES 1:** Applications are deleted by default during an upgrade.
- **OES 2:** Applications installed on an OES 2 server are retained, but might not work after upgrading.

To learn more and for instructions on manually changing these options, see "Planning for the Upgrade to OES 2 SP3" in the *OES 2 SP3: Installation Guide*.

8.1.2 iManager 2.5 Replaced by iManager 2.7 on NetWare

If iManager 2.5 is installed on a NetWare server, and you upgrade it to NetWare 6.5 SP8, iManager and its associated plug-ins are automatically updated to version 2.7. For more information about iManager 2.7, see the *Novell iManager 2.7.6 Administration Guide*.

If you are using iManager 2.02, iManager is not upgraded.

8.1.3 OES 1 Linux to OES 2 Service Differences

eGuide, Novell iFolder 2, and Virtual Office are not supported on OES 2. If you upgrade an OES 1 Linux server with any of these installed to OES 2 SP3, the services cease to function.

8.1.4 Only One eDirectory Instance Is Supported on OES Servers

If your OES server has multiple instances of eDirectory running (multiple trees), any attempt to upgrade the server fails.

You must remove all instances, except the one that uses port 524, prior to an upgrade.

For more information, see Section 7.7.5, “One Instance Only,” on page 68.

8.2 OES 2 SP3 Upgrade Paths

The following are supported upgrade paths for OES 2 SP3:

Table 8-1 *Supported OES 2 SP3 Upgrade Paths*

Source	Destination
OES 1 SP2 (32-bit)	OES 2 SP3 (32-bit)
OES 2 SP2 (32-bit)	OES 2 SP3 (32-bit)
OES 2 SP2 (64-bit)	OES 2 SP3 (64-bit)

NOTE: Physical installations cannot be upgraded to virtual installations, and the reverse is also true. Only physical to physical and virtual to virtual upgrades are supported.

For complete upgrade instructions, see “Upgrading to OES 2 SP3” in the *OES 2 SP3: Installation Guide*.

In addition to upgrading the server itself, data and service migrations from OES 1 to OES 2 are also supported. For more information, see the *OES 2 SP3: Migration Tool Administration Guide*.

8.3 NetWare 6.5 SP8 Upgrade Paths

For help upgrading from NetWare to OES 2, see the *OES 2 SP3: Upgrading to OES—Best Practices Guide*.

9 Migrating and Consolidating Existing Servers and Data

This section briefly outlines the following migration topics:

- Section 9.1, “Supported OES 2 SP3 Migration Paths,” on page 77
- Section 9.2, “Migration Tools and Purposes,” on page 77

9.1 Supported OES 2 SP3 Migration Paths

For a complete list of Open Enterprise Server SP3 migration scenarios and paths, see “Migration Scenarios” in the *OES 2 SP3: Migration Tool Administration Guide*.

9.2 Migration Tools and Purposes

The following sections briefly explain the migration tools included in OES 2 SP3:

- Section 9.2.1, “OES 2 SP3 Migration Tool,” on page 77
- Section 9.2.2, “Migrate Windows Shares Utility,” on page 77

9.2.1 OES 2 SP3 Migration Tool

The OES 2 SP3 Migration Tool lets you migrate and/or consolidate data and services from one or more NetWare, OES 1, or OES 2 source servers to an OES 2 SP3 target server. The source servers must each be running the same platform. Cross-platform consolidations are not directly supported, but can be facilitated as explained in “Cross-Platform Data Consolidations” in the *OES 2 SP3: Migration Tool Administration Guide*.

You can also transfer a complete server identity, including its IP address, hostname, eDirectory identity, NICI keys, and certificates. For more information, see “Transfer ID ” in the *OES 2 SP3: Migration Tool Administration Guide*.

9.2.2 Migrate Windows Shares Utility

OES 2 SP3 includes the Migrate Windows Shares utility to help you migrate data from Windows NT, 2000, or 2003 servers to OES 2 SP3.

For more information, see “Migrating Data from Windows to OES 2 SP3 Linux” in the *OES 2 SP3: Migration Tool Administration Guide*.

10 Virtualization in OES 2

In Open Enterprise Server 2, you can host multiple OES 2 and NetWare servers on Xen virtual machines (VMs) on a single Xen host server.

For information about installing and running OES 2 services on Xen-based virtual machines, see the links on the Virtualization page of the OES 2 Online Documentation (http://www.novell.com/documentation/oes2/virtualization.html).

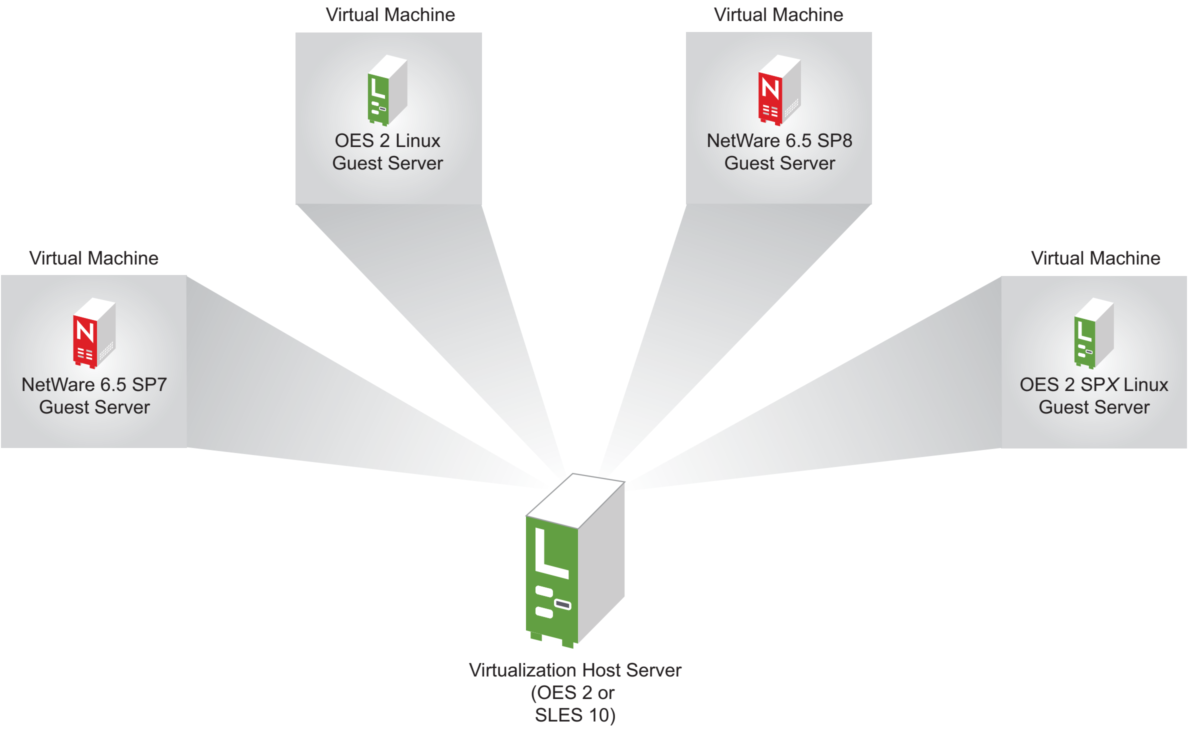
- Section 10.1, "Graphical Overview of Virtualization in OES 2," on page 79
- Section 10.2, "Why Install OES Services on Your VM Host?," on page 80
- Section 10.3, "Services Supported on VM Hosts and Guests," on page 80

IMPORTANT: Support for Xen virtualization of NetWare 6.5 SP7 and later is an OES 2 product feature and is available only to OES 2 registered customers.

10.1 Graphical Overview of Virtualization in OES 2

Figure 10-1 illustrates how a single VM host server can support multiple VM guest servers that in turn provide OES services.

Figure 10-1 *Xen-Based Virtualization in OES 2*


Virtual Machine
OES 2 Linux Guest Server
Virtual Machine
NetWare 6.5 SP8 Guest Server
Virtual Machine
NetWare 6.5 SP7 Guest Server
Virtual Machine
OES 2 SP*X* Linux Guest Server
Virtualization Host Server (OES 2 or SLES 10)

10.2 Why Install OES Services on Your VM Host?

Novell supports three OES 2 services running on a Xen VM host server: Novell Linux User Management, Novell Storage Management Services, and Novell Cluster Services. Additionally, whenever you specify OES 2 as an add-on product, the YaST-based NetWare Response File Utility is automatically installed, whether you install any OES 2 services or not.

Having these components installed on a Xen VM host server provides the following benefits:

- **Linux User Management (LUM):** Lets you SSH into the server for management purposes by using an eDirectory user account.

  This functionality requires that you

  - Enable SSH communications through any firewalls that are running on the server
  - Configure LUM to allow SSH as a LUM-enabled service. For more information see "Section 12.4.2, "Setting Up SSH Access for LUM-enabled eDirectory Users," on page 97."
- **Storage Management Services (SMS):** Lets you back up the VM host server and all of the VM guests.
- **Novell Cluster Services (NCS):** Lets you cluster the VM guests running on the VM host.
- **NetWare Response File Utility:** Lets you pre-answer the same questions as you would during a physical NetWare installation. When the time comes to run the NetWare Install program, the installation reads your responses from the file and proceeds without requiring further intervention.

10.3 Services Supported on VM Hosts and Guests

As you plan your virtualization configurations, you will want to consider which services are supported where Table 10-1 and which combinations of services are supported (see Section 4.9.18, "Unsupported Service Combinations," on page 47).

Table 10-1 *Services Supported on VM Hosts and Guests*

OES 2 Service	Linux VM Host	Linux VM Guest	NetWare VM Guest
AFP (Novell AFP)		✓	✓
Backup/SMS	✓	✓	✓
CIFS (Novell CIFS)		✓	✓
Cluster Services	✓ (non-NSS and Xen templates only)	✓	✓
DHCP		✓	✓
DNS		✓	✓
Domain Services for Windows (DSfW)		✓	
eDirectory		✓	✓

OES 2 Service	Linux VM Host	Linux VM Guest	NetWare VM Guest
FTP		✓	✓
Novell iFolder		✓ (3.7)	✓ (2.1x)
iManager		✓	✓
iPrint		✓	✓
Linux User Management	✓	✓	
NCP Server/Dynamic Storage Technology		✓	
NetStorage		✓	✓
Novell Remote Manager (NRM)		✓	✓
Novell Storage Services (NSS)		✓	✓
QuickFinder		✓	✓
Samba		✓	

IMPORTANT: Adding OES services to a Xen VM host requires that you boot the server with the regular kernel prior to adding the services. See the instructions in the Important note in "Adding/Configuring OES Services on an Existing Server" in the *OES 2 SP3: Installation Guide*.

11 Clustering and High Availability

Open Enterprise Server 2 includes support for a two-node Novell Cluster Services cluster.

The full Novell Cluster Services product (available through a separate purchase) is a multinode clustering product that

- Can include up to 32 servers.
- Is supported for Linux.
- Is eDirectory enabled for single-point ease of management.
- Supports failover, failback, and migration (load balancing) of individually managed cluster resources.
- Supports shared SCSI, iSCSI, and Fibre Channel storage area networks.

For more information, see the topics in "clustering (high availability) (http://www.novell.com/documentation/oes2/cluster-services.html#cluster-services)" in the OES 2 online documentation.

12 Managing OES 2

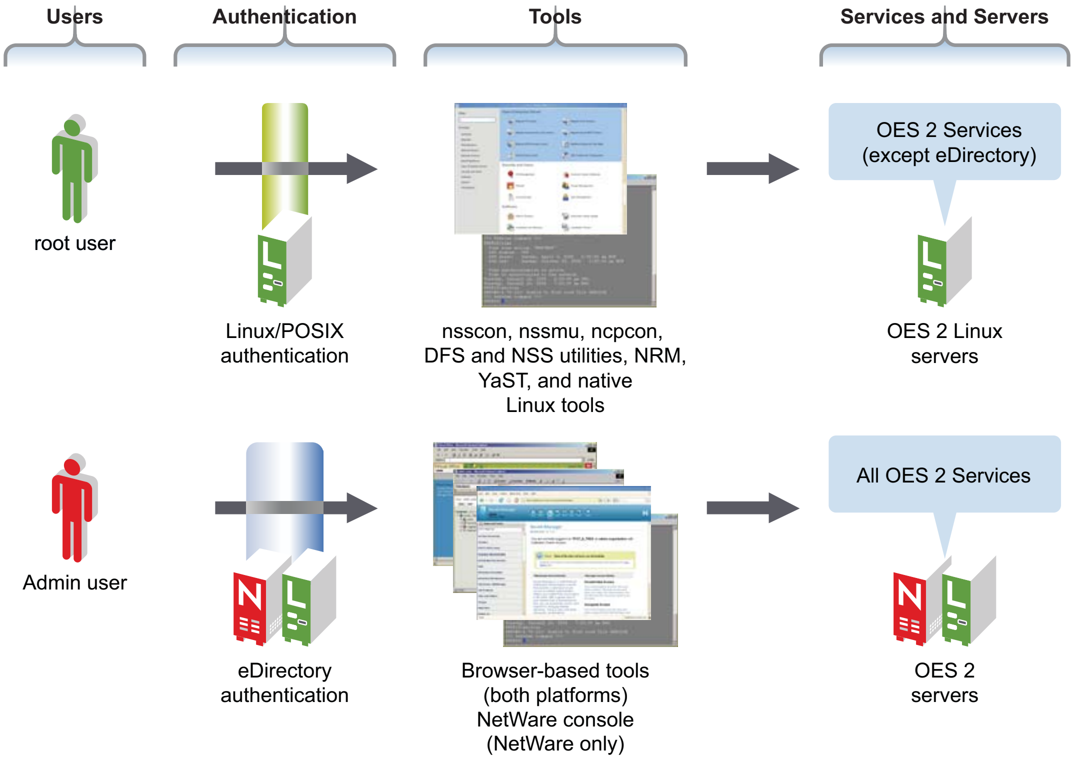
This section includes the following topics:

12.1 Overview of Management Interfaces and Services

As shown in Figure 12-1, Open Enterprise Server provides a rich set of service-management and server-management tools, including browser-based and server-based interfaces that help you implement and maintain your network. Access to most of these management interfaces is controlled through eDirectory. However, a few interfaces, such as YaST on SUSE Linux Enterprise Server 10 servers, require local authentication.

For more information, see Section 12.3, "OES Utilities and Tools," on page 87.

Figure 12-1 *Management Interfaces and Services*

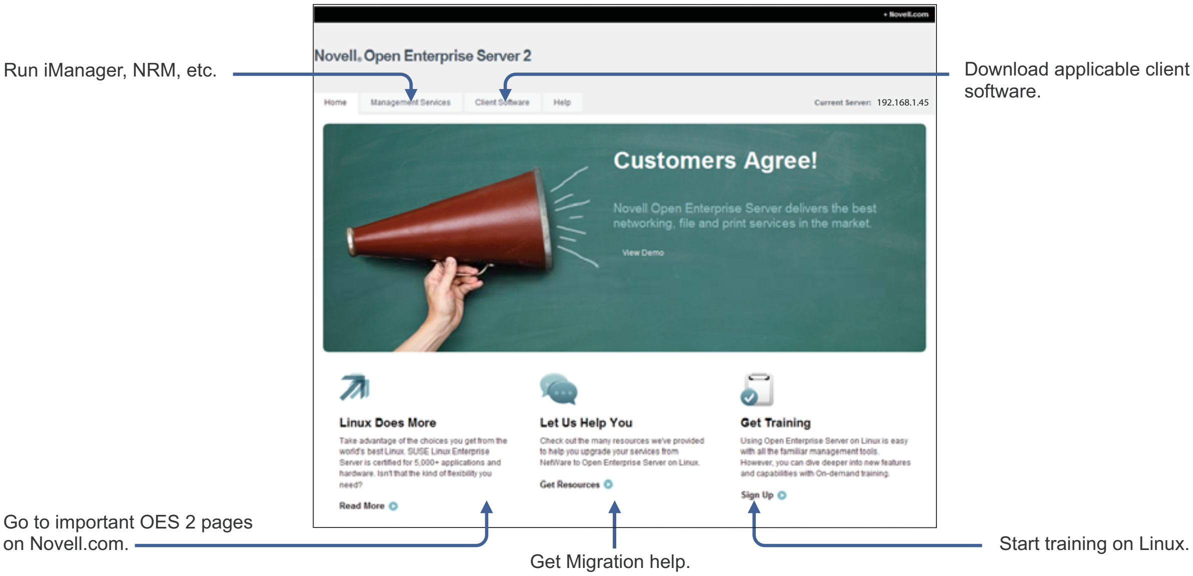


Users
Authentication
Tools
Services and Servers
root user
Linux/POSIX authentication
nsscon, nssmu, ncpcon, DFS and NSS utilities, NRM, YaST, and native Linux tools
OES 2 Services (except eDirectory)
OES 2 Linux servers
Admin user
eDirectory authentication
Browser-based tools (both platforms) NetWare console (NetWare only)
All OES 2 Services
OES 2 servers

12.2 Using OES 2 Welcome Pages

After you install an OES 2 server, anyone with browser access to the server can access its Welcome Web site, which is a collection of dynamic Web pages that provides the features illustrated and explained in Figure 12-2.

Figure 12-2 *The Default OES Welcome Page*



Customers Agree!

Novell Open Enterprise Server delivers the best networking, file and print services in the market.

Linux Does More

Take advantage of the choices you get from the world's best Linux. SUSE Linux Enterprise Server is certified for 5,000+ applications and hardware. Isn't that the kind of flexibility you need?

Let Us Help You

Check out the many resources we've provided to help you upgrade your services from NetWare to Open Enterprise Server on Linux.

Get Training

Using Open Enterprise Server on Linux is easy with all the familiar management tools. However, you can dive deeper into new features and capabilities with On-demand training.

Run iManager, NRM, etc.

Download applicable client software.

Go to important OES 2 pages on Novell.com.

Get Migration help.

Start training on Linux.

This section explains OES Welcome Web Site features, and discusses:

- Section 12.2.1, "The Welcome Site Requires JavaScript, Apache, and Tomcat," on page 86
- Section 12.2.2, "Accessing the Welcome Web Site," on page 87
- Section 12.2.3, "The Welcome Web Site Is Available to All Users," on page 87
- Section 12.2.4, "Administrative Access from the Welcome Web Site," on page 87

12.2.1 The Welcome Site Requires JavaScript, Apache, and Tomcat

Browsers accessing the Welcome site must have JavaScript enabled to function correctly.

Additionally, it is possible to install OES 2 on either supported platform without including the Apache Web Server or the Tomcat Servlet Container. For example, the Apache server and Tomcat container are included with many of the OES 2 server patterns, but not all of them.

If you are unable to access the Welcome Web site, your server is probably missing one or both of these required components. To make the site available, you need to add the components to the OES 2 server.

12.2.2 Accessing the Welcome Web Site

Anyone with browser access to an OES 2 server can access the Welcome site by doing the following:

1 Open a supported Web browser that has a TCP connection to the network where the OES 2 server is installed.

2 Enter the URL to the server, using HTTP.

For example:

```
http://server.example.com/welcome
```

or

```
http://192.168.1.206/welcome
```

IMPORTANT: By default, the Welcome site is accessible by entering only the DNS name or IP address without the path to /welcome as the URL. However, this behavior changes as follows:

- On NetWare, the `sys:/apache2/htdocs/index.html` file redirects requests to the Welcome site page. If the file is changed, then the behavior reflects the changes made.
- On Linux, the Welcome site displays only when there is no `index.html` file in `/srv/www/htdocs`. For example, installing the Web and LAMP Server pattern installs a page that says “It Works!” and the Welcome site is not displayed.

If the Welcome page disappears, include /welcome in the access URL.

For additional information, see “Verifying That the Installation Was Successful” in the *OES 2 SP3: Installation Guide*.

12.2.3 The Welcome Web Site Is Available to All Users

Although the Welcome Web site is designed primarily for administrators, it can also be accessed and used by end users. For example, if iPrint is installed on the server, users can install the iPrint Client by clicking the *Client Software* link and selecting the appropriate client.

12.2.4 Administrative Access from the Welcome Web Site

Administrators can access any of the administrative tools installed on the server by clicking the Management Services link, selecting the tool they want to use, and entering the required authentication information.

12.3 OES Utilities and Tools

TIP: NetWare administrators who are new to Linux will also be interested in “OES2 SP3: Linux Tips for NetWare Administrators,” a reference that outlines the OES equivalents for most of the familiar CLI tools on NetWare.

Novell OES 2 includes several administration utilities that let you manage everything in your network, from configuring and managing eDirectory to setting up network services and open source software. This section lists and briefly explains the most common utilities.

Whenever possible, we recommend that all OES management be performed by using browser-based tools. This ensures that all the system commands required to execute various tasks are performed in proper order and that none of them is skipped by mistake.

Table 12-1 is a quick reference for accessing information about the OES management tools. Specific instructions for the tasks listed are located in the administration guides and other documentation for the services that each tool manages.

***Table 12-1** OES Management Tool Quick Reference*

Tool	Tasks	Access Method or URL/ Username	Notes
bash	◆ Manage the Linux server. ◆ Manage many services running on the server.	Access a command prompt on the Linux server.	For more information or help understanding and using bash, search the Web for any of the numerous articles and tutorials on using the shell.
Health Monitoring Services	◆ Monitor the health of OES servers.	1. In a supported Web browser, access Novell Remote Manager by entering http://*IP_Address*:8008 2. Specify the eDirectory Admin username and password, or on Linux you can use the `root` user and password if needed. 3. Click *Health Monitor* under *Diagnose Server*.	Functionality is limited for non-Admin or non-`root` users on both platforms. NRM on Linux doesn't include all the functionality of NRM on NetWare. For more information, see the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*. Health Monitoring Services on OES 2 use a Common Information Model (CIM) provided by the Web-Based Enterprise Management (WBEM) Initiative. For more information on WBEM, visit the DMTF Web site (http://www.dmtf.org/standards/wbem).

Tool	Tasks	Access Method or URL/ Username	Notes
iManager 2.7	◆ Access various other management tools and plug-ins. ◆ Configure OES network services. ◆ Create and manage users, groups, and other objects. ◆ Delegate administration through Role-Based Services (RBS). ◆ Manage eDirectory objects, schema, partitions, and replicas. ◆ Manage OES 2 services ◆ Set up and manage your Novell eDirectory tree.	1. In a supported Web browser, enter the following URL: `http://IP_or_DNS/iManager.html` 2. Specify the eDirectory Admin username and password.	Requires an SSL connection (HTTPS). Both HTTP and HTTPS requests establish the SSL connection. For more information on using iManager, see the *Novell iManager 2.7.6 Administration Guide*. See also iManager Workstation.
iManager Workstation (formerly Mobile iManager)	◆ Manage eDirectory. ◆ Create and manage users, groups, and other objects. ◆ Manage OES 2 services. ◆ Access various other management tools and plug-ins.	On a Linux workstation: 1. At the `bin` directory of the expanded `iMan_25_Mobile_iManager_linux.tar` directory, run `imanager.sh`. 2. Log in, using the eDirectory Admin username, password, and eDirectory tree name. On a Windows workstation: 1. At the `bin` directory of the unzipped `iMan_25_Mobile_iManager_win` directory, run `imanager.bat`. 2. Log in, using the eDirectory Admin username, password, and eDirectory tree name.	Requires an SSL connection (HTTPS). Both HTTP and HTTPS requests establish the SSL connection. For more information on using iManager Workstation, see "Accessing iManager Workstation" in the *Novell iManager 2.7.6 Administration Guide*. See also iManager.

Tool	Tasks	Access Method or URL/ Username	Notes

iMonitor	- Monitor and diagnose all the servers in your eDirectory tree.
	- Examine eDirectory partitions, replicas, and servers.
	- Examine current tasks taking place in the tree.
		1. In a supported Web browser, enter one of the following URLs:
		(On NetWare)
		`http://IP_or_DNS:81/nds`
		(On Linux)
		`https://IP_or_DNS:8030/nds`
		2. Specify the eDirectory Admin username and password.
			iMonitor provides a Web-based alternative to tools such as DSBrowse, DSTrace, DSDiag, and the diagnostic features available in DSRepair.
			Because of this, iMonitor's features are primarily server focused, meaning that they report the health of individual eDirectory agents (running instances of the directory service) rather than the entire eDirectory tree.
			For more information, see "Using Novell iMonitor" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

iPrint Map Designer	- Create a printer map to aid in printer selection/installation. - Edit an existing printer map.	1. In a supported Web browser, enter the following URL: `http://IP_or_DNS/ippdocs/maptool.htm` 2. Specify the eDirectory Admin username and password.	For OES 2 server instructions, see "Setting Up Location-Based Printing" in the *OES 2 SP3: iPrint for Linux Administration Guide*.
NetStorage Web Interface	- Manage file system access. - Manage file system space restrictions. - Salvage and purge deleted files.	Use the NetStorage Web interface.	As an Admin user (or equivalent), you can set directory and user quotas for NSS data volumes. You can also set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. And you can salvage and purge deleted files. For more information, see "Viewing or Modifying Directory and File Attributes and Rights" in the *OES 2 SP3: NetStorage Administration Guide*.

Tool	Tasks	Access Method or URL/ Username	Notes
Novell Client	◆ Manage file system access. ◆ Manage File System Space Restrictions. ◆ Salvage and purge deleted files.	Use the Novell N icon to access these and other tasks.	As an Admin user (or equivalent), you can set directory and user quotas for NSS data volumes. You can also set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. And you can salvage and purge deleted files. For more information, see "Managing File Security and Passwords" in the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*.
Novell iFolder 3.8	◆ Manage various aspects of iFolder 3.8.	1. In iManager 2.7, click *iFolder 3.8* > *Launch iFolder Admin Console*.	For more information on managing iFolder 3.8, see the following in the *Novell iFolder 3.8.4 Administration Guide*: ◆ iFolder Enterprise Server ◆ iFolder Services via Web Admin ◆ iFolder Users ◆ iFolder Web Access Server ◆ Managing iFolders

Tool	Tasks	Access Method or URL/ Username	Notes
Novell Remote Manager (NRM)	- Manage file system access and attributes for the NetWare Traditional File System and the NSS File System on NetWare. - Manage the NCP Server (Linux) - Manage NCP connections to NSS and NCP volumes (Linux) - Manage Dynamic Storage Technology (Linux) - Manage NetWare Traditional File Systems (NetWare). - Manage OES 2 servers from a remote location. - Monitor your server's health. - Change server configurations. - Perform diagnostic and debugging tasks. - View volume inventories (Linux)	1. In a supported Web browser, enter the following URL: `https://` *`IP_or_DNS`*`:8009` 2. Specify either the eDirectory username and password or a Linux (POSIX) username and password.	Functionality is limited for non-Admin or non-root users on both platforms. NRM on Linux doesn't include all the functionality of NRM on NetWare. For more information, see the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.
NSS Management Utility (NSSMU)	- Manage the Novell Storage Services file system.	At a terminal prompt: 1. Load NSSMU by entering `/opt/novell/nss/sbin/nssmu`	NSS Management Utility (NSSMU) is a server console application used to manage the Novell Storage System (NSS) logical file system. The Snapshot function in NSSMU on Linux is not available in NSSMU on NetWare. Use iManager to create snapshots for NetWare or Linux. For more information, see "NSS Management Utility (NSSMU) Quick Reference" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Tool	Tasks	Access Method or URL/ Username	Notes
OpenSSH (client access)	◆ Securely run commands on remote servers. ◆ Securely copy files and directories to and from other servers using SSH utilities.	Connect to the server using your favorite SSH client.	On Linux, OpenSSH is installed by default and is accessed by eDirectory users as a LUM-enabled service. For more information, see Section 12.4, "SSH Services on OES 2," on page 95.
OpenSSH (Linux)	◆ Manage a SLES 10 (OES 2) server by using OpenSSH.	1. Use standard SSH connection and management options.	Requirements: ◆ The firewall must allow for SSH access. ◆ eDirectory users must be enabled for SSH access. For more information, see Section 12.4, "SSH Services on OES 2," on page 95.
OpenWBEM	◆ Perform tasks instrumented by specific providers.	Access `/etc/openwbem`.	For more information, see the *OES 2 SP3: OpenWBEM Services Administration Guide*.
Perl	A programming language developed by Larry Wall that ◆ Runs faster than shell script programs. ◆ Reads and writes binary files. ◆ Processes very large files. ◆ Lets you quickly develop CGI applications.	Install the associated RPM files.	For more information or help understanding and using Perl, search the Web. There are numerous articles and tutorials on using this versatile programming language.

Tool	Tasks	Access Method or URL/ Username	Notes
QuickFinder Server Manager	◆ Create search indexes for any Web site or attached file systems. ◆ Modify the search dialog look-and-feel to match your corporate design.Create full-text indexes of HTML, XML, PDF, Word, OpenOffice.org, and many other document formats. ◆ Configure and maintain your indexes remotely from anywhere on the Net.	1. In a supported Web browser, enter the following URL: `http://IP_or_DNS/qfsearch/admin` 2. Specify the `root` or other user as documented.	Local users and any eDirectory users that are enabled for Linux access (LUM) can be assigned rights to manage QuickFinder. For more information, see the *QuickFinder 5.0 Server Administration Guide.*
Remote Manager			See Novell Remote Manager.
SNMP for eDirectory	Lets you use standard SNMP tools to ◆ Monitor an eDirectory server. ◆ Track the status of eDirectory to verify normal operations. ◆ Spot and react to potential problems when they are detected. ◆ Configure traps and statistics for selective monitoring. ◆ Plot a trend on the access of eDirectory. ◆ Store and analyze historical data that has been obtained through SNMP. ◆ Use the SNMP native master agent on all eDirectory platforms.	1. Configure SNMP for eDirectory as documented for your platform. 2. Access SNMP for eDirectory services using the SNMP management interface of your choice. 3. Specify the eDirectory Admin username and password.	SNMP support is installed with eDirectory. For more information on SNMP for eDirectory, see "SNMP Support for Novell eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

Tool	Tasks	Access Method or URL/ Username	Notes
SUSE Linux Monitoring Utilities	◆ Manage the Linux server and standard Linux services from the command prompt.	Enter the desired command at the command prompt.	For more information, see "System Monitoring Utilities" (http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_util.html) in the *SLES 10 SP4: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html).
YaST (SUSE Linux)	◆ Install OES 2. ◆ Configure the server and standard Linux services. ◆ Install OES components and services.	To access YaST from the GNOME interface, start the YaST Control Center by clicking *Computer > YaST*. To access YaST at a command prompt, enter `yast`.	For more information, see "Installation with YaST" (http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_inst.html) and "System Configuration with YaST" (http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_yast2.html) in the *SLES 10 SP4: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html).

12.4 SSH Services on OES 2

This section documents the following topics:

- Section 12.4.1, "Overview," on page 95
- Section 12.4.2, "Setting Up SSH Access for LUM-enabled eDirectory Users," on page 97

12.4.1 Overview

SSH (http://www.novell.com/company/glossary.html#4187) services on SLES 10 are provided by OpenSSH (http://www.openssh.org), a free version of SSH connectivity tools developed by the OpenBSD Project (http://www.openbsd.org/).

Linux administrators often use SSH to remotely access a server for management purposes, such as executing shell commands, transferring files, etc. Because many OES 2 services can be managed at a command prompt via an SSH session, it is important to understand how SSH access is controlled in OES 2.

This section discusses the following topics:

- "When Is SSH Access Required?" on page 96
- "How SSH Access for eDirectory Users Works" on page 96
- "SSH Security Considerations" on page 97

When Is SSH Access Required?

SSH access is required for the following:

- **SSH administration access for eDirectory users:** For eDirectory users to manage the server through an SSH connection, they must have SSH access as LUM-enabled users (eDirectory users configured for access to Linux services).

  NOTE: The standard Linux `root` user is a local user, not an eDirectory user. The `root` user always has SSH access as long as the firewall allows it.

- **Access to NSS Volume Management in NetStorage:** When an OES 2 server has NSS volumes, eDirectory contains an object named *nssvolumes* that provides management access to the volumes through the File Access (NetStorage) iManager plug-in. Using the plug-in to manage NSS volumes, assign trustee rights, salvage and purge files, etc. requires SSH access to the server.

  Although eDirectory administrators can create Storage Location Objects to the NSS volumes without SSH access, providing that they know the path to the volume on the POSIX file system and other volume information, having SSH access makes administering NSS volumes in NetStorage much easier.

- **Access to any NetStorage Storage Location Objects based on SSH:** The NetStorage server provides Web access to directories and files on other servers (or on itself).

  Typically, either an NCP or a CIFS connection is used for connecting the NetStorage server with storage targets. However, an SSH connection can also be used, and if it is, the users accessing data through the connection must have SSH access to the data on the target servers.

How SSH Access for eDirectory Users Works

For eDirectory users, the following work together to control SSH access:

- **Firewall:** As mentioned, the default firewall configuration on an OES 2 server doesn't allow SSH connections with the server. This restricts the `root` user as well. Therefore, the first requirement for SSH access is configuring the firewall to allow SSH services.
- **Linux User Management (LUM) must allow SSH as a service:** In OES 2, access to SSH and other Linux services is controlled through Linux User Management (LUM), and each service must be explicitly included in the LUM configuration on each server.
- **LUM-enabling:** After SSH is included as a LUM-enabled service on a server, at least one group and its users must be enabled for LUM. Only LUM-enabled eDirectory users can have SSH access.
- **All eDirectory Groups must allow access:** SSH access is inherited from the LUM-enabled groups that a user belongs to, and access is only granted when all of the groups to which a user belongs allow it.

- **The Samba connection:** Users who are enabled for Samba (CIFS) file services are added by default to an OES-created Samba group that:
    - Is LUM-enabled.
    - Doesn't specify SSH as an allowed service.

  Therefore, because SSH access requires that all of a user's groups must all allow access, Samba users are denied SSH access unless
    - The user is removed from the Samba group.

      or
    - The Samba group is modified to allow SSH access for all Samba users.

SSH Security Considerations

Remember that SSH access lets users browse and view most directories and files on a Linux server. Even though users might be prevented from modifying settings or effecting other changes, there are serious security and confidentiality issues to consider before granting SSH access to anyone.

12.4.2 Setting Up SSH Access for LUM-enabled eDirectory Users

If you need to grant SSH access to an eDirectory user, complete the instructions in the following sections in order, as they apply to your situation.

- "Allowing SSH Access Through the Firewall" on page 97
- "Adding SSH as an Allowed Service in LUM" on page 97
- "Enabling Users for LUM" on page 98
- "Restricting SSH Access to Only Certain LUM-Enabled Users" on page 98
- "Providing SSH Access for Samba Users" on page 99

Allowing SSH Access Through the Firewall

1. On the OES 2 server you are granting access to, open the YaST Control Center and click *Security and Users* > *Firewall*.
2. In the left navigation frame, click *Allowed Services*.
3. In the *Allowed Services* drop-down list, select *SSH*.
4. Click *Add* > *Next* > *Accept*.

   The firewall is now configured to allow SSH connections with the server.

Adding SSH as an Allowed Service in LUM

1. If SSH is already an allowed service for Linux User Management on the server, skip to "Enabling Users for LUM" on page 98.

   or

   If SSH is not an allowed service for Linux User Management on the server, continue with Step 2.
2. On the OES 2 server, open the YaST Control Center; then, in the *Open Enterprise Server* group, click *OES Install and Configuration*.
3. Click *Accept*.

4 When the Novell Open Enterprise Server Configuration screen has loaded, click the *Disabled* link under *Linux User Management*.

The option changes to *Enabled* and the configuration settings appear.

5 Click *Linux User Management*.

6 Type the eDirectory Admin password in the appropriate field, then click *OK* > *Next*.

7 In the list of allowed services, click *sshd*.

8 Click *Next* > *Next* > *Finish*.

Each LUM-enabled group in eDirectory, except the system-created Samba group, now shows SSH as an allowed service. The Samba group shows the service as not allowed (or literally speaking, *sshd* is not checked).

Enabling Users for LUM

There are numerous ways to enable users for LUM.

For example, in iManager > *Linux User Management* there are options for enabling users (and choosing a Group in the process) or enabling groups (and enabling users in the process). Linux enabling is part of the process required for Samba access. And finally, there are also command line options.

For specific instructions, refer to "Managing User and Group Objects in eDirectory" in the *OES 2 SP3: Novell Linux User Management Administration Guide*.

After you configure the server's firewall to allow SSH, add SSH as an allowed service, and LUM-enable the eDirectory users you want to have SSH access, if those same users are not also enabled for Samba on the server, they now have SSH access to the server.

On the other hand, if you have installed Samba on the server, or if you install Samba in the future, the users who are configured for Samba access will have SSH access disabled.

To restore access for users impacted by Samba, see "Providing SSH Access for Samba Users" on page 99.

Of course, many network administrators limit SSH access to only those who have administrative responsibilities. They don't want every LUM-enabled user to have SSH access to the server.

If you need to limit SSH access to only certain LUM-enabled users, continue with "Restricting SSH Access to Only Certain LUM-Enabled Users" on page 98.

Restricting SSH Access to Only Certain LUM-Enabled Users

SSH Access is easily restricted for one or more users by making them members of a LUM-enabled group and then disabling SSH access for that group. All other groups assignments that enable SSH access are then overridden.

1 Open iManager in a browser using its access URL:

http://*IP_Address*/iManager.html

where *IP_Address* is the IP address of an OES 2 server with iManager 2.7 installed.

2 In the *Roles and Tasks* list, click *Groups* > *Create Group*.

3 Type a group name, for example NoSSHGroup, and select a context, such as the container where your other Group and User objects are located. Then click *OK*.

4 In the *Roles and Tasks* list, click *Directory Administration* > *Modify Object*.

5. Browse to the group you just created and click *OK*.
6. Click the *Linux Profile* tab.
7. Select the *Enable Linux Profile* option.
8. In the Add UNIX Workstation dialog box, browse to and select the UNIX Workstation objects for the servers you are restricting SSH access to, then click *OK* > *OK*.
9. Click *Apply* > *OK*.
10. In the Roles and Tasks list, click *Modify Object*, browse to the group again, then click *OK*.
11. Click the *Other* sub-tab.
12. In the *Unvalued Attributes* list, select *uamPosixPAMServiceExcludeList*, then click the left-arrow to move the attribute to the *Valued Attributes* list.
13. In the Add Attribute dialog box, click the plus sign (+) next to the empty drop-down list.
14. In the *Add item* field, type `sshd`, then click *OK* > *OK*.
15. Click the *Members* tab.
16. Browse to and select the User objects that shouldn't have SSH access, then click *OK*.
17. Click *Apply* > *OK*.

Providing SSH Access for Samba Users

There are two options for providing SSH access to users who have been enabled for Samba access:

- You can remove the user from the *server_name*-W-SambaUserGroup.

  IMPORTANT: This presupposes that the user is a member of a different LUM-enabled group that also provides access to the server. If the user was enabled for LUM only as part of a Samba configuration, then removing the user from the Samba group breaks access to Samba and the user does not have SSH access.

- You can change access for the entire Samba group by moving the uamPosicPAMServiceExcludeList attribute from the *Valued Attributes* list to the *Unvalued Attributes* list, using the instructions in "Restricting SSH Access to Only Certain LUM-Enabled Users" on page 98 as a general guide.

  NOTE: Although the option to disable SSH access through the *Modify Group* iManager plug-in is much more simple and straightforward, that option is not working as of this writing. Although the plug-in appears to deselect *sshd* as an allowed service, the service is still selected when group information is reloaded. Novell plans to address this issue in the near future.

13 Network Services

Network services as used in this section, are associated with protocols that provide the following:

- Data packet transport on the network.
- Management of IP addresses and DNS names.
- Time synchronization to make sure that all network devices and eDirectory replicas and partitions have the same time.
- Discovery of network devices and services, such as eDirectory, printers, and so on as required by certain applications, clients, and other services.

This section discusses the following:

For links to more information and tasks, see the "Network Protocols (Http://www.novell.com/documentation/oes2/networking-protocols.html)" page in the OES 2 online documentation.

13.1 TCP/IP

Network nodes must support a common protocol in order to exchange packets. Transport protocols establish point-to-point connections so that nodes can send messages to each other and have the packets arrive intact and in the correct order. The transport protocol also specifies how nodes are identified with unique network addresses and how packets are routed to the intended receiver.

Open Enterprise Server 2 includes the standard Linux TCP/IP support on SUSE Linux Enterprise Server 10.

13.1.1 Coexistence and Migration Issues

Internetwork Packet Exchange (IPX) was the foundational protocol for NetWare from the 1980s until the release of NetWare 5.0, when support for pure TCP/IP became standard.

To aid with migrations from NetWare to OES, coexistence between IPX and TCP/IP networks is still supported on NetWare, but IPX is not supported on Linux.

13.2 DNS and DHCP

Domain Name Service (DNS) is the standard naming service in TCP/IP-based networks. It converts IP addresses, such as 192.168.1.1, to human-readable domain names, such as myserver.example.com, and it reverses the conversion process as required.

The Dynamic Host Configuration Protocol (DHCP) assigns IP addresses and configuration parameters to hosts and network devices.

OES 2 includes a ported version of the NetWare DNS service, and an eDirectory integration with ISC DHCP as explained in the sections that follow.

- Section 13.2.1, "DNS Differences Between NetWare and OES 2," on page 102
- Section 13.2.2, "DHCP Differences Between NetWare and OES 2," on page 103

13.2.1 DNS Differences Between NetWare and OES 2

As you plan to upgrade from NetWare to OES 2, consider the following differences between DNS on NetWare and OES 2:

Table 13-1 *DNS: NetWare 6.5 SP8 vs. OES 2*

Feature or Command	NetWare 6.5 SP8	OES 2
Auditing	Yes	No
DNSMaint	Yes	No
Fault Tolerance	Yes	Yes
Filenames and paths:		
◆ Server binary	◆ `sys:/system/named.nlm`	◆ `/opt/novell/named/bin/novell-named`
◆ `.db`, `.jnl` file	◆ `sys:/etc/dns`	◆ `/etc/opt/novell/named/named.conf`
◆ Stat file, info file		◆ `/var/opt/novell/log/named/named.run`
Console commands:		
◆ Start the server	◆ `named`	◆ `rcnovell-named` or `novell-named`
◆ Stop the server	◆ `named stop`	◆ `rcnovell-named stop`
◆ Check Status	◆ `named status`	◆ `rcnovell-named status`
◆ Unsupported command parameters	◆ N/A	◆ [-dc categories] ◆ [-mstats] ◆ [-nno_of_cpus] ◆ [-qstats]
Journal log size	Specify at the command prompt by using the jsize argument.	Specify by using the iManager plug-in > *max-journal-size* field.

Feature or Command	NetWare 6.5 SP8	OES 2
Management	iManager Command Line Interface	iManager Command Line Interface Unlike the Netware implementation, command line parameters cannot be passed when loading and unloading.
SNMP Support	Yes	No

13.2.2 DHCP Differences Between NetWare and OES 2

As you plan to upgrade from NetWare to OES 2, consider the following differences between DHCP on NetWare and OES 2:

Table 13-2 *DHCP: NetWare 6.5 SP8 vs. OES 2*

Feature or Command	NetWare 6.5 SP8	OES 2
Auditing	Yes	No
Filenames and paths:		
◆ Conf file	◆ N/A	◆ `/etc/dhcpd.conf`
◆ Leases	◆ Stored in eDirectory	◆ `/var/lib/dhcp/db/dhcpd.leases`
◆ Log file	◆ `sys:/etc/dhcp/dhcpsrvr.log`	◆ `/var/log/dhcpd.log`
◆ Startup log	◆ N/A	◆ `/var/log/dhcp-ldap-startup.log` This is a dump of DHCP configurations read from eDirectory when the DHCP server starts.
Management	iManager 2.7 (Wizard-based)	iManager 2.7 (Tab-based) Unlike the NetWare implementation, command line parameters cannot be passed when loading and unloading.
Migration	N/A	There is seamless migration support from NetWare.
Schema changes	N/A	There are separate locator and group objects for centralized management and easy rights management.
SNMP Support	Yes	No
Subnet naming	Yes	No

13.3 Time Services

The information in this section can help you understand your time services options as you move from NetWare to OES 2:

- Section 13.3.1, "Overview of Time Synchronization," on page 104
- Section 13.3.2, "Planning for Time Synchronization," on page 108
- Section 13.3.3, "Coexistence and Migration of Time Synchronization Services," on page 111
- Section 13.3.4, "Implementing Time Synchronization," on page 112
- Section 13.3.5, "Configuring and Administering Time Synchronization," on page 114
- Section 13.3.6, "Daylight Saving Time," on page 114

13.3.1 Overview of Time Synchronization

All servers in an eDirectory tree must have their times synchronized to ensure that updates and changes to eDirectory objects occur in the proper order.

eDirectory gets its time from the server operating system of the OES 2 server where it is installed. It is, therefore, critical that every server in the tree has the same time.

- "Understanding Time Synchronization Modules" on page 104
- "OES 2 Servers as Time Providers" on page 106
- "OES 2 Servers as Time Consumers" on page 107

Understanding Time Synchronization Modules

During the upgrade to OES 2, your eDirectory tree might contain servers running OES 2, NetWare 6.5 SP8, or previous versions of NetWare. Therefore, you must understand the differences in the time synchronization modules that each operating system uses and how these modules can interact with each other.

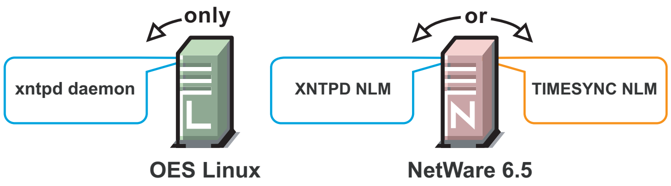
- "OES 2 vs. NetWare 6.5" on page 104
- "OES 2 Servers Use the Network Time Protocol (NTP) to Communicate" on page 105
- "Compatibility with Earlier Versions of NetWare" on page 105

OES 2 vs. NetWare 6.5

As illustrated in Figure 13-1, NetWare 6.5 can use either the Network Time Protocol (NTP) or Timesync modules for time synchronization. Both modules can communicate with OES 2 by using NTP. However, when installing virtualized NetWare, Timesync should always be used (see Section 7.18.2, "Always Use Timesync Rather Than NTP," on page 74).

OES 2 must use the NTP daemon (xntpd).

Figure 13-1 *Time Synchronization for Linux and NetWare*



OES 2 Servers Use the Network Time Protocol (NTP) to Communicate

Because OES 2 and NetWare servers must communicate with each other for time synchronization, and because Linux uses only NTP for time synchronization, it follows that both Linux and NetWare must communicate time synchronization information by using NTP time packets.

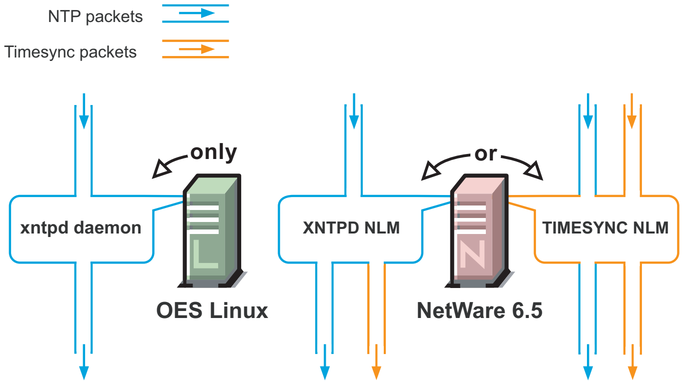
However, this doesn't limit your options on NetWare.

Figure 13-2 illustrates that OES 2 and NetWare 6.5 servers can freely interchange time synchronization information because NetWare 6.5 includes the following:

- A TIMESYNC NLM that both consumes and provides NTP time packets in addition to Timesync packets.
- An XNTPD NLM that can provide Timesync packets in addition to offering standard NTP functionality.

NOTE: Although NetWare includes two time synchronization modules, only one can be loaded at a time.

Figure 13-2 *NTP Packet Compatibilities with All OES Time Synchronization Modules*



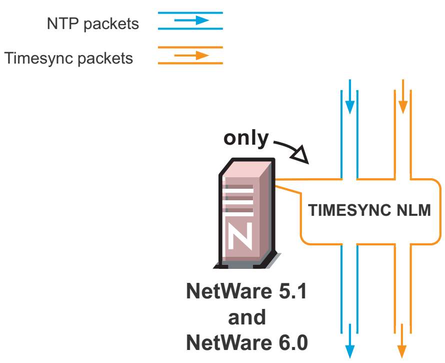
Compatibility with Earlier Versions of NetWare

Earlier versions of NetWare (version 4.2 through version 6.0) do not include an NTP time module. Their time synchronization options are, therefore, more limited.

NetWare 5.1 and 6.0 Servers

Figure 13-3 illustrates that although NetWare 5.1 and 6.0 do not include an NTP time module, they can consume and deliver NTP time packets.

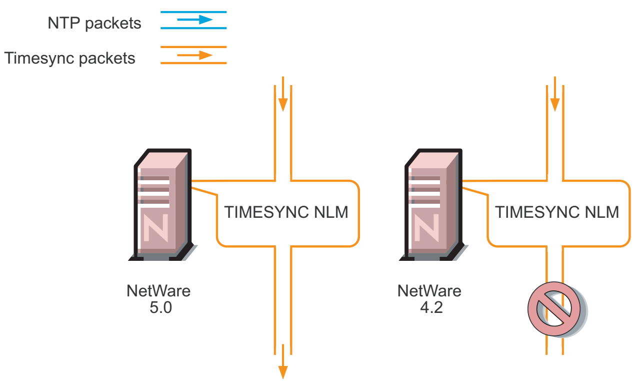
Figure 13-3 *NTP Compatibility of NetWare 5.1 and 6.0*



NetWare 5.0 and 4.2 Servers

Figure 13-4 illustrates that NetWare 4.2 and 5.0 servers can only consume and provide Timesync packets.

Figure 13-4 *Synchronizing Time on NetWare 5.0 and 4.2 Servers*



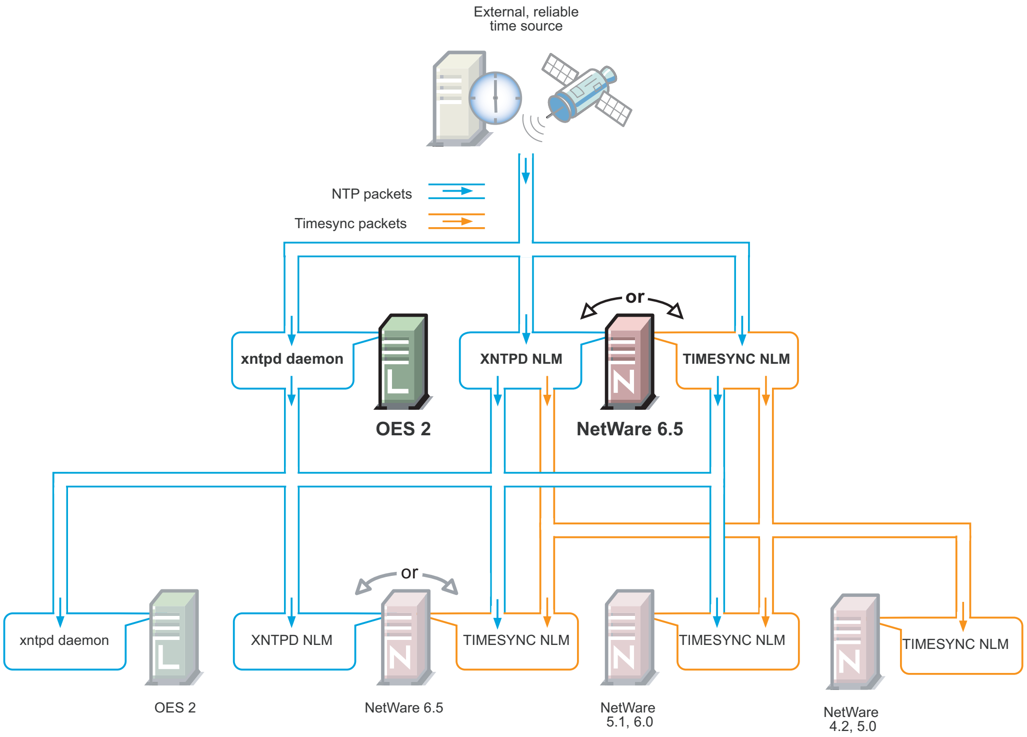
Therefore, if you have NetWare 4.2 or 5.0 servers in your eDirectory tree, and you want to install an OES 2 server, you must have at least one NetWare 5.1 or later server to provide a "bridge" between NTP and Timesync time packets. Figure 13-5 on page 107 illustrates that these earlier server versions can synchronize through a NetWare 6.5 server.

IMPORTANT: As shown in Figure 13-4, we recommend that NetWare 4.2 servers not be used as a time source.

OES 2 Servers as Time Providers

Figure 13-5 shows how OES 2 servers can function as time providers to other OES 2 servers and to NetWare servers, including NetWare 4.2 and later.

Figure 13-5 *OES 2 Servers as Time Providers*

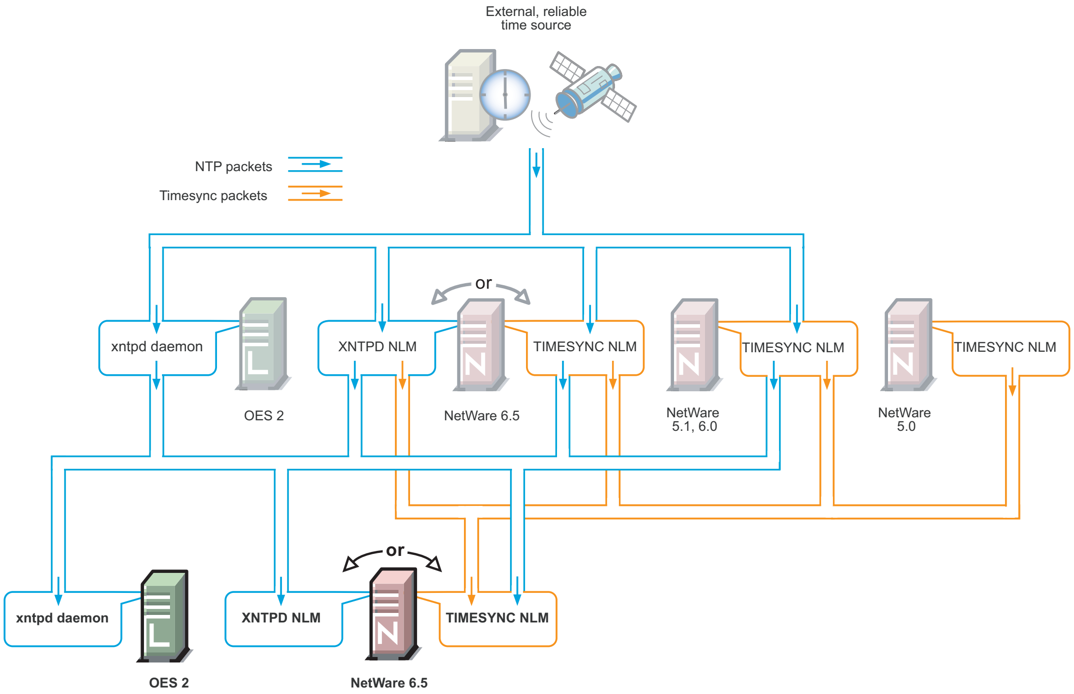


OES 2 Servers as Time Consumers

Figure 13-6 shows the time sources that OES 2 servers can use for synchronizing server time.

IMPORTANT: Notice that NetWare 4.2 is not shown as a valid time source.

Figure 13-6 OES 2 servers as Time Consumers



13.3.2 Planning for Time Synchronization

Use the information in this section to understand the basics of time synchronization planning.

- "NetWork Size Determines the Level of Planning Required" on page 108
- "Choose Timesync for Virtualized NetWare Only" on page 109
- "Planning a Time Synchronization Hierarchy before Installing OES" on page 109

For more detailed planning information, refer to the following resources:

- "How Timesync Works" in the *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- "Network Time Protocol" in the *NW 6.5 SP8: NTP Administration Guide*
- NTP information on the Web (http://www.cis.udel.edu/~mills/ntp.html)

NetWork Size Determines the Level of Planning Required

The level of time synchronization planning required for your network is largely dictated by how many servers you have and where they are located, as explained in the following sections.

- "Time Synchronization for Trees with Fewer Than Thirty Servers" on page 109
- "Time Synchronization for Trees with More Than Thirty Servers" on page 109
- "Time Synchronization across Geographical Boundaries" on page 109

Time Synchronization for Trees with Fewer Than Thirty Servers

If your tree will have fewer than thirty servers, the default installation settings for time synchronization should be sufficient for all of the servers except the first server installed in the tree.

You should configure the first server in the tree to obtain time from one or more time sources that are external to the tree. (See Step 1 in "Planning a Time Synchronization Hierarchy before Installing OES" on page 109.)

All other servers should point to the first server in the tree for their time synchronization needs.

Time Synchronization for Trees with More Than Thirty Servers

If your tree will have more than thirty servers, you need to plan and configure your servers with time synchronization roles that match your network architecture and time synchronization strategy. Example roles might include the following:

- Servers that receive time from external time sources and send packets to other servers further down in the hierarchy
- Servers that communicate with other servers in peer-to-peer relationships to ensure that they are synchronized

Basic planning steps are summarized in "Planning a Time Synchronization Hierarchy before Installing OES" on page 109.

Refer to the following sources for additional help in planning time server roles:

- "Configuring Timesync on Servers" in the *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- "Modes of Time Synchronization" in the *NW 6.5 SP8: NTP Administration Guide*
- NTP information on the Web (http://www.cis.udel.edu/~mills/ntp.html)

Time Synchronization across Geographical Boundaries

If the servers in the tree will reside at multiple geographic sites, you need to plan how to synchronize time for the entire network while minimizing network traffic. For more information, see "Wide Area Configuration" in the *NW 6.5 SP8: NTP Administration Guide*.

Choose Timesync for Virtualized NetWare Only

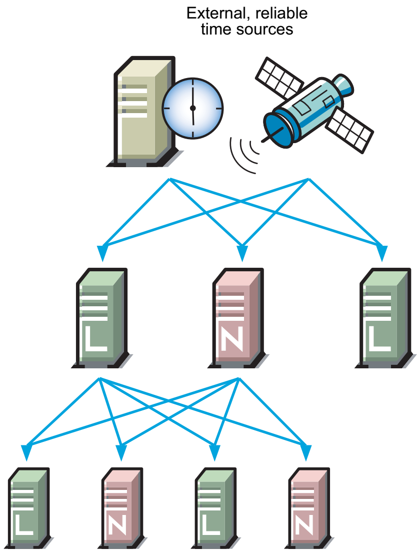
When you install a virtualized NetWare 6.5 server, you should always use Timesync and configure it to communicate using NTP. For more information, see "You Must Use Timesync for Time Synchronization" in the *OES 2 SP3: Installation Guide*.

The dialog box that lets you choose between Timesync and NTP is available as an advanced option in the Time Zone panel during the NetWare installation. Choosing between Timesync and NTP is documented in "Setting the Server Time Zone and Time Synchronization Method" in the *NW65 SP8: Installation Guide*.

Planning a Time Synchronization Hierarchy before Installing OES

The obvious goal for time synchronization is that all the network servers (and workstations, if desired) have the same time. This is best accomplished by planning a time synchronization hierarchy before installing the first OES 2 server, then configuring each server at install time so that you form a hierarchy similar to the one outlined in Figure 13-7.

Figure 13-7 A Basic Time Synchronization Hierarchy



As you plan your hierarchy, do the following:

1 Identify at least two authoritative external NTP time sources for the top positions in your hierarchy.

  - If your network already has an NTP server hierarchy in place, identify the IP address of an appropriate time server. This might be internal to your network, but it should be external to the eDirectory tree and it should ultimately obtain time from a public NTP server.
  - If your network doesn't currently employ time synchronization, refer to the list of public NTP servers published on the ntp.org Web site (http://ntp.isc.org/bin/view/Servers/WebHome) and identify a time server you can use.

2 Plan which servers will receive time from the external sources and plan to install these servers first.

3 Map the position for each Linux server in your tree, including its time sources and the servers it will provide time for.

4 Map the position for each NetWare server in your tree:

  4a Include the server's time sources and the servers it will provide time for.

  4b If your network currently has only NetWare 4.2 or 5.0 servers, be sure to plan for their time synchronization needs by including at least one newer NetWare server in the tree and configuring the older servers to use the newer server as their time source. (See "NetWare 5.0 and 4.2 Servers" on page 106.)

5 Be sure that each server in the hierarchy is configured to receive time from at least two sources.

6 (Conditional) If your network spans geographic locations, plan the connections for time-related traffic on the network and especially across WANs.

  For more information, see "Wide Area Configuration" in the *NW 6.5 SP8: NTP Administration Guide*.

For more planning information, see the following documentation:

- *NW 6.5 SP8: Network Time Synchronization Administration Guide*

- *NW 6.5 SP8: NTP Administration Guide*
- NTP information found on the OES 2 server in /usr/share/doc/packages/xntp and on the Web (http://www.cis.udel.edu/~mills/ntp.html)

13.3.3 Coexistence and Migration of Time Synchronization Services

The time synchronization modules in OES have been designed to ensure that new OES 2 servers can be introduced into an existing network environment without disrupting any of the products and services that are in place.

This section discusses the issues involved in the coexistence and migration of time synchronization in OES in the following sections:

- "Coexistence" on page 111
- "Upgrading from NetWare to OES 2" on page 112

Coexistence

This section provides information regarding the coexistence of the OES time synchronization modules with existing NetWare or Linux networks, and with previous versions of the TIMESYNC NLM. This information can help you confidently install new OES 2 servers into your current network.

- "Compatibility" on page 111
- "Coexistence Issues" on page 112

Compatibility

The following table summarizes the compatibility of OES time synchronization modules with other time synchronization modules and eDirectory. These compatibilities are illustrated in Figure 13-5 on page 107 and Figure 13-6 on page 108.

Table 13-3 *Time Synchronization Compatibility*

Module	Compatibility
TIMESYNC NLM (NetWare)	Can consume time from ◆ All previous versions of Timesync. However, the NetWare 4.2 TIMESYNC NLM should not be used as a time source. ◆ Any TIMESYNC or NTP daemon. Can provide time to ◆ All previous versions of Timesync. ◆ Any TIMESYNC or NTP daemon.
XNTPD NLM (NetWare)	Can consume time from ◆ Any NTP daemon. Can provide time to ◆ All previous versions of Timesync. ◆ Any NTP daemon.

Module	Compatibility
xntpd daemon (SLES 10)	Can consume time from - Any NTP daemon. Can provide time to - Any NTP daemon.
eDirectory	eDirectory gets its time synchronization information from the host OS (Linux or NetWare), not from the time synchronization modules.

Coexistence Issues

If you have NetWare servers earlier than version 5.1, you need to install at least one later version NetWare server to bridge between the TIMESYNC NLM on the earlier server and any OES 2 servers you have on your network. This is because the earlier versions of Timesync can't consume or provide NTP time packets and the xntpd daemon on Linux can't provide or consume Timesync packets.

Fortunately, the TIMESYNC NLM in NetWare 5.1 and later can both consume and provide Timesync packets. And the XNTPD NLM can provide Timesync packets when required.

This is explained in "Compatibility with Earlier Versions of NetWare" on page 105.

Upgrading from NetWare to OES 2

The OES 2 SP3 Migration Tool can migrate time synchronization services from NetWare to Linux. For more information, see "Migrating Timesync/NTP from NetWare to NTP on OES 2 Linux" in the *OES 2 SP3: Migration Tool Administration Guide*.

13.3.4 Implementing Time Synchronization

As you plan to implement your time synchronization hierarchy, you should know how the NetWare and OES 2 product installations configure time synchronization on the network. Both installs look at whether you are creating a new tree or installing into an existing tree.

- "New Tree" on page 112
- "Existing Tree" on page 113

New Tree

By default, both the OES 2 and the NetWare 6.5 SP8 installs configure the first server in the tree to use its internal (BIOS) clock as the authoritative time source for the tree.

Because BIOS clocks can fail over time, you should always specify an external, reliable NTP time source for the first server in a tree. For help finding a reliable NTP time source, see the NTP Server Lists (http://ntp.isc.org/bin/view/Servers/WebHome) on the Web.

- "OES 2" on page 113
- "NetWare 6.5 SP8" on page 113

OES 2

When you configure your eDirectory installation, the OES 2 install prompts you for the IP address or DNS name of an NTP v3-compatible time server.

If you are installing the first server in a new eDirectory tree, you have two choices:

- You can enter the IP address or DNS name of an authoritative NTP time source (recommended).
- You can leave the field displaying Local Time, so the server is configured to use its BIOS clock as the authoritative time source.

  IMPORTANT: We do not recommend this second option because BIOS clocks can fail over time, causing serious problems for eDirectory.

NetWare 6.5 SP8

By default, the NetWare install automatically configures the TIMESYNC NLM to use the server's BIOS clock. As indicated earlier, this default behavior is not recommended for production networks. You should, therefore, manually configure time synchronization (either Timesync or NTP) while installing each NetWare server.

Manual time synchronization configuration is accessed at install time from the Time Zone dialog box by clicking the *Advanced* button as outlined in "Choose Timesync for Virtualized NetWare Only" on page 109 and as fully explained in "Setting the Server Time Zone and Time Synchronization Method" in the *NW65 SP8: Installation Guide*.

Existing Tree

When a server joins an existing eDirectory tree, both OES installations do approximately the same thing.

- "OES 2" on page 113
- "NetWare 6.5 SP8" on page 114

OES 2

If you are installing into an existing tree, the OES 2 install proposes to use the IP address of the eDirectory server (either NetWare or Linux) as the NTP time source. This default should be sufficient unless one of the following is true:

- The server referenced is a NetWare 5.0 or earlier server, in which case you need to identify and specify the address of another server in the tree that is running either a later version of NetWare or OES 2.
- You will have more than 30 servers in your tree, in which case you need to configure the server to fit in to your planned time synchronization hierarchy. For more information, see "Planning a Time Synchronization Hierarchy before Installing OES" on page 109.

The OES 2 install activates the xntp daemon and configures it to synchronize server time with the specified NTP time source. After the install finishes, you can configure the daemon to work with additional time sources to ensure fault tolerance. For more information, see "Changing Time Synchronization Settings on a SLES 10 Server" on page 114.

NetWare 6.5 SP8

If you are installing into an existing tree, the NetWare 6.5 SP8 install first checks to see whether you manually configured either NTP or Timesync time synchronization sources while setting the server Time Zone (see "Setting the Server Time Zone and Time Synchronization Method" in the *NW65 SP8: Installation Guide*).

If you will have more than 30 servers in your tree, you should have developed a time synchronization plan (see "Planning a Time Synchronization Hierarchy before Installing OES" on page 109) and used the Time Zone panel to configure your server according to the plan.

If you haven't manually configured time synchronization sources for the server (for example, if your tree has fewer than 30 servers), the install automatically configures the Timesync NLM to point to the IP address of the server with a master replica of the tree's [ROOT] partition.

13.3.5 Configuring and Administering Time Synchronization

As your network changes, you will probably need to adjust the time synchronization settings on your servers.

- "Changing Time Synchronization Settings on a SLES 10 Server" on page 114
- "Changing Time Synchronization Settings on a NetWare Server" on page 114

Changing Time Synchronization Settings on a SLES 10 Server

This method works both in the GUI and at the command prompt and is the most reliable method for ensuring a successful NTP implementation.

1. Launch YaST on your SLES 10 server by either navigating to the application on the desktop or typing `yast` at the command prompt.
2. Click *Network Services* > *NTP Client*.
3. In the *NTP Client Configuration* dialog box, click *Complex Configuration*.
4. Modify the NTP time settings as your needs require.

Changing Time Synchronization Settings on a NetWare Server

Time synchronization settings and their modification possibilities are documented in the following administration guides:

- Timesync: *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- NTP: *NW 6.5 SP8: NTP Administration Guide*

13.3.6 Daylight Saving Time

For information about daylight saving time (DST), see the DST Master TID on the Novell Support site (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3094409)

13.4 Discovery Services

Various discovery mechanisms are usually available on an OES 2 network.

- DNS/DHCP

- Directory services
- Local host configuration files
- Service Location Protocol (SLP services)
- Universal Description, Discovery, and Integration (UDDI) server

Some systems are designed to leverage only a single discovery technology. Others choose among the various providers. And some use different technologies in combination with each other.

- Section 13.4.1, "Novell SLP and OpenSLP," on page 115
- Section 13.4.2, "WinSock and Discovery Is NetWare only," on page 115
- Section 13.4.3, "UDDI and Discovery," on page 115
- Section 13.4.4, "CIMOM and Discovery," on page 115

13.4.1 Novell SLP and OpenSLP

NetWare 3 and 4 used the IPX-based Service Advertising Protocol (SAP) as the discovery mechanism. All the servers advertised their services automatically. If a server went offline, the SAP information on the network was dynamically refreshed.

Starting with NetWare 5 and pure TCP/IP, the Service Location Protocol was adopted as the default, though optional, discovery mechanism. SLP was chosen because it was the TCP/IP-based protocol most like SAP in its automatic nature and dynamic refresh capabilities.

For more information, see Section 13.5, "SLP," on page 116.

13.4.2 WinSock and Discovery Is NetWare only

There is no WinSock equivalent in the Linux environment. BSDSock provides for transport only, not name resolution. Therefore, services that leveraged WinSock on NetWare use other service-discovery mechanisms on OES 2.

13.4.3 UDDI and Discovery

UDDI is an open source, platform-independent registry that lets you provide a discovery service on the World Wide Web to easily locate, integrate, and manage businesses and services.

For NetWare 6.5, Novell developed a directory-enabled UDDI server for use with the exteNd J2EE Application Server. Starting with NetWare 6.5 SP3, the UDDI server component was removed from the list of products that could be installed.

The Novell UDDI server has been released as open source software and is available for download on the Novell Forge Web site (http://forge.novell.com/modules/xfmod/project/showfiles.php?group_id=1025).

13.4.4 CIMOM and Discovery

The current OpenWBEM implementation of the Common Information Model Object Manager (CIMOM) lists SLP as an optional discovery provider. If SLP is to be used with CIMOM, it must be in compliance with the SLP API specification (RFC 2614). The default discovery vehicle for CIMOM is the statically configured URI. For more information, see the CIMOM specification at the Desktop Management Task Force (DMTF) Web site (http://www.dmtf.org).

13.5 SLP

The OpenSLP services on OES 2 are compatible with NetWare SLP services.

This section discusses the following topics:

- Section 13.5.1, "Overview," on page 116
- Section 13.5.2, "Comparing Novell SLP and OpenSLP," on page 118
- Section 13.5.3, "Setting Up OpenSLP on OES 2 Networks," on page 119
- Section 13.5.4, "Using Novell SLP on OES 2 Networks," on page 123

13.5.1 Overview

The Service Location Protocol (SLP) was developed so that clients and other software modules can dynamically discover and use services on the network without knowing the IP address or the hostname of the server offering the service.

- "Why SLP Is Needed" on page 116
- "About the Three SLP Agents and Their Roles" on page 116
- "Overcoming the Subnet Limitation" on page 117
- "An eDirectory Example" on page 117
- "What Happens When a DA Goes Down?" on page 117

Why SLP Is Needed

NetWare: Although many other applications and server types rely on SLP for service discovery, NetWare services are actually integrated with eDirectory, and if eDirectory is configured correctly, the services work without SLP. However, SLP is automatically provided on NetWare for other services that might be installed.

OES 2: On the other hand, for OES 2 services to work, the server must either:

- Have an eDirectory replica installed.

  This is not automatic after the third server installed in a tree, nor is having more than three to five replicas on servers in the tree recommended.
- Have eDirectory registered with the OpenSLP service running on the server.

  This requires SLP configuration either during the OES 2 installation or manually.

About the Three SLP Agents and Their Roles

Three software "agents" provide the infrastructure for service discovery:

- **Service Agents (SAs):** Are a required component of any SLP infrastructure. They act on behalf of a network service that is running on a server by advertising that the service is available.
- **User Agents (UAs):** Are also required. They act on behalf of clients or other software modules that need network services by searching for the needed services.

- **Directory Agents (DAs):** Are technically optional, but they are used in most SLP infrastructures. They collect service information from Service Agents so that User Agents can more easily locate the services. DAs are like a phone book directory listing of services on the network.

  DAs are not needed when all of the SAs and UAs are on the same subnet. This is because the UAs and SAs can find each other within the subnet using multicast packets, provided that there are no firewalls that are set to block multicast traffic.

Overcoming the Subnet Limitation

Novell recommends against routing multicast packets across subnet boundaries, and most network configurations conform with that recommendation. Therefore, when SAs and UAs are on different subnets, they need an alternative to multicasting for advertizing and locating services on the other subnets.

Network administrators use DAs to solve this problem by setting up organzational or geographical DAs and then configuring the SAs and UAs within the organization or georgraphical area to use them. Many administrators further subdivide the DA workload by defining multiple SLP scopes based on different kinds of network services, and then configuring the SAs and UAs to communicate with the DAs servicing the scope that pertains to them.

An eDirectory Example

When you configure eDirectory during an OES server installation, you have the option of specifying one or more SLP DAs for the server to communicate with. Each time eDirectory starts and every hour thereafter, the server’s SA will send a unicast packet to the server’s assigned DAs, advertising that its eDirectory services are available.

IMPORTANT: Prior to eDirectory 8.8.2, the eDirectory SA advertised service availability every 10 minutes by default. Starting with eDirectory 8.8.2, the refresh interval changed to one hour. This has caused some confusion for network administrators who couldn’t figure out why it took so long for eDirectory to register as a service

For information on how to set the refresh interval to a smaller value, see TID 7001449 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7001449&sliceId=2&docTypeID=DT_TID_1_1&dialogID=104660609&stateId=0%200%20209665064) in the Novell Support Knowledgebase.

What Happens When a DA Goes Down?

As you can imagine, a Directory agent in a large organization can accumulate many service listings after it has been running for a while. Unfortunately, because DAs are inherently cache-only repositories, if they go down for some reason, when they come back up their list of services is initially blank.

Novell SLP solved this problem on NetWare 5.x and later through eDirectory Modified Event notifications. These notifications keep all of the NetWare DA's that are servicing the same scope in sync with each other. After going down and coming back up, a NetWare DA can quickly recover its directory listings.

OpenSLP DA's, on the other hand, have historically been completely independent from each other. Because they are not eDirectory-aware, they have had no means of recovering the directory listings they had prior to going down.

This has now changed in OES 2 SP3.

OpenSLP DAs can now

- Retrieve and/or push service information to and/or from other DAs. For more information, see "Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs" on page 120.
- Back up their service registrations so that when the DA service is started up it can read the backup file and pre-populate its cache. For more information, see "Backing Up Registrations and Managing Persistence" on page 121.

These changes provide, in effect, the same type of DA to DA communication for OES that has traditionally been available only on NetWare.

13.5.2 Comparing Novell SLP and OpenSLP

Table 13-4 *SLP Solutions*

Platform	NetWare	OES 2
SLP Solution	Novell SLP	OpenSLP
About the Solution	The Novell version of SLP adapted portions of the SLP standard to provide a more robust service advertising environment. Novell SLP remains the default discovery mechanism for NetWare 6.5 SP8 servers. However, all NetWare service components that engage in discovery, including Novell Client software, can use alternative mechanisms such as DNS, eDirectory, or local host configuration files.	OpenSLP is an implementation of various IETF specifications, including RFC 2614 (SLP version 2.0). It is the default SLP service installed on SLES 10. In OES 2, OpenSLP is available for those applications that require it. The default discovery mechanism is actually DNS, but SLP must be present for any applications that require it, especially in those cases where the OES 2 server is the fourth or later server added to a tree and doesn't have an eDirectory replica automatically installed.
Differences	Novell SLP directory agents (DAs) store service registrations for their SLP scope in eDirectory. As a new service registration is stored in eDirectory, other DAs assigned to the same scope are notified so that they can refresh their caches with the latest service information. Also, when a Novell SLP DA starts up, it immediately populates its cache with the latest service information stored in eDirectory. **NOTE:** Novell SLP DAs do not directly share information with each other as many administrators have assumed. But they do maintain well synchronized caches through eDirectory as described above.	OpenSLP directory agents (DAs) are able to share service registrations as described in "Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs" on page 120. OpenSLP is also capable of ensuring data persistence when DAs go down, as explained in "Backing Up Registrations and Managing Persistence" on page 121.
Compatibility	Novell SLP user agents (UAs) or service agents (SAs) can access both Novell SLP DAs and OpenSLP DAs.	OpenSLP-based user agents or service agents can access both Novell SLP DAs and OpenSLP DAs.

Platform	NetWare	OES 2
Documentation	"Configuring OpenSLP for eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*	"Configuring OpenSLP for eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

13.5.3 Setting Up OpenSLP on OES 2 Networks

SLP services are always installed as part of both NetWare and SLES 10 SP4 (the underlying OES 2 SP3 platform). On NetWare the Novell SLP service is configured to automatically work with eDirectory and other services. On OES 2, the OpenSLP service must be manually configured to work with eDirectory and other services.

- "When Is OpenSLP Required?" on page 119
- "Setting Up an OpenSLP DA Server" on page 119
- "Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs" on page 120
- "Backing Up Registrations and Managing Persistence" on page 121
- "Configuring OES 2 Servers to Access the OpenSLP DA" on page 121
- "Configuring NetWare Servers to Use the OpenSLP Service" on page 122

When Is OpenSLP Required?

You must set up OpenSLP on your OES 2x server if both of the following apply:

- You plan to install more than three servers into a new tree or a new eDirectory partition being created on an OES 2 server.
- You either don't have an existing Novell SLP service, or you don't want to continue using Novell SLP.

IMPORTANT: If you need to set up OpenSLP for the reasons above, it is most convenient if you do it before you install the fourth server in your tree or partition. That way you can point to the SLP service during the installation. Setting up SLP services on every OES 2 server is recommended.

Setting Up an OpenSLP DA Server

If you need OpenSLP and you don't already have an OpenSLP Directory Agent (DA) set up on your network, for simplicity's sake we recommend that you set up the first OES 2 server in your tree as an OpenSLP DA. Although SLP services can be managed without having a Directory Agent, that approach is far less robust, requires multicasting, and involves disabling the firewall.

After creating the DA, you can then configure all subsequently installed servers to either point to that DA or to other DAs you create later.

1 On the OES 2 server that will become the DA, open the `/etc/slp.conf` file in a text editor.

2 In `slp.conf`, remove the semicolon [;]) from the beginning of the following line:

```
;net.slp.isDA = true
```

so that it reads

```
net.slp.isDA = true
```

3 Find the following line:

```
;net.slp.useScopes = myScope1, myScope2, myScope3
```

IMPORTANT: The example in the configuration file is misleading because the spaces after each comma are not ignored as one might expect them to be.

Therefore, the scope names created or configured by the statement after the first comma actually have leading spaces in them. For example, the first scope name is “myScope1” but the scope names that follow it all have leading spaces, “ myScope2”, “ myScope3” and so on. This is a problem, especially if one of the later names becomes the first name in a subsequent SLP configuration and the leading space is ignored.

If you use the scopes given in the example, remove the spaces between the entries.

4 Modify the line by removing the semicolon and typing the name of the scope you want this DA to use to provide service information on the network. For example, you might change the line as follows:

```
net.slp.useScopes = Directory
```

IMPORTANT: Although SLP provides a default scope if no scope is specified, it is always good practice to define one or more scopes by configuring the net.slp.useScopes parameter in `slp.conf`.

Scopes group and organize the services on your network into logical categories. For example, the services that the Accounting group needs might be grouped into an Accounting scope.

More information about scope planning is available in “Configuring OpenSLP for eDirectory” in the *Novell eDirectory 8.8 SP7 Administration Guide* and on the OpenSLP Web site (http://www.openslp.org/).

When no scope is specified, all services are registered in a scope named Default.

5 Configure the firewall on the DA server to allow SLP daemon traffic:

5a In the YaST Control Center, click *Security and Users* > *Firewall*.

5b In the left navigation frame, click *Allowed Services*.

5c Click the *Services to Allow* drop-down list and select *SLP Daemon*.

5d Click *Add* > *Next*.

5e Click *Accept*.

6 At the command prompt, enter the following command to restart the SLP daemon:

```
rcslpd restart
```

7 (Conditional) If you are doing this after installing OES 2 and eDirectory, you must also restart eDirectory by entering the following command:

```
rcndsd restart
```

8 Continue with the following sections that apply to your situation:

- Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs (page 120)
- Backing Up Registrations and Managing Persistence (page 121)
- Configuring OES 2 Servers to Access the OpenSLP DA (page 121)
- Configuring NetWare Servers to Use the OpenSLP Service (page 122)

Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs

This is accomplished through setting the following parameters in the `slp.conf` file:

```
net.slp.dasyncreg = true/false
```

```
slp.DAaddresses = IP_address_1,IP_address_2
```

If the `net.slp.dasyncreg` parameter value is set to `true`, then synchronization is achieved by the DA pushing or pulling SLP registrations from the DAs listed for the `slp.DAaddresses` parameter, as follows:

1. When the DA starts up, it pulls the registration information from all of the server DAs listed in the the `slp.DAaddresses` parameter, including any Novell SLP DAs listed.
2. When the DA receives a service registration, it forwards the information to the OpenSLP DAs that are listed.

IMPORTANT: Service registrations cannot be pushed to Novell SLP DA's.

Backing Up Registrations and Managing Persistence

This is accomplished through setting the following parameters in the `slp.conf` file:

```
net.slp.isDABackup = true/false
```

```
net.slp.DABackupInterval = time_in_seconds
```

If the `net.slp.isDABackup` parameter is set to `true`, service registrations are backed up in the `/etc/slp.reg.d/slpd/DABackup` file at the interval specified for the `net.slp.DABackupInterval` parameter. By default, the interval parameter value is 900 secs.

Configuring OES 2 Servers to Access the OpenSLP DA

If you created the OpenSLP DA on an OES 2 server installed in your tree, then SLP is properly configured on that server and these instructions do not apply to it.

For all other OES 2 servers installed in your eDirectory tree, you should complete one of the following procedures as it applies to your situation:

- "Configuring for DA Access During the OES 2 Installation" on page 121
- "Configuring for DA Access Before or After Installing the OES 2 Server" on page 122

Configuring for DA Access During the OES 2 Installation

As you install OES 2 by using the instructions in the "Novell eDirectory Services" section of the *OES 2 SP3: Installation Guide*, do the following:

1 When you reach the "eDirectory Configuration - NTP and SLP" section of the installation, select *Configure SLP to Use an Existing Directory Agent*.

The first option, *Do not configure SLP*, causes problems with eDirectory and other services if this is the fourth or later server installed in the tree. The second option, *Use Multicast*, requires that you disable the firewall on the server. Disabling the firewall is always discouraged.

2 In the *Service Location Protocol Scopes* field, specify the scope you defined in Step 4 on page 120. You can also list additional scopes, separated by commas (no spaces).

For example, you might type `Directory` in the field if that is the scope name you assigned to the DA you created.

3. In the *Configured SLP Directory Agent* field, type the IP address of the DA server you defined in "Setting Up an OpenSLP DA Server" on page 119. You can also list additional DA addresses, separated by commas.
4. Return to the "Novell Modular Authentication Services" instructions in the *OES 2 SP3: Installation Guide*.

Configuring for DA Access Before or After Installing the OES 2 Server

Whether you configure DA access before installing OES 2 on a SLES 10 server or after a simultaneous install of SLES 10 and OES 2, the manual DA configuration process is the same.

1. Open `/etc/slp.conf` in a text editor.
2. Find the following line:

   ```
   ;net.slp.useScopes = myScope1, myScope2, myScope3
   ```

   IMPORTANT: The example in the configuration file is misleading because the spaces after each comma are not ignored as one might expect them to be.

   Therefore, the scope names created or configured by the statement after the first comma actually have leading spaces in them. For example, the first scope name is "myScope1" but the scope names that follow it all have leading spaces, " myScope2", " myScope3" and so on. This is a problem, especially if one of the later names becomes the first name in a subsequent SLP configuration and the leading space is ignored.

   If you use the scopes given in the example for some reason, remove the spaces between the entries.
3. Modify the line by removing the semicolon and typing the name or names of the scopes you want this server to have access to. Be sure to include the scope you defined in Step 4 on page 120.

   For example, you might change the line as follows:

   ```
   net.slp.useScopes = Directory
   ```
4. Find the following line:

   ```
   ;net.slp.DAAddresses = myDa1,myDa2,myDa3
   ```
5. Modify the line by removing the semicolon and typing the actual IP address of the OpenSLP DA you defined in "Setting Up an OpenSLP DA Server" on page 119.

```
net.slp.DAAddresses = IP_Address
```

6. Save the file and close it.
7. At the Linux command prompt, enter the following to restart the SLP daemon and reset its configuration:

   ```
   rcslpd restart
   ```

Configuring NetWare Servers to Use the OpenSLP Service

IMPORTANT: NetWare uses Novell SLP by default and will configure a server for that service if possible.

Complete one of the following as it applies to your situation:

- "Configuring for DA Access During the NetWare Server Installation" on page 123
- "Configuring for DA Access After Installing the NetWare Server" on page 123

Configuring for DA Access During the NetWare Server Installation

1. In the dialog box where you set up IP addresses for network boards, click *Advanced*.
2. Click the *SLP* tab.
3. Specify the IP address of the OES 2 DA servers—up to three.
4. Type the list of scopes covered by the configured DAs that you want the NetWare server to have access to.

   IMPORTANT: We recommend you do not configure the server to use multicast because that necessitates disabling firewalls, which is never recommended.

5. Click OK.

Configuring for DA Access After Installing the NetWare Server

1. Using a text editor, edit the `SYS:ETC/slp.cfg` file on the NetWare server and add the following line for each DA server you want the NetWare server to have access to:

```
DA IPV4, IP_Address1

DA IPV4, IP_Address2
```

   where *IP_AddressX* is the IP address of an OES 2 DA server.

2. Save the file and close it.
3. At the NetWare console prompt, specify the scopes you want the NetWare server to have access to, write the SLP cache to the registry, and restart the SLP service:

```
set slp scope list = scope1,scope2,...
    flush cdbe
    set slp reset = on
```

4. Verify that SLP is functioning correctly by entering the following command:

   ```
   display slp services
   ```

13.5.4 Using Novell SLP on OES 2 Networks

If you have a NetWare tree, you automatically have Novell SLP on your network and you can continue to use it as the SLP service during the upgrade to OES 2 until you are ready to switch to OpenSLP.

This section discusses the following:

- "NetWare Is Configured with Novell SLP By Default" on page 123
- "Configuring OES 2 Servers to Access the Novell SLP DA" on page 124
- "Checking the Status of Novell SLP Services" on page 125

NetWare Is Configured with Novell SLP By Default

When you install NetWare, if you don't specify an alternate SLP configuration, the server is automatically configured to use Novell SLP in a way that is sufficient for most networks. Information about Novell SLP and customization instructions is available in "Configuring OpenSLP for eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

Configuring OES 2 Servers to Access the Novell SLP DA

For each of the OES 2 servers installed in your eDirectory tree, you should complete one of the following procedures as it applies to your situation:

- "Configuring for DA Access During the OES 2 Installation" on page 124
- "Configuring for DA Access Before or After Installing the OES 2 Server" on page 124

Configuring for DA Access During the OES 2 Installation

As you install OES 2, in the "Novell eDirectory Services" section of the *OES 2 SP3: Installation Guide*, do the following:

1. When you reach the SLP section of the installation, select *Configure SLP to Use an Existing Directory Agent*.

   The first option, *Do not configure SLP*, causes problems with eDirectory and other services if this is the fourth or later server installed in the tree. The second option, *Use Multicast*, requires that you disable the firewall on the server. Disabling the firewall is always discouraged.

2. In the *Service Location Protocol Scopes* field, specify one or more appropriate scopes that are defined on your network.

   If you aren't sure about the exact scope names, you can view the SLP configuration of a NetWare server on the same network segment. Log into Novell Remote Manager on the server and click *Manage Applications* > *SLP*.

   You can list multiple scopes, separated by commas (no spaces).

   For example, you might type `Directory` in the field.

3. In the *Configured SLP Directory Agent* field, type the IP address of an appropriate DA server.

   You can use Novell Remote Manager on a NetWare server if you aren't sure which address to use.

   You can also list additional DA addresses, separated by commas.

4. Return to the "Novell eDirectory Services" instructions in the *OES 2 SP3: Installation Guide*.

Configuring for DA Access Before or After Installing the OES 2 Server

Whether you configure DA access before installing OES 2 on a SLES 10 server or after a simultaneous install of SLES 10 and OES 2, the manual DA configuration process is the same.

1. Open `/etc/slp.conf` in a text editor.
2. Find the following line:

   ```
   ;net.slp.useScopes = myScope1, myScope2, myScope3
   ```

   IMPORTANT: The example in the configuration file is misleading because the spaces after each comma are not ignored as one might expect them to be.

   Therefore, the scope names created or configured by the statement after the first comma actually have leading spaces in them. For example, the first scope name is "myScope1" but the scope names that follow it all have leading spaces, " myScope2", " myScope3" and so on. This is a problem, especially if one of the later names becomes the first name in a subsequent SLP configuration and the leading space is ignored.

   If you use the scope names given in the example, remove the spaces between the entries.

3. Modify the line by removing the semicolon and typing the name or names of the scopes you want this server to have access to.

If you aren't sure about the exact scope names, you can view the SLP configuration of a NetWare server on the same network segment. Log into Novell Remote Manager on the server and click *Manage Applications* > *SLP*.

You can list multiple scopes, separated by commas (no spaces).

For example, you might change the line as follows:

```
net.slp.useScopes = Directory
```

4 Find the following line:

```
;net.slp.DAAddresses = myDa1,myDa2,myDa3
```

5 Modify the line by removing the semicolon and typing the actual IP address of the Novell SLP DA (using Novell Remote Manager if necessary).

```
net.slp.DAAddresses = IP_Address
```

6 Save the file and close it.

7 At a terminal prompt, enter the following to restart the SLP daemon and reset its configuration:

```
rcslpd restart
```

8 Enter the following commands to verify that the DA and scopes you configured are recognized.

```
slptool findsrvs service:
```

The DA server should be listed.

```
slptool findscopes
```

The scopes should be listed.

9 If you did this after installing OES 2, enter the following to verify that the tree is found:

```
slptool findsrvs service:ndap.novell
```

Checking the Status of Novell SLP Services

There are several ways to check the status of Novell SLP services.

- If you know the IP addresses of the DAs, check the `SYS:\etc\slp.cfg` file on non-DA servers to see if the DA IP addresses are listed.
- If you know the scope names, check for the proper scope name configuration by using the `SET SLP SCOPE LIST` command.
- Use the `DISPLAY SLP SERVICES` command to list all of the services that are registered in all of the scopes that the server is configured to use.
- Use iManager to open the scope container object to see all of the registered services.
- If you are registering different services in different scopes, look in the `SYS:\etc\slp.cfg` file for `REGISTER TYPE` lines.
- At the DOS prompt on a Windows workstation with Client32 installed, use the `SLPINFO /ALL` command.

14 Storage and File Systems

Hosting shared data storage is one of the primary functions of network servers. Whether data volumes are directly attached to the server in RAID configurations or externally accessible in Storage Area Network (SAN) or Network Attached Storage (NAS) configurations, users need to be able to access their data on a continual basis.

Use this section to understand the file storage solutions available in Open Enterprise Server 2 and then to plan a storage solution that meets your file system management needs.

The "Storage and File Systems (http://www.novell.com/documentation/oes2/storage.html)" section in the OES 2 online documentation provides overview, planning, implementation, and configuration links.

This section provides the following information about the process of planning and implementing storage services in OES:

- Section 14.1, "Overview of OES 2 Storage," on page 127
- Section 14.2, "Planning OES File Storage," on page 132
- Section 14.3, "Coexistence and Migration of Storage Services," on page 138
- Section 14.4, "Configuring and Maintaining Storage," on page 140

Other storage-related topics in this guide:

- Chapter 17, "Access Control and Authentication," on page 167
- Section 17.2, "Authentication Services," on page 178
- Appendix D, "Backup Services," on page 257
- Chapter 18, "File Services," on page 183

14.1 Overview of OES 2 Storage

This section presents the following overview information for the file systems included in OES:

- Section 14.1.1, "Databases," on page 128
- Section 14.1.2, "iSCSI," on page 128
- Section 14.1.3, "File System Support in OES," on page 128
- Section 14.1.4, "Storage Basics by Platform," on page 130
- Section 14.1.5, "Storage Options," on page 130
- Section 14.1.6, "NetWare Core Protocol Support (Novell Client Support) on Linux," on page 132

14.1.1 Databases

See the topics in "databases (http://www.novell.com/documentation/oes2/storage.html#b1in185q)" in the OES online documentation.

14.1.2 iSCSI

See the topics in "iSCSI for Linux (http://www.novell.com/documentation/oes2/storage.html#iscsi)" in the OES online documentation.

14.1.3 File System Support in OES

As shown in Figure 14-1, both OES 2 and NetWare support Novell Storage Services as well as their traditional file systems.

Figure 14-1 *File System Choices on OES 2 Servers*

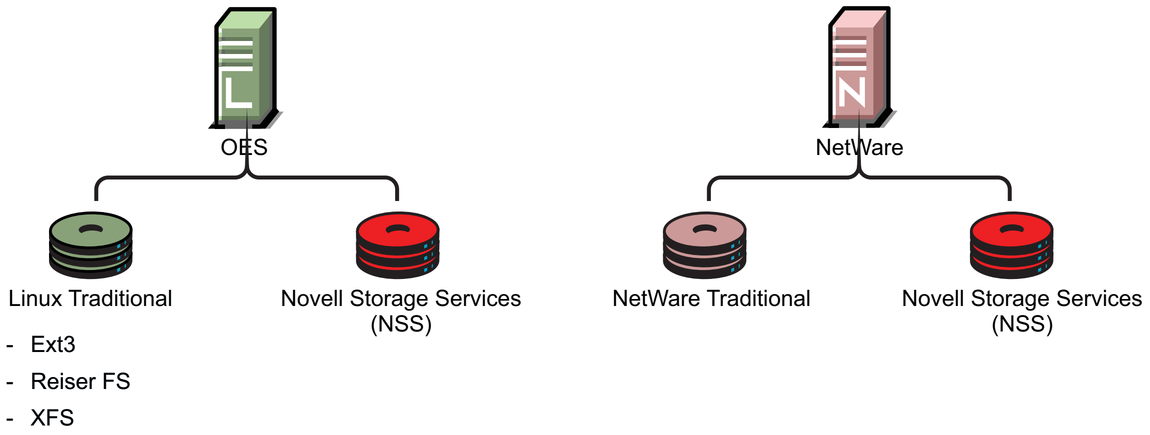


Table 14-1 summarizes OES file system types and provides links to more information.

Table 14-1 *File Systems Available on OES 2 Servers*

File System Type	Summary	Link for More Information
Linux POSIX File Systems	SLES 10 includes a number of different file systems, the most common of which are Ext3, Reiser, and XFS. OES 2 services are supported on Ext3, Reiser, and XFS.	For an overview of the supported file systems in OES 2, see "File Systems Overview" in the *OES 2 SP3: File Systems Management Guide*.
NetWare Traditional File System	This is a legacy file system on NetWare servers that supports the Novell file service trustee access control model.	For more information, see the *NW6.5 SP8: Traditional File System Administration Guide*.

File System Type	Summary	Link for More Information
Novell Storage Services (NSS)	NSS lets you manage your shared file storage for any size organization. On Netware, NSS features include visibility, a trustee access control model, multiple simultaneous name space support, native Unicode, user and directory quotas, rich file attributes, multiple data stream support, event file lists, and a file salvage subsystem. Most of these features are also supported on NSS on Linux. For a feature comparison, see "Comparison of NSS on NetWare and NSS on Linux" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.	For an overview of NSS, see "Overview of NSS" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Novell Storage Services (NSS)

The following sections summarize key points regarding NSS:

- "Understanding NSS Nomenclature" on page 129
- "Comparing NSS with Other File Systems" on page 129
- "NSS and Storage Devices" on page 129

Understanding NSS Nomenclature

NSS uses a specific nomenclature to describe key media objects. These terms appear in both the NSS documentation and in NSS error messages.

For more information, see "NSS Nomenclature" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Comparing NSS with Other File Systems

Because OES 2 supports a variety of file systems, you might want to compare their features and benefits as outlined in the following sections of the *OES 2 SP3: NSS File System Administration Guide for Linux*:

- **NSS Linux vs. NSS NetWare:** "Comparison of NSS on NetWare and NSS on Linux"
- **NSS Linux vs. Linux POSIX:** "Comparison of NSS on Linux and NCP Volumes on Linux POSIX File Systems"

NSS and Storage Devices

NSS supports both physical devices (such as hard disks) and virtual devices (such as software RAIDs and iSCSI devices).

For more information on the various devices that NSS supports, see "Managing Devices" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

14.1.4 Storage Basics by Platform

The following sections summarize storage basics for Linux and NetWare.

- "Linux and File Systems" on page 130
- "NetWare Directories" on page 130
- "NetWare Storage Devices" on page 130

Linux and File Systems

For a high-level overview of the file system on Linux, including the root (/) directory, mount points, standard folders, and case sensitivity, see "Understanding Directory Structures in Linux POSIX File Systems" in the *OES 2 SP3: File Systems Management Guide*.

NetWare Directories

NetWare uses volumes and directories (or folders) to organize data. NetWare file systems support directory paths, fake root directories, Directory Map objects, and drive mappings.

For more information, see "Understanding Directory Structures for the NSS File System" in the *OES 2 SP3: File Systems Management Guide*.

NetWare Storage Devices

NetWare lets you use many different kinds of storage devices, including server disks, single storage devices, arrays of storage devices, and virtual storage devices.

To understand how NetWare connects with and uses storage devices, see "Overview of Server Disks and Storage Devices for NetWare" in the *NW6.5 SP8: Server Disks and Storage Devices*.

14.1.5 Storage Options

The following sections summarize OES storage options.

- "Dynamic Storage Technology" on page 130
- "Direct-Attached Storage Options (NSS and Traditional)" on page 131
- "Advanced Storage Options" on page 131

Dynamic Storage Technology

Dynamic Storage Technology for OES 2 lets you present the files and subdirectories on two separate NSS volumes as though they were on a single, unified NSS volume called a shadow volume.

NCP client users and Samba/CIFS users who access the primary volume see the files and subdirectories from both volumes as if they were all on one volume. All the actions they take—renaming, deleting, moving, etc.—are synchronized by Dynamic Storage Technology across the two volumes.

Unlike the NCP client, backup tools see the volumes separately and can therefore apply one backup policy to the primary and a different backup policy to the secondary volume.

You can use Dynamic Storage Technology to substantially reduce storage costs by placing your less frequently accessed files on less expensive storage media. You can even employ a “move on demand” migration strategy by defining new, more expensive SAN or RAID storage that is initially empty as the primary volume, and then configuring Dynamic Storage Technology so that data is migrated to this primary storage only when it is accessed.

In addition, Dynamic Storage Technology doesn’t suffer the performance penalty that HSM solutions do.

For more information about Dynamic Storage Technology, see the *OES 2 SP3: Dynamic Storage Technology Administration Guide*.

Direct-Attached Storage Options (NSS and Traditional)

As shown in Figure 14-1 on page 128, you can install traditional volumes and Novell Storage System (NSS) volumes on both OES platforms. These devices can be installed within the server or attached directly to the server through an external SCSI bus.

For more information, see “Direct Attached Storage Solutions” in the *OES 2 SP3: Storage and File Services Overview*.

Advanced Storage Options

NSS volumes support the following advanced storage solutions, as documented in the *OES 2 SP3: Storage and File Services Overview*.

- Network Attached Storage Solutions

  A dedicated data server or appliance that provides centralized storage access for users and application servers through the existing network infrastructure and by using traditional LAN protocols such as Ethernet and TCP/IP. When Gigabit Ethernet is used, access speeds are similar to direct attached storage device speeds.

  The disadvantage is that data requests and data compete for network bandwidth.
- Storage Area Network Solutions

  A separate, dedicated data network consisting of servers and storage media that are connected through high-speed interconnects, such as Fibre Channel.
  - iSCSI SAN

    You can create a SAN using Linux iSCSI.
- Fault-Tolerant and High-Availability Architectures

  Use one or more of the following technologies:
  - Multiple Path I/O: The Linux Device Mapper Multipath I/O tool helps prevent failure in the connection between the CPU and the storage device by automatically identifying multiple paths between each Linux server and its storage devices.
  - Software RAIDs: NSS supports software RAIDS to improve storage availability and performance by enhancing data fault tolerance and I/O performance.

    For more information, see “Managing NSS Software RAID Devices” in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
  - Server Clusters: You can configure up to 32 NetWare servers or Linux servers into a high-availability cluster where resources and services are dynamically allocated to any server in the cluster and automatically switched to another server if the hosting server fails.

By manually switching services, IT organizations can maintain and upgrade servers during production hours and eliminate scheduled downtime.

For more information, see the *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide* and the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

14.1.6 NetWare Core Protocol Support (Novell Client Support) on Linux

Many organizations rely on Novell Client software and the NetWare Core Protocol (NCP) for highly secure file storage services.

Novell Storage Services (NSS) volumes are NCP volumes by nature, and you can also define Linux POSIX volumes as NCP volumes. The main difference in access control between NSS volumes and Linux POSIX volumes that are defined as NCP volumes is that NSS extended file and directory attributes are not available on Linux POSIX volumes.

The NCP server for OES 2 lets you attach to Linux POSIX volumes that are defined as NCP volumes using Novell Client software. For more information, see Section 18.6, "NCP Implementation and Maintenance," on page 208.

14.2 Planning OES File Storage

The following sections can help you plan for storage on your OES network:

- Section 14.2.1, "Directory Structures," on page 132
- Section 14.2.2, "File Service Support Considerations," on page 132
- Section 14.2.3, "General Requirements for Data Storage," on page 133
- Section 14.2.4, "OES 2 Storage Planning Considerations," on page 133
- Section 14.2.5, "NSS Planning Considerations," on page 138

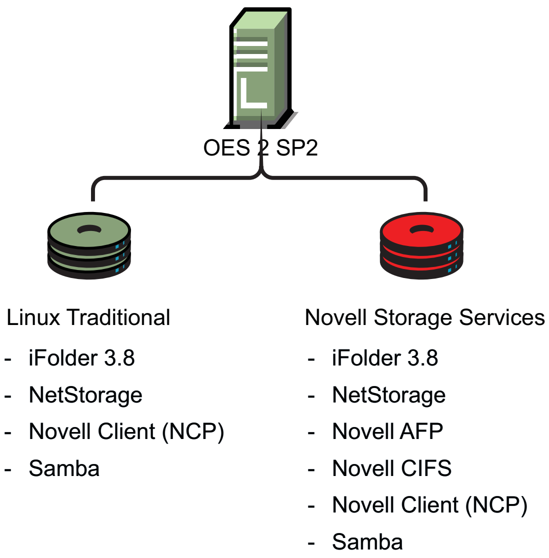
14.2.1 Directory Structures

To plan the directory structures you need on OES 2, see "Understanding Directory Structures in Linux POSIX File Systems" in the *OES 2 SP3: File Systems Management Guide*.

14.2.2 File Service Support Considerations

Figure 14-2 shows which file services can access which volume types.

Figure 14-2 *File Services Supported on Volume Types*



14.2.3 General Requirements for Data Storage

Finding the right storage solution requires you to identify your data storage requirements. You might want to compare your list of requirements against those described in "Storage Solutions" in the *OES 2 SP3: Storage and File Services Overview*.

14.2.4 OES 2 Storage Planning Considerations

Not all data is the same. Not all workloads are the same. Not all file systems are the same. Matching your data and workloads to the available file systems and their capabilities lets you build efficient, scalable, and cost-effective solutions. This section discusses issues to consider when planning your file systems on OES 2 servers, and includes the following topics:

- "The Workgroup Environment" on page 133
- "File System Support" on page 134
- "File Access Protocol Support" on page 136
- "OES 2 Workloads" on page 136

The Workgroup Environment

When selecting a file system, it is important to understand the environment in which it operates. For OES 2, the primary target environment is the workgroup, which requires the following:

- A shared file system for Linux, Macintosh, and Windows desktops. Think of this as a NAS (network-attached storage) for desktops.
- A rich, flexible permissions model to maintain security while providing for the management of many different users with different permissions throughout the file system. The permissions must be granular, allow for delegation of permission management, and ease the administrative burden in an environment where change is constant.
- A robust enterprise-wide identity management system tied into authentication and file system permissions is a must.

- The capabilities for correcting end user mistakes that are made daily (accidental overwrites, deletes, etc.).
- Integration with collaboration tools.
- Data encryption on an individual user or group basis for compliance and security.
- Departmental Web servers and databases.
- SAN support to provide flexible storage management.
- Backup support for both desktop and server data, with rich tools for monitoring the health of the backup system and quickly locating and repairing problems with data protection.
- Regulatory compliance. Regulatory requirements are now pushing new models of protecting and storing employee-generated data that is in LAN systems. It is important to apply correct regulatory requirements only on those users to which they must be applied, and then to produce audits showing compliance.
- Highly available collaboration (e-mail) services, with rich tools to monitor, audit, and trend resource usage.

File System Support

OES 2 offers support for four file systems: Novell Storage Services (NSS), Ext3, Reiser, and XFS. Following is an explanation of each file system and the pros and cons of using them in the workloads supported by OES 2.

- "Novell Storage Services (NSS)" on page 134
- "Ext2" on page 135
- "Ext3" on page 135
- "Reiser" on page 135
- "XFS" on page 135

Novell Storage Services (NSS)

- Supported only through EVMS; not currently supported through LVM.
- Best for shared LAN file serving; excellent scalability in the number of files
- Journaled
- Novell Trustee Model and NSS directory and file attributes (such as Rename Inhibit) provide access control that is much richer than POSIX

The Novell Storage Services file system is used in NetWare 5.0 and above, and most recently is open sourced and included in the SUSE Linux Enterprise Server (SLES) 9 SP1 Linux distribution and later (used in the Novell Open Enterprise Server Linux product).

The NSS file system is unique in many ways, especially in its ability to manage and support shared file services from simultaneous different file access protocols. It is designed to manage access control (using a unique model, called the Novell Trustee Model, that scales to hundreds of thousands of different users accessing the same storage securely) in enterprise file sharing environments.

NSS and its predecessor NWFS are the only file systems that can restrict the visibility of the directory tree based on the user ID accessing the file system. NSS and NWFS have built-in ACL (access control list) rights inheritance. NSS includes mature and robust features tailored for the file-sharing environment of the largest enterprises. The file system also scales to millions of files in a single directory. NSS also supports multiple data streams and rich metadata; its features are a superset of existing file systems on the market for data stream, metadata, name space, and attribute support.

Ext2

- Legacy file system
- Not journaled
- POSIX access control

Ext2 does not maintain a journal, so it is generally not desirable to use it for any server that needs high availability, with one important exception. If the server is running as a Xen VM guest, you should format the `/boot` partition with Ext2 as explained in "Paravitual Mode and Journaling File Systems" (http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_filesystem.html) in the *Virtualization with Xen* (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html) guide.

Ext3

- Most popular Linux file system; limited scalability in size and number of files
- Journaled
- POSIX extended access control

The Ext3 file system is a journaled file system that has the widest use in Linux today. It is regarded by many in the Linux user community as the default Linux file system. It is quite robust and quick, although it does not scale well to large volumes or a great number of files.

A scalability feature has been added called H-trees, which significantly improved Ext3's scalability. However, it is still not as scalable as some of the other file systems. With H-trees, it scales similarly to NTFS. Without H-trees, Ext3 does not handle more than about 5,000 files in a directory.

Reiser

- Best performance and scalability when the number of files is great and/or files are small
- Journaled
- POSIX extended access control

The Reiser file system is the default file system in SUSE Linux distributions. Reiser was designed to remove the scalability and performance limitations that exist in Ext2 and Ext3 file systems.

Reiser scales and performs extremely well on Linux, outscaling Ext3 with H-trees. In addition, Reiser was designed to use disk space very efficiently. As a result, it is the best file system on Linux where there are a great number of small files in the file system. Because collaboration (e-mail) and many Web servings applications have many small files, Reiser is best suited for these types of workloads.

XFS

- Best for extremely large file systems, large files, and lots of files
- Journaled (an asymmetric parallel cluster file system version is also available)
- POSIX extended access controls

The XFS file system is open source and is included in major Linux distributions. It originated from SGI (Irix) and was designed specifically for large files and large volume scalability.

Video and multimedia files are best handled by this file system. Scaling to petabyte volumes, it also handles very large amounts of data. It is one of the few file systems on Linux that supports HSM data migration.

File Access Protocol Support

OES 2 offers support for a variety of file access protocols.

- **AFP:** The Apple Filing Protocol (AFP) is a network protocol that offers file services for Mac OS X and the original Mac OS.
- **CIFS (Novell CIFS and Samba):** The Common Internet File Services (CIFS) protocol is the protocol for Windows networking and file services.

  Novell CIFS is a ported version of the CIFS file service traditionally available only on NetWare but now available for OES 2.

  Samba is an open source software version of CIFS based on extensive use and analysis of the wire protocol of Microsoft Windows machines.
- **FTP:** The File Transfer Protocol (FTP) is one of the most common and widely used simple protocols in the Internet. Virtually all platforms and devices support FTP at some level, but it is a very simple protocol, only allowing for uploading and downloading of files.
- **HTTP:** The Hypertext Transfer Protocol (HTTP) is the dominant protocol on the World Wide Web today, and is the one “spoken” by Web browser clients and Web servers. It is like FTP in being designed strictly for transfers of HTML (Hypertext Markup Language) and additional markup languages that have been invented, such as XML (Extensible Markup Language).
- **NCP:** The NetWare Core Protocol (NCP) is the client server protocol developed by Novell for supporting DOS, Windows, OS/2, Macintosh, UNIX (UnixWare), and Linux for shared file services.

  The NCP Server on Linux includes emulation for the Novell Trustee Model and inheritance plus visibility when it runs on traditional POSIX file systems such as Ext3, Reiser, and XFS. When it runs on NSS on Linux, these capabilities are synchronized with the NSS File system and its extended directory and file attributes, such as Rename Inhibit.

OES 2 Workloads

Each file system has its strengths and weaknesses depending on the workload the file system supports. This section gives some guidelines for picking and building the right file system for a given workload. In determining which file system to use for a particular workload, consider your environment and the following explanation of each workload to determine which file system best meets your workload environment.

Table 14-2 *File System Support per Workload*

Workload Type	NSS File System	Ext3 File System	Reiser File System	XFS File System
File serving – Application server	Supported	Supported	Recommended	Recommended
File serving – end user files	Recommended	Supported	Supported	Supported
Network printing (iPrint)	Recommended	Recommended	Recommended	Recommended
iFolder	Recommended	Supported	Recommended	Recommended
Collaboration (GroupWise)	Recommended	Supported	Recommended	Recommended
Cluster services	Supported	Supported	Supported	Supported
Dynamic Storage Technology	Supported	Not Supported	Not Supported	Not Supported

The following sections provide a brief summary of considerations for each workload listed in Table 14-2.

File Serving (NAS)

Generally there are two types of NAS use cases: Serving files to application servers in a tiered service oriented architecture (SOA), and serving files to end user desktops and workstations. The former has minimal access control requirements. The latter has quite heavy access control requirements.

Typically for serving files to application servers (traditional NAS), you would choose a file system that is scalable and fast. Reiser and XFS would be good choices in this environment. For file serving to end user workstations, the access control and security management capabilities of the NSS file systems with CIFS and NCP file access protocols are important.

The NSS model does better than the other file systems for very large numbers of users. It allows for security between users and also allows for very fine granular sharing between given users and groups. NSS includes a visibility feature implemented in the file system that prevents unauthorized users from even seeing subdirectory structures they don't have rights to access.

Network Printing (iPrint)

iPrint is file system agnostic. There is no noticeable difference in performance or reliability on any of the file systems.

iFolder

Novell iFolder does not depend on a particular file system. Based on the client workload, the file system should be chosen at the server side. Because it mostly serves user data, a file system that can scale with a large number of files is the best suited in most deployments, making Reiser and NSS the best bets. Novell iFolder maintains its own ACL, so having an NSS file system that supports a rich ACL might be redundant.

GroupWise

GroupWise deals with many little files. Because only the application process is accessing the file system, the added overhead of the rich ACL and file attributes found in NSS is redundant. The necessary characteristics are a file system whose performance remains relatively constant regardless of the number of files that are in the volume, and that performs well with small files. Best bets would be ReiserFS, XFS, and NSS. Ext3 does not handle large systems well (where you have more than 10,000 files in the system).

Novell Cluster Services

Although Novell Cluster Services does not depend on a particular file system, you must use the same file systems from node to node. For example, if you are using NSS on one node, you need to use NSS on the failover node as well.

Dynamic Storage Technology

Dynamic Storage Technology does not depend on a particular file system in principle; however, it is currently supported only on NSS volumes.

Novell plans to add support for additional file systems in the future. When that happens, it will be important to remember that file systems cannot be mixed between volumes and shadow volumes. For example, if you choose to shadow an NSS volume, the secondary volume must also be NSS.

14.2.5 NSS Planning Considerations

Consider the following when planning for NSS:

- "Device Size Limit" on page 138
- "Other NSS Planning Topics" on page 138

Device Size Limit

NSS recognizes logical or physical devices up to 2 terabytes (TB) in size. If you have a storage disk larger than 2 TB, use the storage device's management utility to carve the disk into smaller logical devices to use with the NSS file system.

This is especially important to remember when planning for NSS volumes on Linux because the size limit for Linux POSIX volumes is 8 TB.

Other NSS Planning Topics

To plan for NSS volumes—including prerequisites, security considerations, and moving volumes between Linux and NetWare—see "Planning NSS Storage Solutions" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

14.3 Coexistence and Migration of Storage Services

The following sections summarize the coexistence and migration issues related to storage services.

- Section 14.3.1, "MySQL," on page 139
- Section 14.3.2, "OES 2 Options," on page 139
- Section 14.3.3, "NetWare 6.5 SP8 Options," on page 140

14.3.1 MySQL

OES 2 includes the open source MySQL database. When combined with a Web application and a Web server, MySQL is a very reliable and scalable database for use in hosting e-commerce and business-to-business Web applications.

NOTE: The more powerful PostgreSQL database server comes with SUSE Linux Enterprise Server 10.

14.3.2 OES 2 Options

OES 2 provides support for Novell Storage Services (NSS) as well as Linux POSIX file systems.

- "NSS Volumes" on page 139
- "Linux POSIX File Systems" on page 139

NSS Volumes

NSS volumes are cross-compatible between NetWare and Linux.

To use NSS on OES 2, you must have a disk available to be managed by Enterprise Volume Management System (EVMS). The boot partition (such as `/boot` for Grub) and system partition (such as for the swap and system volumes) are managed by Logical Volume Manager 2 (LVM2). Any disk managed by LVM2 cannot be managed by EVMS, which makes the disks where the boot partition and system partition reside unavailable to NSS.

If you have a single-disk server that you want to install OES 2 for Linux on and create an NSS volume, see "Installing with EVMS as the Volume Manager of the System Device" in the *OES 2 SP3: Installation Guide*.

On OES 2, you can use NSS volumes only as data volumes. Configure NSS pools and volumes in iManager or NSSMU after the server installation completes successfully.

Starting with NetWare 6.5 SP4 and OES 2, a new metadata structure provides enhanced support for hard links. After you install or upgrade your operating system, you must upgrade the media format in order to use the new metadata structure; some restrictions apply. For more information, see "Upgrading the NSS Media Format" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

For additional information about coexistence and migration of NSS volumes, as well as access control issues for NSS on Linux, see "Cross-Platform Issues for NSS" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Linux POSIX File Systems

You can install NCP Server for Linux to provide NetWare Core Protocol access to Linux POSIX file systems. This allows users running the Novell Client software to map drives to the Linux file system data, with access controls being enforced by NCP.

For more information on using NCP Server for Linux in OES, see the *OES 2 SP3: NCP Server for Linux Administration Guide*.

Users can access data storage on OES 2 servers through a number of methods. For more information, see "Overview of File Services" on page 183.

14.3.3 NetWare 6.5 SP8 Options

NetWare 6.5 SP8 supports both the NetWare Traditional file system and Novell Storage Services (NSS).

- "NetWare Traditional File System" on page 140
- "NSS Volumes" on page 140

NetWare Traditional File System

After upgrading an older NetWare server to NetWare 6.5 SP8, it is possible for a NetWare Traditional file system volume to still reside on that server. Although you can continue to use Traditional volumes with NetWare 6.5 SP8, you will want to consider upgrading them to NSS to support a data migration to OES 2.

NSS Volumes

NSS volumes are cross-compatible between NetWare and Linux servers. You can mount an NSS data volume on either kernel—Linux or NetWare—and move it between them as long as they both support the same media format. In a clustered SAN, volumes that were originally created on a NetWare server can fail over between kernels, allowing for full data and file system feature preservation when migrating data to Linux.

Supporting NSS volumes in a mixed environment and migrating data between OES platforms presents a number of possibilities for your storage solutions. However, to ensure success you must fully understand the proper methods and limitations involved.

For additional information about coexistence and migration of NSS volumes, as well as access control issues for NSS on Linux, see "Migrating NSS Devices from NetWare 6.5 SP8 to OES 2 Linux" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

14.4 Configuring and Maintaining Storage

- Section 14.4.1, "Managing Directories and Files," on page 140
- Section 14.4.2, "Managing NSS," on page 140
- Section 14.4.3, "Optimizing Storage Performance," on page 142

14.4.1 Managing Directories and Files

To learn about managing directories and files on an OES 2 server, see "Understanding Directory Structures in Linux POSIX File Systems" in the *OES 2 SP3: File Systems Management Guide*.

14.4.2 Managing NSS

Use the links in Table 14-3 to find information on the many management tasks associated with NSS volumes.

***Table 14-3** NSS Management*

Category/Feature	Description	Link
Archive and Version Services	Use Archive and Version Services with NSS volumes to save interval-based copies of files that can be conveniently restored by administrators and users.	*OES 2 SP3: Novell Archive and Version Services 2.1 Administration Guide for Linux*
Compression	Conserve disk space and increase the amount of data a volume can store.	"Managing Compression on NSS Volumes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Console Commands	Manage NSS volumes at an NetWare 6.5 SP8 server console, or an OES 2 terminal console via the NSS Console (`nsscon`) utility.	"NSS Commands" and "NSS Utilities" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Distributed File Services (DFS)	Use DFS junctions to transparently redirect data requests, split volumes while maintaining transparent access, and quickly move volume data to another volume.	*OES 2 SP3: Novell Distributed File Services Administration Guide for Linux*
Encryption	Create and manage encrypted NSS volumes that make data inaccessible to software that circumvents normal access control.	"Managing Encrypted NSS Volumes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
EVMS	Use EVMS, which is required for NSS, to manage volumes on Linux, including the system (root [`/`]) volume if NSS is installed on the same disk.	"Using EVMS to Manage Devices with NSS Volumes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Hard Links	Create multiple names for a single file in the same or multiple directories in an NSS volume.	"Managing Hard Links" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Monitoring	Monitor NSS file systems.	"Monitoring the Status of the NSS File System and Services" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Multipath Support on Linux	Use Linux Device Mapper Multipath I/O tools to manage the dynamic, multiple, redundant connection paths between a Linux server and its external storage devices.	"Managing Multipath I/O to Devices" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Partitions	Manage partitions on NSS volumes.	"Managing Partitions" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Pools	Create and manage NSS pools.	"Managing NSS Pools" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Quotas	Set space restrictions for users and directories to control storage usage.	"Managing Space Quotas for Volumes, Directories, and Users" in the *OES 2 SP3: NSS File System Administration Guide for Linux*

Category/Feature	Description	Link
Salvage subsystem	Use the salvage subsystem to make deleted files and directories available for undelete or purge actions.	"Salvaging and Purging Deleted Volumes, Directories, and Files" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Tools	Learn about the various tools available to manage NSS volumes, the tool capabilities, and how to use them.	"Management Tools for NSS" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Troubleshooting	Troubleshoot NSS on OES 2 and NetWare 6.5 SP8.	"Troubleshooting the NSS File System" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
File System Trustees and Attributes	Control user access to data by setting trustees, trustee rights, and inherited rights filters for files. Control file behavior by setting file and folder attributes.	"Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Volumes	Create and manage NSS volumes in NSS pools.	"Managing NSS Volumes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*

14.4.3 Optimizing Storage Performance

See "Tuning NSS Performance on Linux" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

15 eDirectory, LDAP, and Domain Services for Windows

This section discusses the following topics:

- Section 15.1, “Overview of Directory Services,” on page 143
- Section 15.2, “eDirectory,” on page 144
- Section 15.3, “LDAP (eDirectory),” on page 146
- Section 15.4, “Domain Services for Windows,” on page 146

15.1 Overview of Directory Services

Storing and managing network identities in directory services is a fundamental expectation for networking.

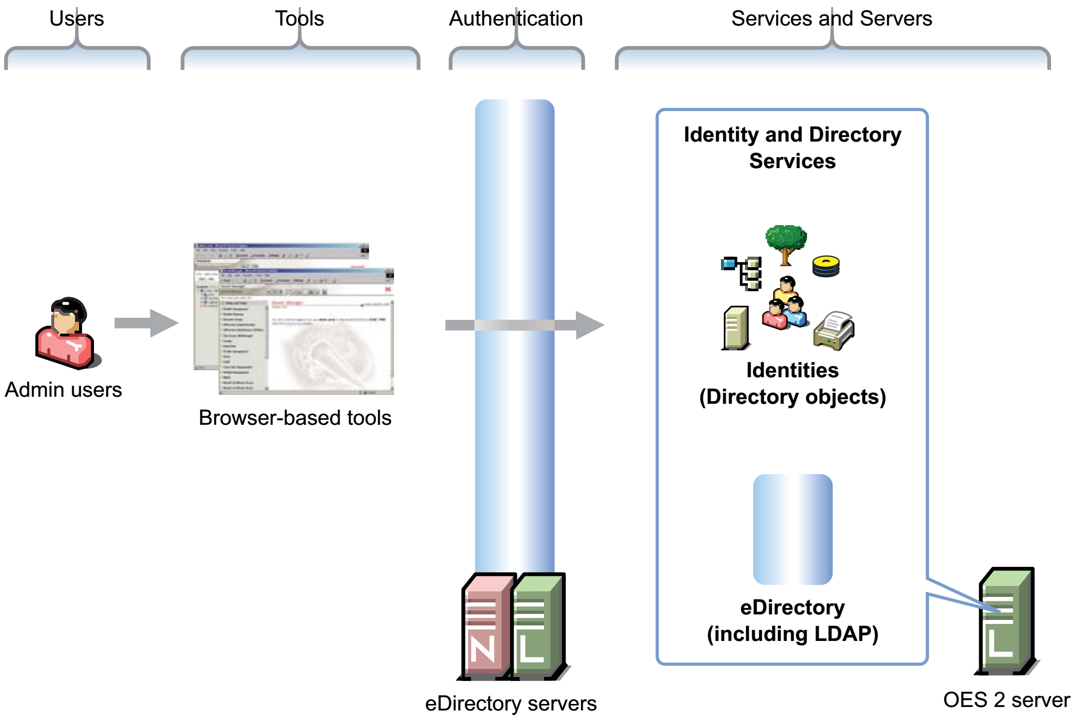
In the simplest terms, Novell eDirectory is a tree structure containing a list of objects (or identities) that represent network resources, such as the following:

- Network users
- Servers
- Printers
- Applications

eDirectory is designed to provide easy, powerful, and flexible management of network resources (including eDirectory itself) in ways that no other directory service can match. You can administer eDirectory through the same browser-based tools on both OES and NetWare.

For more information, see Chapter 15, “eDirectory, LDAP, and Domain Services for Windows,” on page 143.

Figure 15-1 eDirectory Overview



15.2 eDirectory

Novell eDirectory is the central, key component of Novell Open Enterprise Server (OES) and provides the following:

- Centralized identity management
- The underlying infrastructure for managing your network servers and the services they provide
- Access security both within the firewall and from the Web

This section discusses the following tasks:

- Section 15.2.1, "Installing and Managing eDirectory on OES," on page 144
- Section 15.2.2, "Planning Your eDirectory Tree," on page 145
- Section 15.2.3, "eDirectory Coexistence and Migration," on page 145

15.2.1 Installing and Managing eDirectory on OES

The tools you can use to install and manage eDirectory on OES are outlined in the following sections.

- "OES Installation Programs" on page 144
- "iManager" on page 145

OES Installation Programs

OES requires that eDirectory be installed by using the NetWare Install or the YaST-based install for OES.

IMPORTANT: Other utilities, such as ndsconfig and ndsmanage, are not supported for installing or removing eDirectory on OES servers, unless explicitly called for in OES-specific instructions.

iManager

iManager is the OES eDirectory management tool and is used for all eDirectory management and most OES component management tasks, including the following:

- Creating eDirectory objects, including User and Group objects
- Managing eDirectory objects
- Configuring and managing OES service component controls in eDirectory
- Accessing other OES component management tools

For information on using iManager, see the *Novell iManager 2.7.6 Administration Guide*.

15.2.2 Planning Your eDirectory Tree

If you don't have eDirectory installed on your network, it is critical that you and your organization take time to plan and design your eDirectory tree prior to installing OES.

For those who are new to eDirectory, the *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare* provides an introduction to eDirectory planning that you might find useful for getting started with eDirectory.

For detailed information on getting started using eDirectory, see "Designing Your Novell eDirectory Network" in the *Novell eDirectory 8.8 SP7 Installation Guide*.

To learn what's new in eDirectory 8.8, see the *Novell eDirectory 8.8 SP7 What&apos;s New Guide*.

15.2.3 eDirectory Coexistence and Migration

Novell Directory Services (NDS) was introduced with NetWare 4.0. The successor to NDS, Novell eDirectory, is also available for Microsoft Windows, Red Hat*, and SUSE versions of Linux, as well as various flavors of UNIX (Solaris*, AIX*, and HP-UX*).

As eDirectory has evolved, backward compatibility issues have arisen. For example, moving from NetWare 4.*x* to 5.*x* involved not only upgrading NDS, but also moving from IPX to TCP/IP. This transition brought significant changes to the core schema and security-related components. Novell has consistently provided the migration tools and support required to migrate to new eDirectory versions.

OES 2 includes eDirectory 8.8. For those upgrading an existing NetWare 6.5 SP6 server, eDirectory 8.7.3 is still available. New NetWare installations require eDirectory version 8.8.

For complete coexistence and migration information and instructions, see "Migrating to eDirectory 8.8 SP7 " in the *Novell eDirectory 8.8 SP7 Installation Guide*.

15.3 LDAP (eDirectory)

This section contains information about LDAP support in OES.

15.3.1 Overview of eDirectory LDAP Services

Lightweight Directory Access Protocol (LDAP) Services for Novell eDirectory is a server application that lets LDAP clients access information stored in eDirectory.

Most OES 2 services leverage the LDAP server for eDirectory for authentication, as illustrated in the service overviews in this guide.

15.3.2 Planning eDirectory LDAP Services

LDAP for eDirectory provides LDAP authentication for the objects stored in eDirectory. As you plan your eDirectory tree, be sure you understand the information in "Understanding LDAP Services for Novell eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

15.3.3 Migration of eDirectory LDAP Services

If you have users in an OpenLDAP database and you want to migrate them to eDirectory, you can use the Novell Import Conversion Export (ICE) utility. For more information, see "Novell eDirectory Management Utilities" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

15.3.4 eDirectory LDAP Implementation Suggestions

For help with setting up and using LDAP for eDirectory, refer to "Configuring LDAP Services for Novell eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

15.4 Domain Services for Windows

Novell Domain Services for Windows (DSfW) allows eDirectory users on Windows workstations to access storage on both OES servers and Windows servers through native Windows and Active Directory authentication and file service protocols.

DSfW enables companies with Active Directory and Novell eDirectory deployments to achieve better coexistence between the two platforms.

- Users can work in a pure Windows desktop environment and still take advantage of some OES back-end services and technology, without the need for a Novell Client™ or even a matching local user account on the Windows workstation.
- Network administrators can use Microsoft Management Console (MMC) to administer users and groups within the DSfW domain, including their access rights to Samba-enabled storage on OES servers.

This section discusses the following:

- Section 15.4.1, "Graphical Overview of DSfW," on page 147
- Section 15.4.2, "Planning Your DSfW Implementation," on page 150
- Section 15.4.3, "Implementing DSfW on Your Network," on page 150

15.4.1 Graphical Overview of DSfW

- "File Access" on page 147
- "User Management" on page 148
- "Storage Management" on page 149

File Access

Figure 15-2 *DSfW File Access Overview*

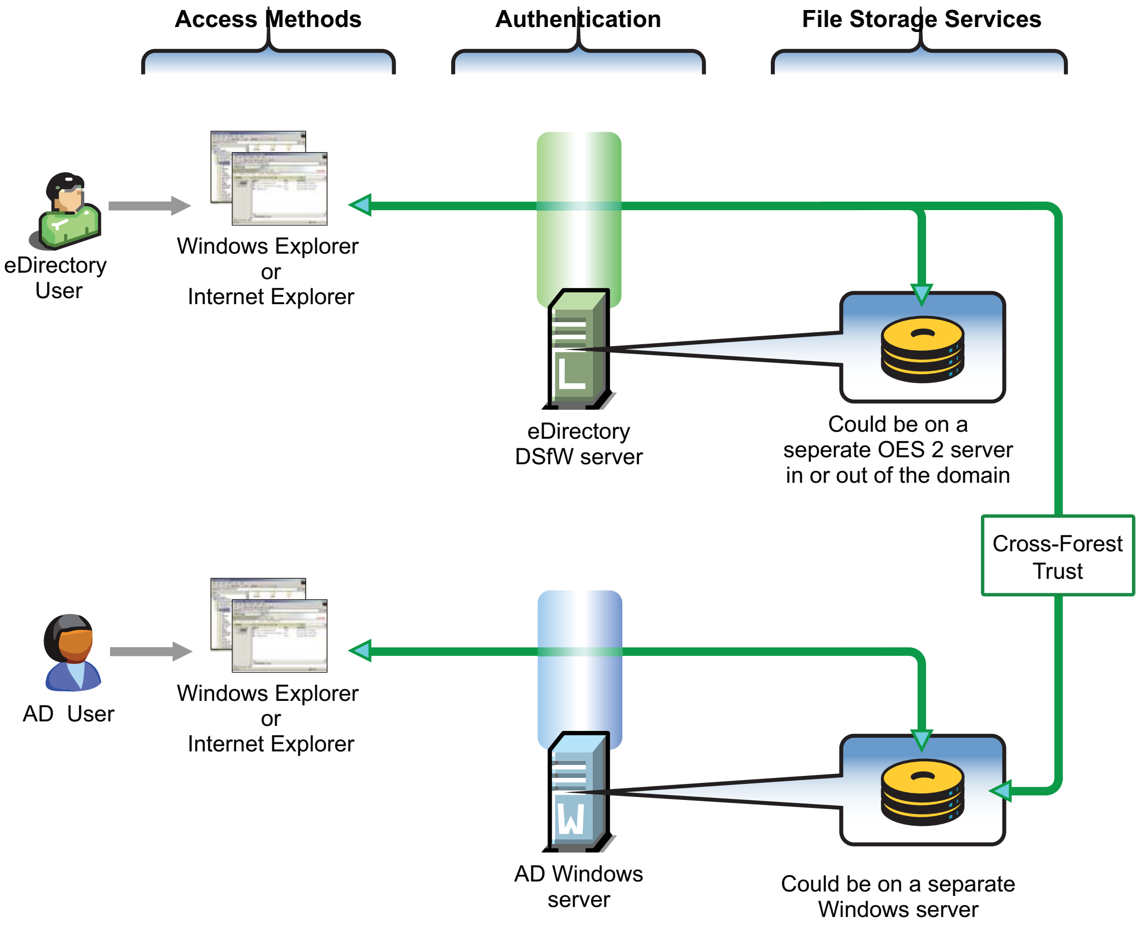

Access Methods
Authentication
File Storage Services
eDirectory User
Windows Explorer or Internet Explorer
eDirectory DSfW server
Could be on a seperate OES 2 server in or out of the domain
Cross-Forest Trust
AD User
Windows Explorer or Internet Explorer
AD Windows server
Could be on a separate Windows server

Table 15-1 DSfW File Access

Access Methods	Authentication	File Storage Services
eDirectory and Active Directory users on Windows workstations can access files through Windows Explorer (CIFS) or Internet Explorer (WebDAV Web Folders). No Novell Client can be on the machine. Unlike Windows workgroup or Novell Samba, the user doesn't need to have a matching username and password on the local workstation. Although not shown, Novell Client users can also access files through a normal NCP connection.	For eDirectory users, file service access is controlled by authentication through the eDirectory server using common Windows authentication protocols, including Kerberos, NTLM, and SSL/TLS. For AD users, file service access is controlled by authentication through the AD server.	On OES 2 servers, file storage services are provided by Samba to NSS or traditional Linux file systems. For eDirectory users, access to storage on Windows servers is available through a cross-forest trust. Access rights are granted by the AD administrator following the establishment of the cross-forest trust.

User Management

Figure 15-3 DSfW User Management Overview

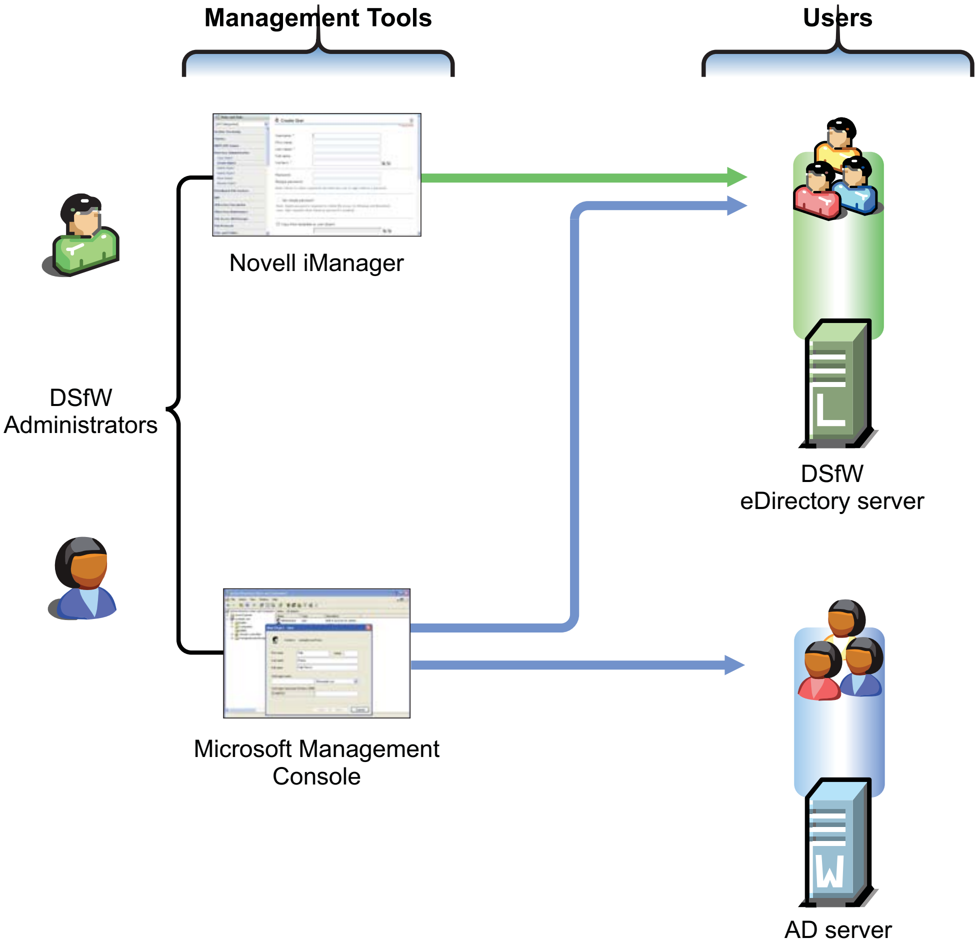


Table 15-2 DSfW User Management

Management Tools	Users
iManager manages DSfW users like other eDirectory users.	DSfW users must have the Default Domain Password policy assigned and a valid Universal Password.
MMC manages both AD users and DSfW users as though they were AD users.	DSfW users are automatically enabled for Samba and LUM.

Storage Management

Figure 15-4 DSfW Storage Management Overview

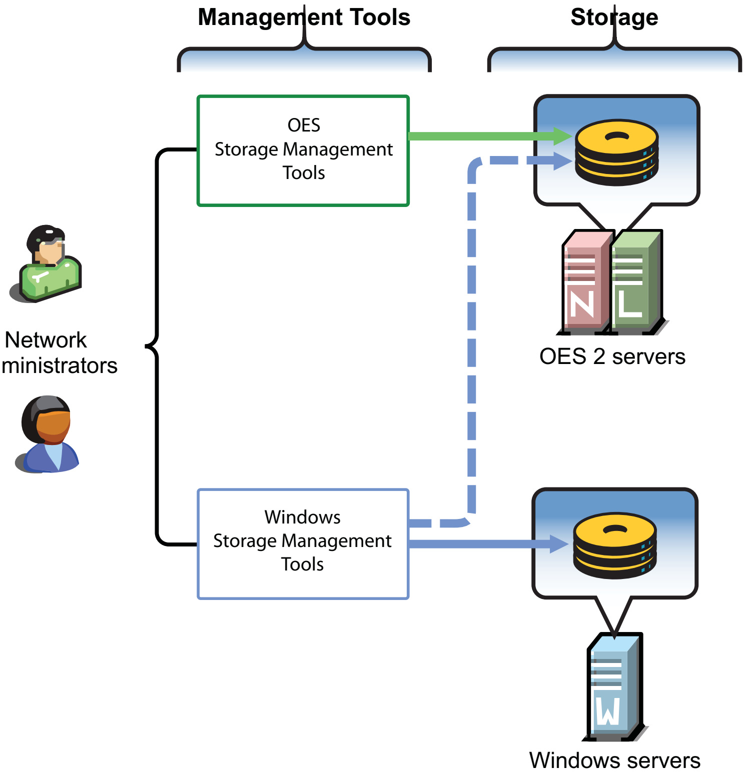


Table 15-3 *DSfW Storage Management*

Management Tools	Storage
Network administrators use native OES and Windows storage management tools to create and manage storage devices on OES and Windows servers, respectively. Windows management tools can also manage share access rights and POSIX file system rights on DSfW storage devices after the shares are created. They cannot create the shares or perform other device management tasks.	Storage devices on OES 2 servers can be either NSS or traditional Linux volumes. Samba management standards apply to both volume types.

15.4.2 Planning Your DSfW Implementation

For planning information, see the *OES 2 SP3: Domain Services for Windows Administration Guide*.

15.4.3 Implementing DSfW on Your Network

This section highlights some of the potential caveats to consider when installing DSfW. For complete information, see the *OES 2 SP3: Domain Services for Windows Administration Guide*, especially the "Troubleshooting DSfW" section.

- "Universal Password in a Name-Mapped Scenario" on page 150
- "DSfW Must Be Installed at the Root of an eDirectory Partition" on page 150
- "Hierarchical Placement of Users in the eDirectory Tree" on page 151
- "OES 2 Service Limitations" on page 151
- "Domain and Container Names Must Match" on page 151
- "Install DSfW on a New OES 2 Server When Possible" on page 151
- "DNS Configuration" on page 151

Universal Password in a Name-Mapped Scenario

If you install DSfW into an existing tree and your users don't currently have a Universal Password policy assigned, they won't be able to log in without the Novell Client until the Universal Password has been set.

Therefore, you should consider implementing Universal Password and giving users an opportunity to log into the network before installing DSfW. Logging in after a password policy is in place creates a Universal Password for users so that their transition to DSfW is seamless.

DSfW Must Be Installed at the Root of an eDirectory Partition

You must install DSfW in the root container or an eDirectory partition, either one that currently exists or one that you create for DSfW. In both cases, the first DSfW server installed in the partition becomes the master of the partition.

Hierarchical Placement of Users in the eDirectory Tree

DSfW users must reside in the same eDirectory partition where DSfW is installed, either in the same container or in a container below it in the hierarchy. Therefore, DSfW should be installed high enough in the eDirectory tree that it encompasses all of the users that you want to enable for DSfW access.

OES 2 Service Limitations

Only designated OES 2 services can be installed on a DSfW server. For more information, see "Unsupported Service Combinations" in the *OES 2 SP3: Domain Services for Windows Administration Guide*.

Domain and Container Names Must Match

When you install DSfW, the Domain name you specify must match the name of the container you are installing into. For more information, see "Container is Partitioned" in the *OES 2 SP3: Domain Services for Windows Administration Guide*.

Install DSfW on a New OES 2 Server When Possible

Because of the service limitations mentioned in OES 2 Service Limitations, Novell strongly recommends that you install DSfW on a new server.

DNS Configuration

As you set up DNS, observe the following guidelines:

- **First DSfW Server (FRD):** This should point to itself as the primary DNS server, and to the network DNS server as the secondary DNS server (if applicable).
- **Subsequent DSfW Servers:** These must point to the FRD as their primary DNS server and optionally to the network DNS server as their secondary DNS server.
- **DSfW Workstations:** These must be able to resolve the FRD of the DSfW forest. For example, you might configure workstations to point to the FRD as their primary DNS server and to the network DNS server secondarily. Or if the network DNS server is configured to forward requests to the DSfW server, then workstations could point to it as their primary DNS server.

16 Users and Groups

Networks exist to serve users and groups of users. Open Enterprise Server 2 provides strong user and group management through eDirectory and its associated technologies.

16.1 Creating Users and Groups

All OES 2 services require that you create User objects to represent the users on your system. The Linux User Management (LUM) and Samba components on OES 2 also require that you create a LUM-enabled Group object that you can assign the users to.

In addition to these basic objects, it is usually helpful to organize your tree structure by using Organizational Unit objects to represent the structure of your organization and to serve as container objects to help manage the users, groups, servers, printers, and other organization resources you can manage through eDirectory.

The *Lab Guide for OES 2* provides basic instructions for creating container objects as well as Group and User objects in eDirectory.

For more information about Samba, see Creating eDirectory Users for Samba in the *OES2 SP3: Samba Administration Guide*.

For detailed information on understanding, creating, and managing the various objects your organization might require, see the *Novell eDirectory 8.8 SP7 Administration Guide*.

16.2 Linux User Management: Access to Linux for eDirectory Users

Users and groups on NetWare servers are created in and managed through eDirectory; users and groups on Linux servers are usually created locally and managed according to the POSIX (Portable Operating System Interface) standard.

Because Open Enterprise Server provides services running on both Linux and NetWare, Novell has developed a technology that lets eDirectory users also function as "local" POSIX users on Linux servers. This technology is called Linux User Management or LUM.

The following sections outline the basic principles involved in Novell LUM and cover the following topics:

- Section 16.2.1, "Overview," on page 154
- Section 16.2.2, "LUM Changes in SP3," on page 159
- Section 16.2.3, "Planning," on page 159
- Section 16.2.4, "LUM Implementation Suggestions," on page 160

16.2.1 Overview

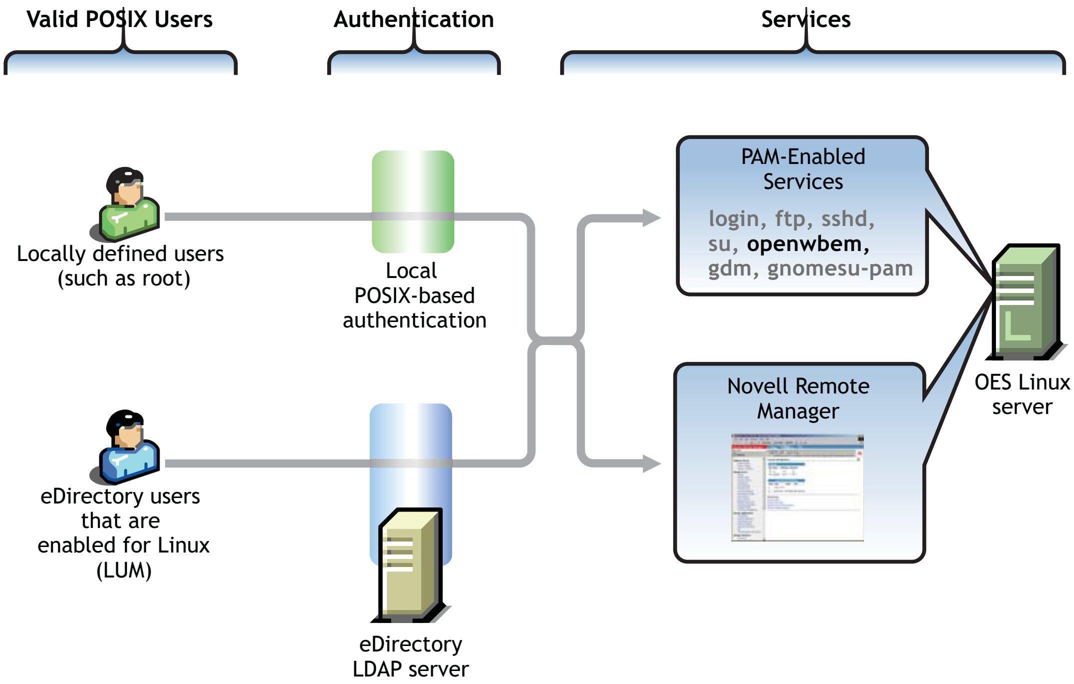
The topics in this section are designed to help you understand when LUM-enabled access is required so that your network services are accessible and work as expected. For more information about Linux User Management, see "Overview" in the *OES 2 SP3: Novell Linux User Management Administration Guide*.

- "A Graphical Preview of Linux User Management" on page 154
- "Linux Requires POSIX Users" on page 155
- "Linux Users Can Be Local or Remote" on page 156
- "The root User Is Never LUM-Enabled" on page 156
- "About Service Access on OES 2" on page 156
- "Services in OES 2 That Require LUM-Enabled Access" on page 156
- "Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements" on page 158
- "Services That Do Not Require LUM-enabled Access" on page 158
- "LUM-Enabling Does Not Provide Global Access to ALL OES 2 Servers" on page 159

A Graphical Preview of Linux User Management

Figure 16-1 illustrates how Linux User Management controls access to the OES 2 server.

Figure 16-1 LUM Provides POSIX Access for eDirectory Users


Valid POSIX Users
Authentication
Services
Locally defined users (such as root)
Local POSIX-based authentication
PAM-Enabled Services
login, ftp, sshd, su, openwbem, gdm, gnomesu-pam
OES Linux server
Novell Remote Manager
eDirectory users that are enabled for Linux (LUM)
eDirectory LDAP server

The following table explains the information presented in Figure 16-1.

Table 16-1 Linux User Management

Valid POSIX Users	Authentication	eDirectory Authenticated Services
Some services on OES 2 servers must be accessed by POSIX users. eDirectory users can function as POSIX users if they are enabled for Linux access (LUM).	When the system receives an action request, it can authenticate both local POSIX users and users who have been enabled for Linux access.	Users can potentially access PAM-enabled services, Samba shares, and Novell Remote Manager as either local or eDirectory users. By default, only the `openwbem` command (required for server management) is enabled for eDirectory access.

Linux Requires POSIX Users

Linux requires that all users be defined by standard POSIX attributes, such as username, user ID (UID), primary group ID (GID), password, and other similar attributes.

Linux Users Can Be Local or Remote

Users that access a Linux server can be created in two ways:

- **Locally (on the server):** Local users are managed at a command prompt (using commands such as `useradd`) or in YaST. (See the useradd(8) man page and the YaST online help for more information.) These local users are stored in the `/etc/passwd` file. (See the passwd(5) man page for more information.)

  IMPORTANT: As a general rule on OES 2 servers, the only local user account that should exist is `root`. All other user accounts should be created in eDirectory and then be enabled for Linux access (LUM). You should never create duplicate local and eDirectory user accounts.

  For more information, see Section 7.2, "Avoiding POSIX and eDirectory Duplications," on page 64.

- **Remotely (off the server):** Remote users can be managed by other systems, such as LDAP-compliant directory services. Remote user access is enabled through the Pluggable Authentication Module (PAM) architecture on Linux.

The Linux POSIX-compliant interfaces can authenticate both kinds of users, independent of where they are stored and how they are managed.

The root User Is Never LUM-Enabled

The OES 2 user management tools prevent you from creating an eDirectory user named `root`, thus replacing the `root` user on an OES 2 server. If `root` were to be a LUM user and eDirectory became unavailable for some reason, there would be no root access to the system.

Even if eDirectory is not available, you can still log into the server through Novell Remote Manager and perform other system management tasks as the `root` user.

About Service Access on OES 2

Novell Linux User Management (LUM) lets you use eDirectory to centrally manage remote users for access to one or more OES 2 servers.

In other words, LUM lets eDirectory users function as local (POSIX) users on an OES 2 server. Access is enabled by leveraging the Linux Pluggable Authentication Module (PAM) architecture. PAM makes it possible for eDirectory users to authenticate with the OES 2 server through LDAP.

In OES, the terms *LUM-enabling* and *Linux-enabling* are both used to describe the process that adds standard Linux (POSIX) attributes and values to eDirectory users and groups, thus enabling them to function as POSIX users and groups on the server.

You can use iManager to enable eDirectory users for Linux. For instructions, see "About Enabling eDirectory Users for Linux Access" on page 160.

Services in OES 2 That Require LUM-Enabled Access

Some services on an OES 2 server require that eDirectory users be LUM-enabled:

- **Novell Samba (CIFS) Shares on the Server:** Windows workgroup users who need access to Samba shares defined on the server must be LUM-enabled eDirectory users who are configured to access the server. This is because Samba requires POSIX identification for access.

By extension, NetStorage users who need access to Samba (CIFS) Storage Location objects that point to the server must also be LUM-enabled eDirectory users with access to the server.

NOTE: Although Samba users must be enabled for LUM, Samba is not a PAM-enabled service. Logging in to the OES 2 server through Samba does not create a home directory.

- **Core Linux Utilities Enabled for LUM:** These are the core utilities and other shell commands that you can specify during the OES install to be enabled for authentication through eDirectory LDAP. In Linux, these are known as PAM-enabled utilities.

IMPORTANT: Before you accept the default PAM-enabled service settings, be sure you understand the security implications explained in Section 22.2.2, "User Restrictions: Some OES 2 Limitations," on page 229.

The core utilities available for LUM-enablement are summarized in Table 16-2.

***Table 16-2** PAM-enabled Services Controlled by LUM*

Command	Where Executed	Task
`ftp`	Another host	Transfer files to and from the OES 2 server which, in this case, is a remote host.
`login`	◆ OES 2 server ◆ SSH session with OES 2 server	Log in to the OES 2 server, either directly or in an SSH session with the server.
`openwbem`	Local host	Required for iPrint, NSS, SMS, Novell Remote Manager, and iManager.
`gdm`	◆ Local host ◆ Remote host	Run and manage the X servers using XDMCP.
`gnomesu-pam`	Local host	Required for GNOME applications that need superuser access.
`sshd`	Another host	Establish a secure encrypted connection with the OES 2 server which, in this case, is a remote host.
`su`	◆ OES 2 server ◆ SSH session with OES 2 server	Temporarily become another user. This is most often used to temporarily become the `root` user, who is not a LUM user and is, therefore, not affected by LUM.

NOTE: Logging in to the OES 2 server through a PAM-enabled service for the first time causes the creation of a home directory on the server.

- **Novell Remote Manager on Linux:** You can access Novell Remote Manager as the following:
  - The `root` user with rights to see everything on the Linux server.
  - A local Linux user with access governed by POSIX access rights. (Having local users in addition to `root` is not recommended on OES 2 servers.)
  - A LUM-enabled eDirectory user, such as the Admin user created during the install.
- **Novell Storage Management Services (SMS) on Linux:** You can access SMS utilities as
  - The `root` user with rights to see everything on the Linux server.

- A local Linux user with access governed by POSIX access rights. (Having local users in addition to `root` is not recommended on OES 2 servers.)
- A LUM-enabled eDirectory user, such as the Admin user created during the install.

Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements

Some services do not require eDirectory users to be LUM-enabled for service access:

- **NetStorage:** NetStorage users don't generally need to be LUM-enabled. However, salvaging and purging files through NetStorage on an NSS volume can only be done by users who are enabled for Linux.

  IMPORTANT: Files that are uploaded by non-LUM users via NetStorage are owned, from a POSIX perspective, by the `root` user. The assumption is that such users are accessing their data on NSS or NCP volumes by using an NCP storage location object. In both cases, the Novell Trustee Model applies and POSIX ownership is irrelevant.

  If non-LUM NetStorage users are later enabled for Samba access (which includes LUM-enabling) and begin using Samba as a file service, their NetStorage uploaded files are not accessible through Samba until you change POSIX file ownership. Although the Novell implementation of Samba leverages eDirectory for authentication, Samba file and directory access is always controlled by POSIX. The Novell Trustee Model doesn't apply to Samba.

  Both Novell trustee assignments and POSIX file ownership are tracked correctly after users are LUM-enabled.

  Although NetStorage doesn't require LUM-enabled access, the service itself runs as a POSIX-compliant system User (initially a local user on the OES 2 server) who functions on behalf of the end users that are accessing the service.

  If NetStorage must access NSS volumes, this local system user must be moved to eDirectory and LUM-enabled because only eDirectory users can access NSS volumes. The OES 2 installation program configures this correctly by default.

  For more information, see Appendix I, "System User and Group Management in OES 2 SP3," on page 269.
- **NSS:** eDirectory users that access NSS volumes directly through NCP (the Novell Client) are not required to be LUM-enabled.

  However, because Novell Samba accesses NSS through the virtual file system layer that makes NSS appear to be a POSIX-compliant file system, Samba users must be LUM–enabled to access an NSS volume.

Services That Do Not Require LUM-enabled Access

The following end user services do not require LUM-enabled access:

- iFolder 3.8
- iPrint
- NCP Client to an NCP Volume
- NCP Client to an NSS Volume
- Novell AFP

- Novell CIFS
- QuickFinder

LUM-Enabling Does Not Provide Global Access to ALL OES 2 Servers

As you plan to LUM-enable users for access to the services that require it, keep in mind that each OES 2 server being accessed must be associated with a LUM-enabled group that the accessing users belong to.

In other words, it is not sufficient to LUM-enable users for access to a single OES 2 server if they need access to multiple servers. An association between the LUM-enabled groups that the users belong to and the eDirectory UNIX Workstation object associated with the server must be formed by using iManager for each server the users need access to. This can be accomplished for multiple servers by using the process described in "Enabling Users to Access Multiple OES 2 Servers" on page 160.

For more information on LUM, see the *OES 2 SP3: Novell Linux User Management Administration Guide*.

16.2.2 LUM Changes in SP3

In reponse to customer requests for improved LDAP performance, persistent searching for new Linux-enabled users and groups has been disabled in OES 2 SP3.

For more information, see Section 7.11, "LUM Cache Refresh No Longer Persistent," on page 70 and "What's New" in the *OES 2 SP3: Novell Linux User Management Administration Guide*.

16.2.3 Planning

The following sections summarize LUM planning considerations.

- "eDirectory Admin User Is Automatically Enabled for Linux Access" on page 159
- "Planning Which Users to Enable for Access" on page 159
- "Be Aware of System-Created Users and Groups" on page 160

eDirectory Admin User Is Automatically Enabled for Linux Access

When you install Linux User Management on an OES 2 server, the Admin User object that installs LUM is automatically enabled for eDirectory LDAP authentication to the server.

Planning Which Users to Enable for Access

You need to identify the eDirectory users (and groups) who need access to services on OES 2 servers that require LUM-enabled users.

This can be easily determined by doing the following:

1. Review the information in "Services in OES 2 That Require LUM-Enabled Access" on page 156.
2. Identify the servers that will run the services mentioned.
3. On your planning sheets, note the users and groups that you need to enable and the servers you need to enable them to access.

Be Aware of System-Created Users and Groups

You should also be aware of the system-created users and groups that are LUM-enabled when NSS is installed. For more information, see Appendix I, "System User and Group Management in OES 2 SP3," on page 269.

16.2.4 LUM Implementation Suggestions

The following sections summarize LUM implementation considerations.

- "About Enabling eDirectory Users for Linux Access" on page 160
- ""UNIX Workstation" and "Linux Workstation" Are the Same Thing" on page 160
- "Enabling Users to Access Multiple OES 2 Servers" on page 160
- "Enabling eDirectory Groups for Linux Access" on page 161
- "Enabling eDirectory Users for Linux Access" on page 161

About Enabling eDirectory Users for Linux Access

You can enable eDirectory users for Linux User Management by using either iManager 2.7 or the `nambulkadd` command.

- **iManager:** You can enable existing eDirectory users for Linux access by using the Linux User Management tasks in iManager.

  You can enable multiple users in the same operation as long as they can be assigned to the same primary LUM-enabled group. The enabling process lets you associate the group with one or more OES 2 servers or Linux workstations. For more information, see "Enabling Users to Access Multiple OES 2 Servers" on page 160.

  Samba users are also enabled for Linux access as part of the Samba-enabling process.

- **nambulkadd:** If you have eDirectory users and groups that need to be enabled for Linux access, you can use the `nambulkadd` command to modify multiple objects simultaneously. For more information, see the *OES 2 SP3: Novell Linux User Management Administration Guide*.

"UNIX Workstation" and "Linux Workstation" Are the Same Thing

When you use iManager to manage OES 2 access, you might notice some inconsistencies in naming.

When OES 2 servers are created, a "UNIX Workstation - *server_name*" object is created in eDirectory, where *server_name* is the DNS name of the OES 2 server. In some places the iManager help refers to these server objects as "Linux Workstation" objects.

Both "UNIX Workstation" and "Linux Workstation" refer to the same eDirectory objects.

Enabling Users to Access Multiple OES 2 Servers

IMPORTANT: Users gain server access through their LUM-enabled group assignment rather than through a direct assignment to the UNIX Workstation objects themselves.

You can enable users for access to multiple OES 2 servers by associating the LUM-enabled groups to which the users belong with the UNIX Workstation objects you want users to have access to.

Enabling eDirectory Groups for Linux Access

There are two methods for enabling eDirectory groups for Linux access:

- "Using iManager" on page 161
- "Using LUM Utilities at the Command Prompt" on page 161

Using iManager

The following steps assume that the eDirectory Group objects already exist and that any User objects you want to enable for Linux also exist and have been assigned to the groups.

1. Log in to iManager as the eDirectory Admin user or equivalent.
2. Click *Linux User Management* > *Enable Groups for Linux*.
3. Browse to and select one or more Group objects, then click *OK*.
4. If you want all users assigned to the group to be enabled for Linux, make sure the *Linux-Enable All Users in These Groups* option is selected.
5. Click *Next* twice.
6. Browse to and select one or more UNIX Workstation (OES 2 server) objects, then click *OK*.
7. Click *Next*, click *Finish*, then click *OK*.

Using LUM Utilities at the Command Prompt

Novell Linux User Management includes utilities for creating new LUM-enabled groups, and for enabling existing eDirectory groups for Linux access.

- The nambulkadd utility lets you use a text editor to create a list of groups you want enabled for Linux access. For more information, see "nambulkadd" in the OES 2 SP3: Novell Linux User Management Administration Guide.

  IMPORTANT: Be sure to include a blank line at the end of each text file. Otherwise, the last line of the file won't be processed properly.

- The namgroupadd utility lets you create a new LUM-enabled group or enable an existing eDirectory group for Linux access. For more information, see "namgroupadd" in the OES 2 SP3: Novell Linux User Management Administration Guide.

Enabling eDirectory Users for Linux Access

There are two methods for enabling eDirectory users for Linux access:

- "Using iManager" on page 161
- "Using LUM Utilities at the Command Prompt" on page 162

Using iManager

The following steps assume that the eDirectory User objects already exist.

1. Log in to iManager as the eDirectory Admin user or equivalent.
2. Click *Linux User Management* > *Enable Users for Linux*.
3. Browse to and select one or more User objects, then click *OK*.
4. Click *Next*.

5 As indicated, you can do the following:

- Select and enable an existing eDirectory group for Linux.
- Select an eDirectory group that is already enabled for Linux.
- Specify the name and context of a new eDirectory group to create and enable for Linux.

Select the option that matches your requirements.

6 Click *Next*.

7 Browse to and select one or more UNIX Workstation (OES 2 server) objects, then click *OK*.

8 Click *Next*, click *Finish*, then click *OK*.

Using LUM Utilities at the Command Prompt

Novell Linux User Management includes utilities for creating new LUM-enabled users, and for enabling existing eDirectory users for Linux access.

- The nambulkadd utility lets you use a text editor to create a list of users you want enabled for Linux access. For more information, see "nambulkadd" in the OES 2 SP3: Novell Linux User Management Administration Guide.

IMPORTANT: Be sure to include a blank line at the end of each text file. Otherwise, the last line of the file won't be processed properly.

- The namuseradd utility lets you create a single LUM-enabled user or enable an existing eDirectory user for Linux access. For more information, see "namuseradd" in the OES 2 SP3: Novell Linux User Management Administration Guide.

16.3 Identity Management Services

Providing network users with a network identity is a fundamental expectation for networking, but it can also become confusing when users need to track multiple identities to use network services. When you add the traditional POSIX users found on Linux systems to the mix, the picture becomes even more complex.

The identity management services provided by Novell Open Enterprise Server (OES) leverage Novell eDirectory to simplify and customize identity management to fit your needs:

- If you currently store and manage all your users and groups in eDirectory, you can continue to do so.
- If you use Novell Client software to provide network file and print services, you can now provide seamless file and print access to OES 2 servers by using the NCP server for Linux and iPrint services. For more information, see Section 18.6, "NCP Implementation and Maintenance," on page 208 and Chapter 20, "Print Services," on page 217.
- If you want eDirectory users to have access to OES 2 services that require POSIX authentication, you can enable the users for Linux access. For more information, see Section 16.2, "Linux User Management: Access to Linux for eDirectory Users," on page 153.
- If you need to store and manage users in multiple directories, you can greatly strengthen your organization's security and dramatically decrease your identity management costs by deploying Novell Identity Manager. For more information, see Section 16.4, "Using the Identity Manager 3.6.1 Bundle Edition," on page 163.

16.4 Using the Identity Manager 3.6.1 Bundle Edition

Novell Identity Manager is a data-sharing solution that leverages the Identity Vault to synchronize, transform, and distribute information across applications, databases, and directories.

The Identity Manager Bundle Edition provides licensed synchronization of information (including passwords) held in Active Directory Domains and eDirectory systems. When data from one system changes, Identity Manager detects and propagates these changes to other connected systems based on the business policies you define.

In this document:

- Section 16.4.1, "What Am I Entitled to Use?," on page 163
- Section 16.4.2, "System Requirements," on page 163
- Section 16.4.3, "Installation Considerations," on page 163
- Section 16.4.4, "Getting Started," on page 164
- Section 16.4.5, "Activating the Bundle Edition," on page 164

16.4.1 What Am I Entitled to Use?

The Bundle Edition allows you to use the Identity Manager engine and the following Identity Manager drivers:

- Identity Manager Driver for eDirectory
- Identity Manager Driver for Active Directory

Other Identity Manager Integration Modules (drivers) are included in the software distribution. You can install and use these additional Integration Modules for 90 days, at which time you must purchase *Novell Identity Manager* and the Integration Modules you want to use.

The User Application and the service drivers (Loopback, Manual Task, and Entitlements) are not included as part of the license agreement for the Bundle Edition. In order to use these Identity Manager components, you must purchase *Identity Manager*.

16.4.2 System Requirements

For the latest Identity Manager system requirements, see the *Identity Manager Installation Guide* (http://www.netiq.com/documentation/idm36/install/data/front.html).

The Bundle Edition does not include Solaris or AIX support. If you would like to run the Metadirectory engine or Integration Modules on these platforms, you must purchase Identity Manager.

16.4.3 Installation Considerations

Novell Identity Manager Bundle Edition contains components that can be installed within your environment on multiple systems and platforms. Depending on your system configuration, you might need to run the installation program several times to install Identity Manager components on the appropriate systems.

In order for the product to be activated, you must install Open Enterprise Server before installing the Identity Manager Bundle Edition. For more information on Activation issues, see "Activating the Bundle Edition" on page 164.

16.4.4 Getting Started

The following sections will help you plan, install, and configure your Identity Manager Bundle Edition.

- Overview (https://www.netiq.com/documentation/idm36/idm_overview/data/front.html)
- Planning Your Implementation (https://www.netiq.com/documentation/idm36/idm_install/data/be59u4z.html)
- Installing Identity Manager (https://www.netiq.com/documentation/idm36/idm_install/data/a7c9ie0.html)
- Installing Active Directory and eDirectory Drivers (http://www.netiq.com/documentation/idm36drivers/index.html)
- Configuring the Identity Manager Drivers for Use with the Remote Loader (https://www.netiq.com/documentation/idm36/idm_remoteloader/data/bs35plh.html)

For information about customizing your implementation:

- Policy Builder and Driver Customization Guide (http://www.novell.com/documentation/idm36/policy/data/bookinfo.html)

16.4.5 Activating the Bundle Edition

If you choose to purchase additional Identity Manager Integration Modules, you need to install the activation credential for those Integration Modules *and* also the credential for *Novell Identity Manager*.

In order to use the Bundle Edition, you must obtain and install an activation credential. Use the following instructions to complete the Bundle Edition activation tasks.

1. Browse to the Identity Manager Bundle Edition Registration (http://download.novell.com/delivery/reg/idm_bundled.jsp) Web site.
2. Enter your OES activation code, then click *Submit*.
3. Do one of the following:
    - Save the Product Activation Credential file.

      or
    - Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard.

      Carefully copy the contents, and make sure that no extra lines or spaces are included. You should begin copying from the first dash (-) of the credential (----BEGIN PRODUCT ACTIVATION CREDENTIAL) through the last dash (-) of the credential (END PRODUCT ACTIVATION CREDENTIAL-----).
4. Open iManager.
5. Choose *Identity Manager* > *Identity Manager Overview*.
6. Select the driver set or browse to a driver set, then click *Next*.
7. On the Identity Manager Overview page, locate the driver set, click the red *Activation required by* link, then click *Install Activation*.
8. Select the driver set where you want to activate an Identity Manager component.
9. Do one of the following:
    - Specify where you saved the Identity Manager Activation Credential, then click *Next*.

or

- Paste the contents of the Identity Manager Activation Credential into the text area, then click *Next*.

10 Click *Finish*.

Frequently Asked Questions about Activation

Do I need to Install Identity Manager on a specific server?

Yes. As a Bundle Edition user, you must install Identity Manager on the server where you installed Open Enterprise Server. In order for activation to work properly, you must install Identity Manager on Linux or NetWare, and create a driver set on that server.

I installed the Bundle Edition on Linux or NetWare, but it's not activated. Why is this?

You must install the Bundle Edition on the server where OES exists. If you install it on a non-OES server, the Bundle Edition cannot activate.

Can I run Identity Manager on a Windows Server?

Not with the Bundle Edition. However, you can still synchronize data held on a Windows server by using the Identity Manager Remote Loader service. The Remote Loader enables synchronization between the DirXML Engine (on your Linux or NetWare server) and a remote driver (on the Windows server.) See Configuring the Identity Manager Drivers for Use with the Remote Loader (https://www.netiq.com/documentation/idm36/idm_remoteloader/data/bs35plh.html) for more information.

In order to run Identity Manager on a Windows server, you need to purchase *Novell Identity Manager*.

Can I run Identity Manager on a Solaris or AIX Server?

Not with the Bundle Edition. However, you can still synchronize data held on these platforms by using the Identity Manager Remote Loader service. The Remote Loader enables synchronization between the Metadirectory Engine and a remote driver (on the Solaris or AIX server.) See Configuring the Identity Manager Drivers for Use with the Remote Loader (https://www.netiq.com/documentation/idm36/idm_remoteloader/data/bs35plh.html) for more information.

In order to run Identity Manager on Solaris or AIX, you need to purchase *Novell Identity Manager*.

My drivers stopped working. What happened?

You might have installed the Bundle Edition on a non-OES server. The Bundle Edition must be installed on your Linux or NetWare server where OES exists. If Identity Manager is installed on a non-OES platform, activation cannot work. After 90 days, your drivers will stop running.

I purchased an additional Integration Module. Why doesn't it work?

With your OES purchase, you are entitled to use the Bundle Edition products. If you want to add new Integration Modules, you also need to purchase *Novell Identity Manager*. The Integration Module cannot activate until you purchase *Novell Identity Manager*.

If I purchase a license for *Novell Identity Manager* and a license for an additional Integration Module, do I need to re-install the software?

No, you just need to install the activation credentials associated with your purchase.

How do I know what's activated?

For information about how to view currently activated products, see Viewing Product Activations (http://www.netiq.com/documentation/idm36/idm_install/data/agfhtax.html).

17 Access Control and Authentication

Access Control and Authentication are the keys to:

- Providing services for users.
- Ensuring that the network is secure.

This section discusses the following:

- Section 17.1, "Controlling Access to Services," on page 167
- Section 17.2, "Authentication Services," on page 178

17.1 Controlling Access to Services

OES 2 supports a number of options for service access, including

- Web browsers.
- File managers and applications on Linux, Macintosh, and Windows workstations.
- Novell Client software.
- Personal digital assistants (PDAs) and other electronic devices that are enabled for Web access.

You control which of these options can be used through the services you offer and the ways your configure those services.

This section can help you understand access control at a high level so that you can plan, implement, and control access to services. More detail about the items discussed is contained in individual service guides.

The topics that follow are:

- Section 17.1.1, "Overview of Access Control," on page 167
- Section 17.1.2, "Planning for Service Access," on page 173
- Section 17.1.3, "Coexistence and Migration of Access Services," on page 176
- Section 17.1.4, "Access Implementation Suggestions," on page 176
- Section 17.1.5, "Configuring and Administering Access to Services," on page 176

17.1.1 Overview of Access Control

The following sections present overviews of methods for accessing Open Enterprise Server 2 services.

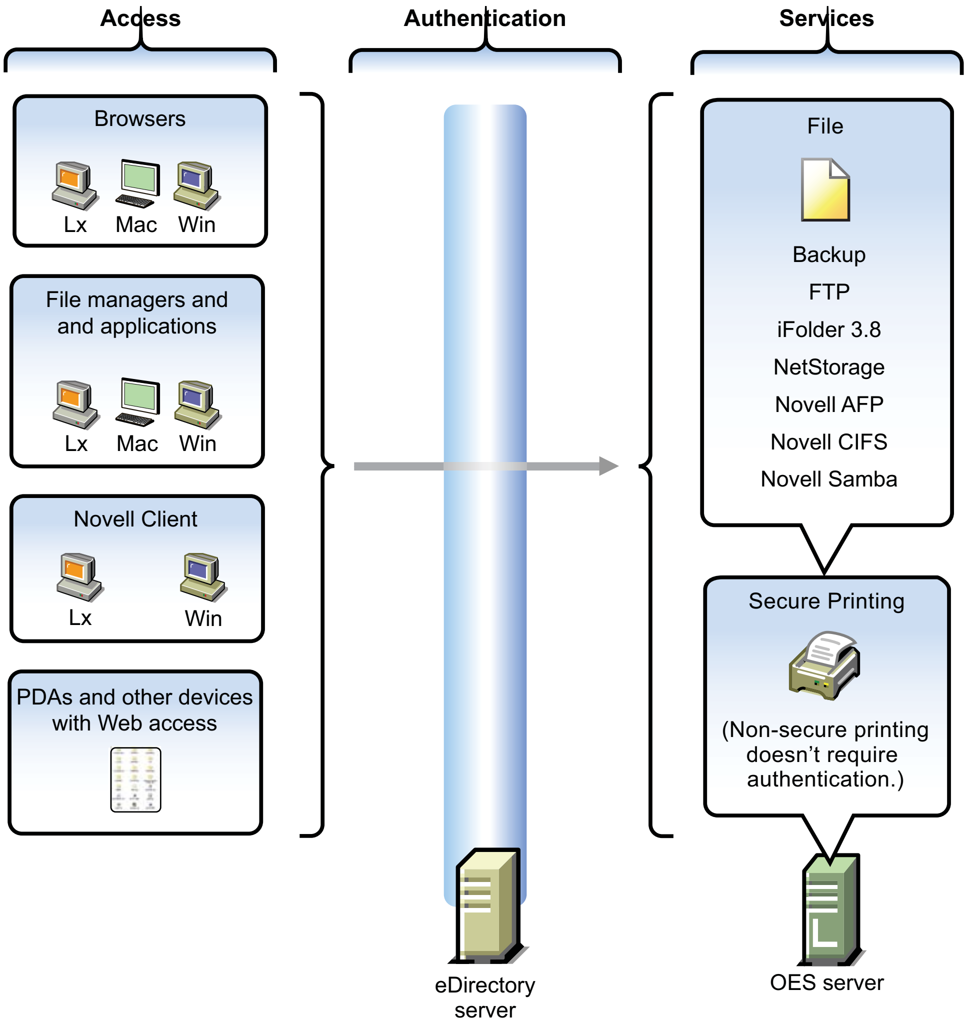
- "Access to OES 2 Services" on page 168
- "Access Control Options in OES 2" on page 169
- "The Traditional Novell Access Control Model" on page 170
- "NSS Access Control on OES" on page 171

- "Novell Client (NCP File Services) Access" on page 172
- "eDirectory User Access to OES 2 Servers" on page 173

Access to OES 2 Services

Figure 17-1 illustrates the access methods supported by OES 2 services. Novell eDirectory provides authentication to each service.

Figure 17-1 *Access Interfaces and the Services They Can Access*



The interfaces available for each service are largely determined by the protocols supported by the service.

- Browsers and personal digital assistants require support for the HTTP protocol.
- Each workstation type has file access protocols associated with it. Linux uses NFS as its native protocol for file services access, Macintosh workstations communicate using AFP or CIFS, and Windows workstations use the CIFS protocol for file services.
- Novell Client software for both Windows and Linux uses the NetWare Core Protocol (NCP) to provide the file services for which Novell is well known.

Understanding the protocol support for OES 2 services can help you begin to plan your OES implementation. For more information, see "Matching Protocols and Services to Check Access Requirements" on page 175.

Access Control Options in OES 2

Because OES 2 offers both traditional Novell access control and POSIX access control, you have a variety of approaches available to you, including combining the two models to serve various aspects of your network services.

Table 17-1 provides links to documentation that discusses OES 2 access control features.

Table 17-1 *General File System Access Control*

Feature	To Understand	See
Access Control Lists (ACLs) on Linux	How ACLs are supported on the most commonly used Linux POSIX file systems and let you assign file and directory permissions to users and groups who do not own the files or directories.	"Access Control Lists in Linux" (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html)in the *SLES 10 SP4: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html)
Aligning NCP and POSIX access rights	How to approximate the NCP (or NetWare) access control model on POSIX file systems.	"Section 18.4, "Aligning NCP and POSIX File Access Rights," on page 198"
Directory and file attributes	Directory and file attributes on NSS volumes.	"Understanding Directory and File Attributes for NSS Volumes" in the *OES 2 SP3: File Systems Management Guide*
File system trustee rights	File system trustee rights on NetWare (NSS and traditional volumes), including how effective file system trustee rights are determined.	"Understanding the Novell Trustee Model for File System Access" in the *OES 2 SP3: File Systems Management Guide*
Novell trustee rights and directory and file attributes	How to control who can see which files and what they can do with them.	"Understanding File System Access Control Using Trustees" in the *OES 2 SP3: File Systems Management Guide*
POSIX file system rights and attributes on Linux	How to configure file system attributes on OES 2 servers.	"Access Control Lists in Linux" (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html) in the *SLES 10 SP4: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html)
Security Equivalence in eDirectory	The concept of Security Equivalence in eDirectory.	"Security Equivalence" in the *OES 2 SP3: File Systems Management Guide*

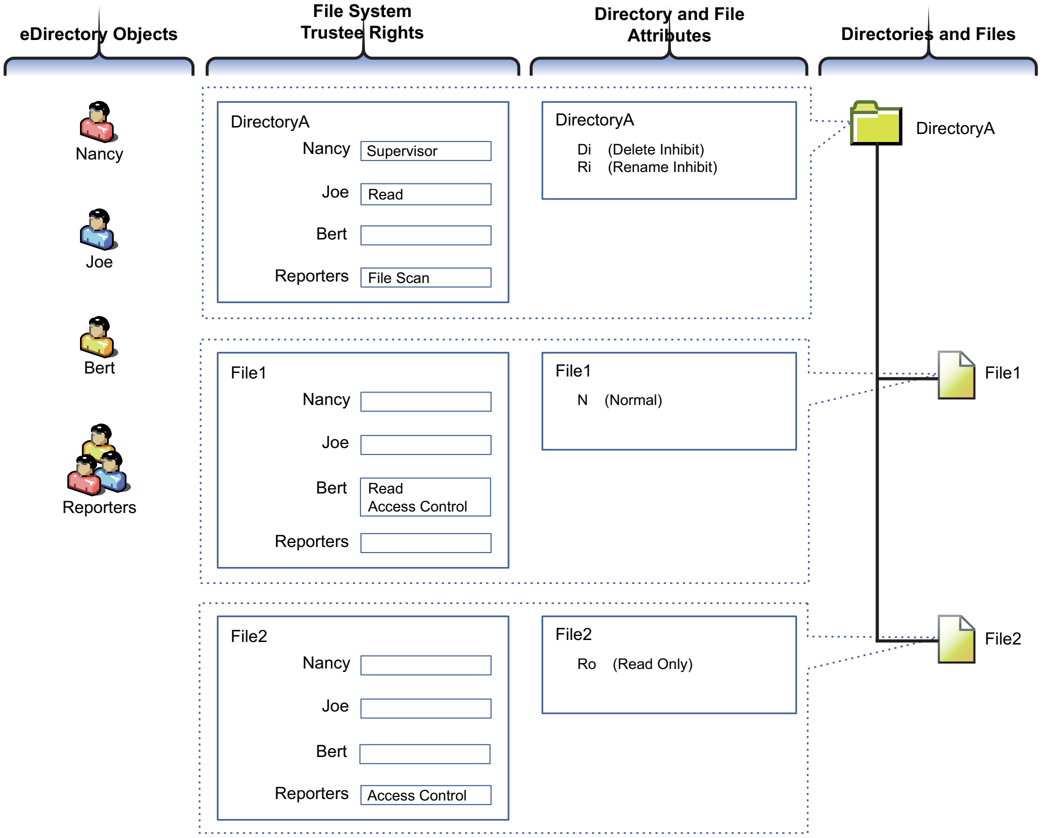
The Traditional Novell Access Control Model

NetWare is known for its rich access control. OES makes these controls available on Linux through NSS volume support. In addition, some of the controls are available on Linux POSIX file systems through NCP volume creation. NCP volumes are limited because Linux POSIX systems offer only a subset of the directory and file attributes that NSS offers.

In the Novell access control model, eDirectory objects, such as users and groups, are assigned File System Trustee Rights to directories and files on NSS and NCP volumes. These trustee rights determine what the user or group can do with a directory or file, provided that the directory or file attributes allow the action.

This is illustrated in Figure 17-2.

Figure 17-2 *Directory and File Access under the NetWare Access Control Model*



DirectoryA
Nancy: Supervisor
Joe: Read
Bert:
Reporters: File Scan

DirectoryA
Di (Delete Inhibit)
Ri (Rename Inhibit)

File1
Nancy:
Joe:
Bert: Read, Access Control
Reporters:

File1
N (Normal)

File2
Nancy:
Joe:
Bert:
Reporters: Access Control

File2
Ro (Read Only)

Table 17-2 explains the effective access rights illustrated in Figure 17-2.

Table 17-2 Access Rights Explanation

eDirectory Objects	File System Trustee Rights	Directory and File Attributes	Directories and Files
eDirectory objects (in most cases users and groups) gain access to the file system through eDirectory.	File system trustee rights govern access and usage by the eDirectory object specified for the directory or file to which the rights are granted. Trustee rights are overridden by directory and file attributes. For example, even though Nancy has the Supervisor (all) trustee right at the directory (and, therefore, to the files it contains), she cannot delete File2 because it has the Read Only attribute set. Of course, Nancy could modify the file attributes so that File2 could then be deleted.	Each directory and file has attributes associated with it. These attributes apply universally to all trustees regardless of the trustee rights an object might have. For example, a file that has the Read Only attribute is Read Only for all users. Attributes can be set by any trustee that has the Modify trustee right to the directory or file.	The possible actions by the eDirectory users and group shown in this example are as follows: ◆ Nancy has the Supervisor trustee right at the directory level, meaning that she can perform any action not blocked by a directory or file attribute. The Di (Delete Inhibit) and Ri (Rename Inhibit) Attributes on Directory A prevent Nancy from deleting or renaming the directory unless she modifies the attributes first. The same principle applies to her ability to modify File2. ◆ Because Joe is a member of the Reporters group, he can view file and directory names inside DirectoryA and also see the directory structure up to the root directory. Joe also has rights to open and read any files in DirectoryA and to execute any applications in DirectoryA. ◆ Because Bert is a member of the Reporters group, he can view file and directory names inside DirectoryA and also see the directory structure up to the root directory. Bert also has rights to open and read File1 and to execute it if it's an application. And Bert has rights to grant any eDirectory user access to File1. ◆ Because all three users are members of the Reporters group, they can grant any eDirectory user access to File2. Of course, for Nancy this is redundant because she has the Supervisor right at the directory level.

NSS Access Control on OES

Table 17-3 provides links to documentation that discusses the various NSS-specific access control features.

Table 17-3 Summary of NSS Access Control Documentation Links

Feature	To Understand	See
Independent Mode vs. NetWare Mode This applies only to OES servers, not NetWare.	The difference between Independent Mode access and NetWare Mode access.	"Access Control for NSS on Linux" in the *OES 2 SP3: File Systems Management Guide*
POSIX directory and file attributes on NSS volumes on OES 2 This is only about what is displayed. POSIX permissions are not used for access control to NSS volumes.	How NSS file attributes are reflected in Linux directory and file permissions viewable through POSIX.	"Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions" in the *OES 2 SP3: File Systems Management Guide*

Novell Client (NCP File Services) Access

If you have not already determined whether to use the Novell Client on your network, we recommend that you consider the following information:

- "About the Novell Client" on page 172
- "Is the Novell Client Right for Your Network?" on page 172
- "Differences between Linux and Windows" on page 173

About the Novell Client

The Novell Client extends the capabilities of Windows and Linux desktops with access to NetWare and OES 2 servers.

After installing Novell Client software, users can enjoy the full range of Novell services, such as

- Authentication via Novell eDirectory
- Network browsing and service resolution
- Secure and reliable file system access
- Support for industry-standard protocols

The Novell Client supports the traditional Novell protocols (NDAP, NCP, and RSA) and interoperates with open protocols (LDAP, CIFS, and NFS).

Is the Novell Client Right for Your Network?

Although Novell offers services that don't require Novell Client, (such as NetStorage, Novell iFolder 3.8, and iPrint), many network administrators continue to prefer the Novell Client as the access choice for their network users for the following reasons:

- They prefer eDirectory authentication to LDAP authentication because they believe it is more secure.
- They prefer the NetWare Core Protocol (NCP) over the Microsoft CIFS protocol because they believe that CIFS is more vulnerable to the propagation of viruses on the network.

Conversely, other network administrators are equally adamant that their users function better without the added overhead of running an NCP client on each workstation.

We can’t determine what is best for you or your network, but we do provide you with viable choices.

Differences between Linux and Windows

There are some differences between the Linux and Windows clients. These are documented in “Understanding How the Novell Client for Linux Differs from the Novell Client for Windows 2000/XP” in the *Novell Client 2.0 SP3 for Linux Administration Guide*.

eDirectory User Access to OES 2 Servers

Some services that run on OES 2 servers require that the users accessing them be (or, at least, appear to the Linux system to be) standard Linux users with Linux user credentials, such as a user ID (UID) and primary group ID (GID).

So that eDirectory users can access these services, Novell provides the Linux User Management (LUM) technology. The impact of this on you as the network administrator is that these users and groups must be enabled for eDirectory LDAP authentication to the local server. For more information, see “Linux User Management: Access to Linux for eDirectory Users” on page 153.

17.1.2 Planning for Service Access

After you understand the access options available to your network users, you can decide which will work best on your network.

Planning tips for network services are contained in the following sections:

- “Planning File Service Access” on page 173
- “Planning Print Service Access” on page 174
- “Matching Protocols and Services to Check Access Requirements” on page 175

Planning File Service Access

As you plan which file services to provide, be aware of the file service/volume and feature support limitations outlined in the following sections.

- “Service Access to Volume Type Limitations” on page 173
- “Feature Support” on page 174

Service Access to Volume Type Limitations

Supported combinations are outlined in Table 17-4.

Table 17-4 *Service Access to Volume Types*

File Service	Linux POSIX Volumes	NSS Volumes on Linux
AFP	No	Yes-Novell AFP
CIFS	Yes-Novell CIFS, Novell Samba	Yes-Novell CIFS, Novell Samba
NetStorage	Yes	Yes
NetWare Core Protocol (NCP)	Yes	Yes

File Service	Linux POSIX Volumes	NSS Volumes on Linux
NFS	Yes	Yes-NFSv3
Novell iFolder 2.1*x*	No	No
Novell iFolder 3.8	Yes	Yes

Details about the file systems supported by each file service are explained in the documentation for each service.

Be aware that file services support different sets of access protocols. A summary of the protocols available for access to the various OES file services is presented in "Matching Protocols and Services to Check Access Requirements" on page 175.

Feature Support

Table 17-5 *Features Supported on Each Volume Type*

Feature	Linux POSIX Volumes	NSS Volumes on Linux
Directory quotas	No	Yes
Login scripts	Yes (if also defined as an NCP volume)	Yes
Mapped drives	Yes (if also defined as an NCP volume)	Yes
Novell directory and file attributes	No	Yes
Purge/Salvage	No	Yes
Trustee rights	Yes (if also defined as an NCP volume)	Yes
User space quotas	No	Yes

Planning Print Service Access

Novell iPrint has access control features that let you specify the access that each eDirectory User, Group, or container object has to your printing resources.

You can also use iPrint to set up print services that don't require authentication.

NOTE: Access control for printers is supported only on the Windows iPrint Client.

For more information on access control and iPrint, see "Setting Access Control for Your Print System" in the *OES 2 SP3: iPrint for Linux Administration Guide*

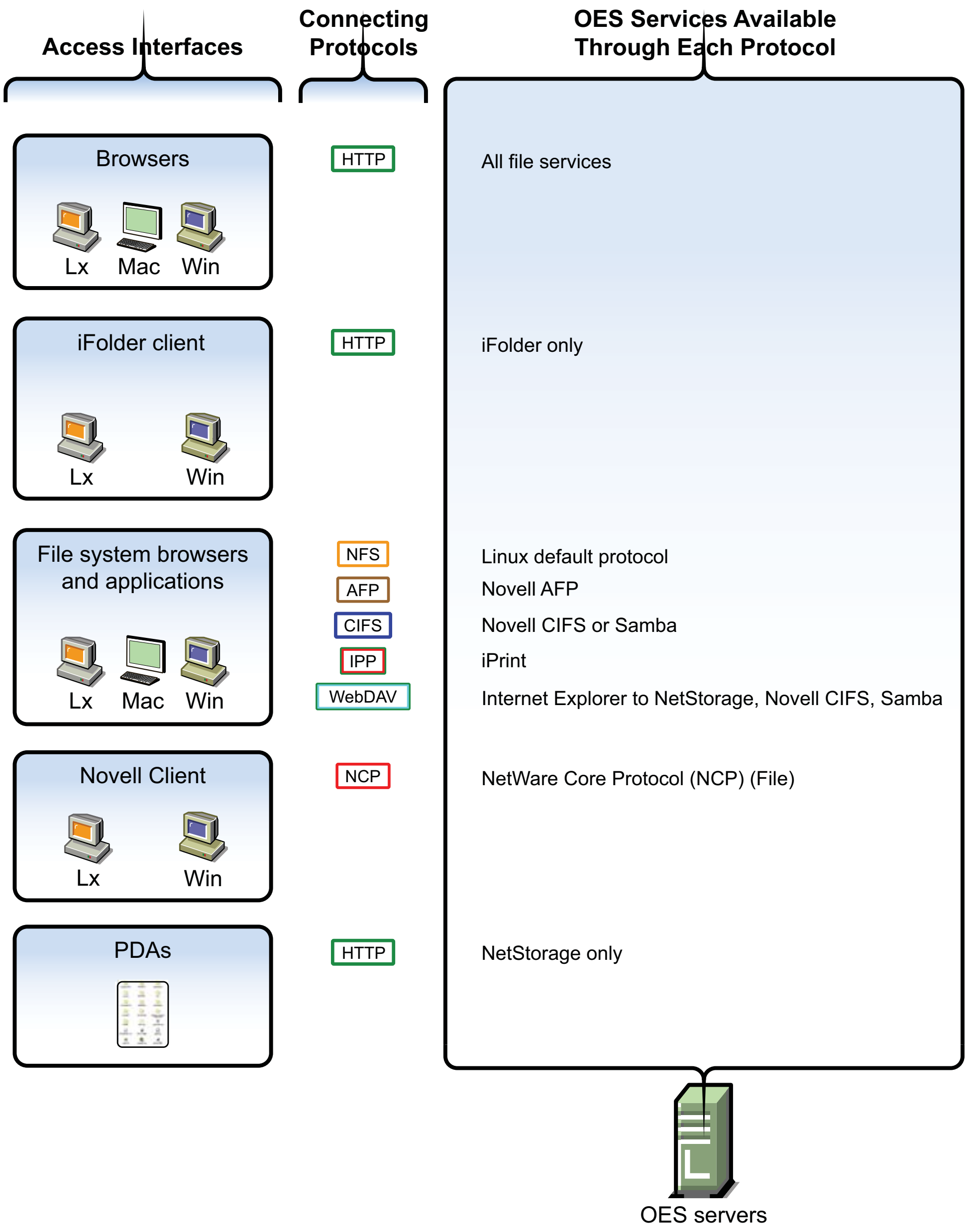
Matching Protocols and Services to Check Access Requirements

Figure 17-3 illustrates the access interfaces available to users in OES and the services that each interface can connect to. It also shows the protocols that connect access interfaces with network services.

To use this for planning:

1. Review the different access interfaces in the left column.
2. In the middle column, review the protocols each interface supports.
3. In the right column, view the services available to the interfaces via the protocols.

Figure 17-3 *Access Interfaces and Services, and the Protocols That Connect Them*



17.1.3 Coexistence and Migration of Access Services

Because NetWare Core Protocol (NCP) is now available on Linux, your Novell Client users can attach to OES 2 servers as easily as they have been able to attach to NetWare servers. In fact, they probably won't notice any changes.

NCP Server for Linux enables support for login scripts, mapping drives to OES 2 servers, and other services commonly associated with Novell Client access. This means that Windows users with the Novell Client installed can now be seamlessly transitioned to file services on OES 2. And with the Novell Client for Linux, Windows users can be moved to SUSE Linux Enterprise Desktop with no disruption in NCP file services.

For more information, see the *OES 2 SP3: NCP Server for Linux Administration Guide*.

17.1.4 Access Implementation Suggestions

After you plan and install OES 2 services, be sure to provide clear access instructions to your network users. For a summary of access methods, see Appendix E, "Quick Reference to OES 2 User Services," on page 259.

17.1.5 Configuring and Administering Access to Services

The following sections discuss administering access to services.

- "Password Management" on page 176
- "Linux (POSIX) File System Access Rights" on page 176
- "NSS File and Directory Trustee Management" on page 177

Password Management

Many network administrators let users administer their own passwords. For more information on password self management, see "Password Self-Service" in the *Novell Password Management 3.3.2 Administration Guide*.

Linux (POSIX) File System Access Rights

Access control to Linux POSIX file systems is controlled through POSIX file system access rights or attributes associated with directories and files. In general, the directories and files can be accessed by three POSIX entities:

- The user who owns the directory or file
- The group who owns the directory or file
- All other users defined on the system

These users and the affected group are each assigned (or not assigned) a combination of three attributes for each directory and file:

Table 17-6 *Linux Access Rights*

Attribute	Effect on Directory when Assigned	Effect on File when Assigned
Read	Lets the user or group view the directory's contents.	Lets the user or group open and read the file.
Write	Lets the user or group create or delete files and subdirectories in the directory.	Lets the user or group modify the file.
Execute	Lets the user or group access the directory by using the `cd` command.	Lets the user or group run the file as a program.

For more information, see "Configuring Trustees and File System Attributes" in the *OES 2 SP3: File Systems Management Guide*.

NSS File and Directory Trustee Management

The *OES 2 SP3: File Systems Management Guide* contains a thorough discussion of file and directory trustee management in its "Configuring Trustees and File System Attributes" section.

The following sections present brief information about managing trustees on NSS volumes.

- "Using NetStorage to Change File and Directory Attributes and Trustees" on page 177
- "Using the Novell Client to Change File and Directory Attributes and Trustee Rights" on page 177
- "Using iManager 2.7 to Change File and Directory Attributes and Trustee Rights" on page 177
- "Using the Linux Command Prompt to Change File Attributes" on page 177
- "Using the Linux Command Prompt to Change Trustee Rights" on page 178

Using NetStorage to Change File and Directory Attributes and Trustees

You can use the NetStorage Web browser interface to change attributes and trustees for directories and files on NSS volumes, but you can't change them by using a WebDAV connection to NetStorage.

Using the Novell Client to Change File and Directory Attributes and Trustee Rights

You can use the Novell Client to change NSS file and directory attributes and to grant trustee rights to an NSS volume on an OES 2 server. For more information, see "NetWare File Security" in the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide* and "Managing File Security" in the *Novell Client 2.0 SP3 for Linux Administration Guide*.

Using iManager 2.7 to Change File and Directory Attributes and Trustee Rights

You can use the iManager 2.7 Files and Folders plug-in to manage directories and files on NCP and NSS volumes. For more information, see the plug-in help.

Using the Linux Command Prompt to Change File Attributes

Use the `attrib` command to change file and directory attributes on an NSS volume.

The `attrib` command is also documented in "Using the Attrib Utility to Set NSS File System Attributes" in the *OES 2 SP3: File Systems Management Guide*.

You can also enter the following command at the command prompt:

```
attrib --help
```

Using the Linux Command Prompt to Change Trustee Rights

To grant NSS trustee rights to an NSS volume, enter the following command:

```
rights -f /full/directory/path -r rights_mask trustee full.object.context
```

where */full/directory/path* is the path to the target directory on the NSS volume, *rights_mask* is the list of NSS rights, and *full.object.context* is the object (User or Group) in its full eDirectory context including the tree name.

For example, you might enter the following:

```
rights -f /data/groupstuff -r rwfc trustee mygroup.testing.example_tree
```

For a complete list of command options, enter `rights` at the command prompt.

The rights command is also documented in "Using the Rights Utility to Set Trustee Rights for the NSS File System" in the *OES 2 SP3: File Systems Management Guide*.

17.2 Authentication Services

This section briefly discusses the following topics:

- Section 17.2.1, "Overview of Authentication Services," on page 178
- Section 17.2.2, "Planning for Authentication," on page 181
- Section 17.2.3, "Authentication Coexistence and Migration," on page 181
- Section 17.2.4, "Configuring and Administering Authentication," on page 181

17.2.1 Overview of Authentication Services

This section provides specific overview information for the following key OES components:

- "NetIdentity Agent" on page 178
- "Novell Modular Authentication Services (NMAS)" on page 179
- "Password Support in OES 2" on page 179

For more authentication topics, see "Access, Authenticate, Log in (http://www.novell.com/documentation/oes2/access-control.html)" in the OES online documentation.

NetIdentity Agent

In OES 2, the NetIdentity Agent works with Novell eDirectory authentication to provide background eDirectory authentication to NetStorage through a secure identity "wallet" on the workstation.

NetIdentity Agent browser authentication is supported only by Windows Internet Explorer.

The Novell Client provides authentication credentials to NetIdentity, but it does not obtain authentication credentials from NetIdentity because it is not a Web-based application.

NetIdentity Agent requires

- XTier (NetStorage) on the OES 2 server presented in the URL for the Web-based applications.
- The NetIdentity agent installed on the workstations.

For more information on using the NetIdentity agent, see the *NetIdentity Administration Guide for NetWare 6.5*.

Novell Modular Authentication Services (NMAS)

Novell Modular Authentication Services (NMAS) lets you protect information on your network by providing various authentication methods to Novell eDirectory on NetWare, Windows, and UNIX networks.

These login methods are based on three login factors:

- Password
- Physical device or token
- Biometric authentication

For example:

- You can have users log in through a password, a fingerprint scan, a token, a smart card, a certificate, a proximity card, etc.
- You can have users log in through a combination of methods to provide a higher level of security.

Some login methods require additional hardware and software. You must have all of the necessary hardware and software for the methods to be used.

NMAS software consists of the following:

- **NMAS server components:** Installed as part of OES 2.
- **The NMAS Client:** Required on each Windows workstation that will be authenticating using NMAS.

Support for Third-Party Authentication Methods

Novell Client distributions include a number of NMAS login methods.

Other third-party methods are available for download. For information on the available third-party login methods, see the NMAS Partner’s Web site (http://www.novell.com/products/nmas/partners_communities.html). Each method has a `readme.txt` file or a `readme.pdf` file that includes specific installation and configuration instructions.

More Information

For more information on how to use NMAS, see the *Novell Modular Authentication Services 3.3.4 Administration Guide*.

Password Support in OES 2

In the past, administrators have needed to manage multiple passwords (simple password, NDS passwords, Samba passwords) because of password differences. Administrators have also needed to deal with keeping the passwords synchronized.

In OES you have the choice of retaining your current password maintenance methods or deploying Universal Password to simplify password management. For more information, see the *Novell Password Management 3.3.2 Administration Guide*.

All Novell products and services are being developed to work with extended character (UTF-8 encoded) passwords. For a current list of products and services that work with extended characters, see Novell TID 3065822 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3065822&sliceId=1&docTypeID=DT_TID_1_1&dialogID=77556590&stateId=0%200%2077560425).

The password types supported in eDirectory are summarized in Table 17-7.

Table 17-7 *eDirectory Password Types*

Password Type	Description
NDS	The NDS password is stored in a hash form that is nonreversible in eDirectory. Only the NDS system can make use of this password, and it cannot be converted into any other form for use by any other system.
Novell AFP and Novell CIFS	In OES 2, AFP and CIFS users have Universal Password policies assigned by default. More information about password policy planning is available in Appendix K, "Coordinating Password Policies Among Multiple File Services," on page 295.
Samba	In OES 2, Samba users have a Universal Password policy assigned by default. OES 2 also supports the Samba hash password if desired. However, you must choose to not deploy Universal Password if you want to use the Samba hash password. Choosing the Samba password requires that users always remember to synchronize it when changing their eDirectory password. For more information, see "Samba Passwords" in the *OES2 SP3: Samba Administration Guide*.
Simple	The simple password provides a reversible value stored in an attribute on the User object in eDirectory. NMAS securely stores a clear-text value of the password so that it can use it against any type of authentication algorithm. To ensure that this value is secure, NMAS uses either a DES key or a triple DES key (depending on the strength of the Secure Domain Key) to encrypt the data in the NMAS Secret and Configuration Store. The simple password was originally implemented to allow administrators to import users and hashed passwords from other LDAP directories such as Active Directory and iPlanet*. The limitations of the simple password are that no password policy (minimum length, expiration, etc.) is enforced. Also, by default, users do not have rights to change their own simple passwords.

Password Type	Description
Universal	Universal Password (UP) enforces a uniform password policy across multiple authentication systems by creating a password that can be used by all protocols and authentication methods. Universal Password is managed in iManager by the Secure Password Manager (SPM), a component of the NMAS module installed on OES 2 servers. All password restrictions and policies (expiration, minimum length, etc.) are supported. All the existing management tools that run on clients with the UP libraries automatically work with the Universal Password. Universal Password is not automatically enabled unless you install Novell AFP, Novell CIFS, Domain Services for Windows, or Novell Samba on an OES 2 server. You can optionally choose to have the Samba hash password stored separately. This requires, however, that users always synchronize the Samba password when changing their eDirectory password. The Novell Client supports the Universal Password. It also supports the NDS password for older systems in the network. The Novell Client automatically upgrades to use Universal Password when UP is deployed. For more information, see "Deploying Universal Password" in the *Novell Password Management 3.3.2 Administration Guide*.

17.2.2 Planning for Authentication

For planning topics, see the "Access, Authenticate, Log in (http://www.novell.com/documentation/oes2/access-control.html)" in the OES online documentation.

17.2.3 Authentication Coexistence and Migration

For authentication and security coexistence and migration information, see "Chapter 22, "Security," on page 225 and Chapter 23, "Certificate Management," on page 239" in this guide.

17.2.4 Configuring and Administering Authentication

For a list of configuration and administration topics, see "Access, Authenticate, Log in (http://www.novell.com/documentation/oes2/access-control.html)" in the OES online documentation.

18 File Services

The file services in Open Enterprise Server 2 let you provide Web-based and network-based file services to your network users.

This section contains the following information:

18.1 Overview of File Services

The file service components in OES include the following:

- FTP Services (page 184): Lets users securely transfer files to and from OES 2 servers.
- NetWare Core Protocol (page 184): Provides NetWare Core Protocol (NCP) access to NCP volumes (including NSS volumes) that you define on OES 2 server partitions.
- NetStorage (page 185): Provides network and Web access to various file services through common file service protocols, such as CIFS.

  The NetStorage server doesn't actually store files and folders. Rather, it provides access to other file services that support the native TCP/IP protocol.
- Novell AFP (page 188): Provides native Macintosh access to files stored on an NSS volume on an OES 2 server.
- Novell CIFS (page 189): Provides native Windows (CIFS and HTTP-WebDAV) access to files stored on an NSS volume on an OES 2 server.
- Novell iFolder 3.8 (page 190): Provides a Web-based and network-based repository (Novell iFolder server) that stores master copies of locally accessible files on the OES 2 server.
- Novell Samba (page 192): Provides Windows (CIFS and HTTP-WebDAV) access to files stored on an OES 2 server's file system.

The file service components in OES are generally compatible. However you cannot run Novell Samba on the same OES 2 server as Novell AFP, Novell CIFS, or Domain Services for Windows, which is not reviewed as a file service, but does include an alternative Samba file service.

18.1.1 Using the File Services Overviews

Each graphical overview in the following sections introduces one of the OES file service components. If visual presentations help you grasp basic concepts, continue with the following overviews. If you prefer to skip the overviews, go to Section 18.2, "Planning for File Services," on page 193.

18.1.2 FTP Services

OES 2 offers a level of integration between eDirectory and Pure-FTP that allows users to authenticate to eDirectory for FTP access to the server. You simply select the *Novell FTP Server* pattern in the OES 2 installation and then make sure the users needing access are LUM-enabled and have access rights to the areas on the server they need to use. You can also migrate an existing FTP server configuration from a NetWare server to OES 2.

For migration instructions and a brief FAQ, see "Migrating FTP from NetWare to OES 2 Linux" in the *OES 2 SP3: Migration Tool Administration Guide*.

For documentation on Pure-FTP, visit the Pure-FTP Web site (http://pureftpd.sourceforge.net/documentation.shtml).

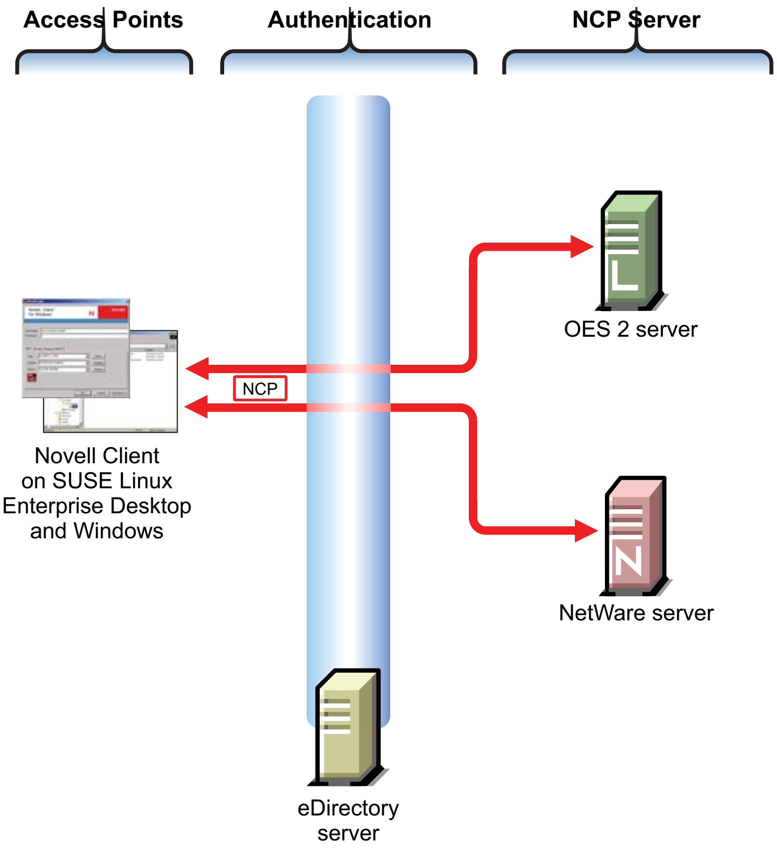
18.1.3 NetWare Core Protocol

NetWare Core Protocol (NCP) is the technology beneath many of the network services for which NetWare is famous.

In OES, NCP is also available on Linux. The Novell NCP Server for Linux provides the rich file services that Novell is known for. Windows and Linux users who run Novell Client software can now access data, manage files and folders, map drives, etc., using the same methods as they do on NetWare servers.

Figure 18-1 illustrates the basics of NCP file services. For more information on how NCP can help you manage access to network resources, see "Access Control and Authentication" on page 167.

Figure 18-1 *NCP Services for Linux and NetWare*



The following table explains the information illustrated in Figure 18-1.

Table 18-1 *NCP Access*

Access Methods	Authentication	NCP Services
Access is through an NCP client—specifically, the Novell Client.	All file service access is controlled by eDirectory authentication.	Files are stored on NetWare or NCP volumes that the administrator has created. The same core set of NetWare file attributes are available on both Linux and NetWare.

18.1.4 NetStorage

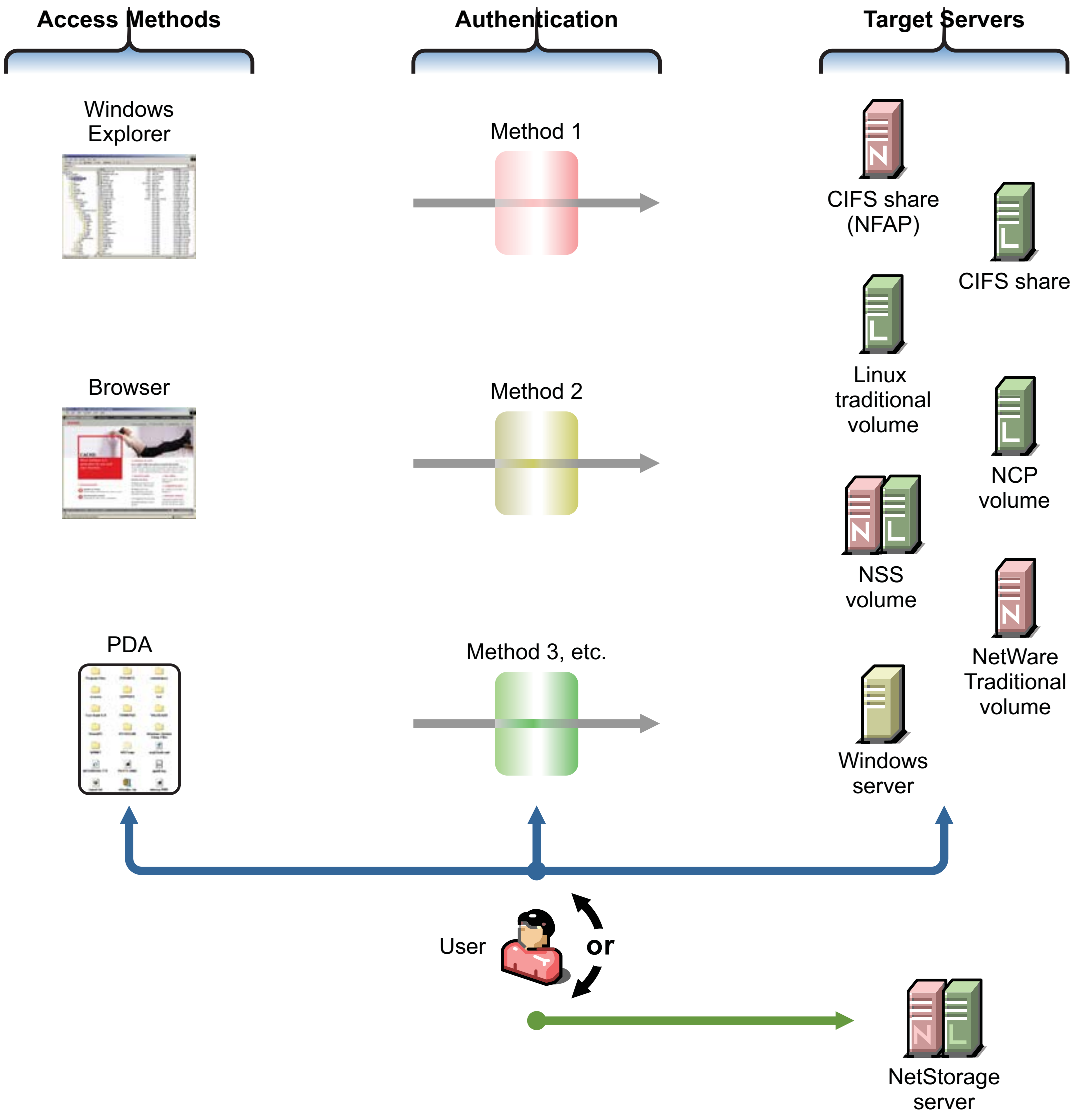
- "Common Network File Storage Problems" on page 185
- "Novell NetStorage on Linux" on page 187

NetStorage makes network files available anywhere, any time.

Common Network File Storage Problems

Network file access is often confusing and frustrating to users, as illustrated in Figure 18-2.

Figure 18-2 Common Network File Storage Problems



The following table explains the information illustrated in Figure 18-2.

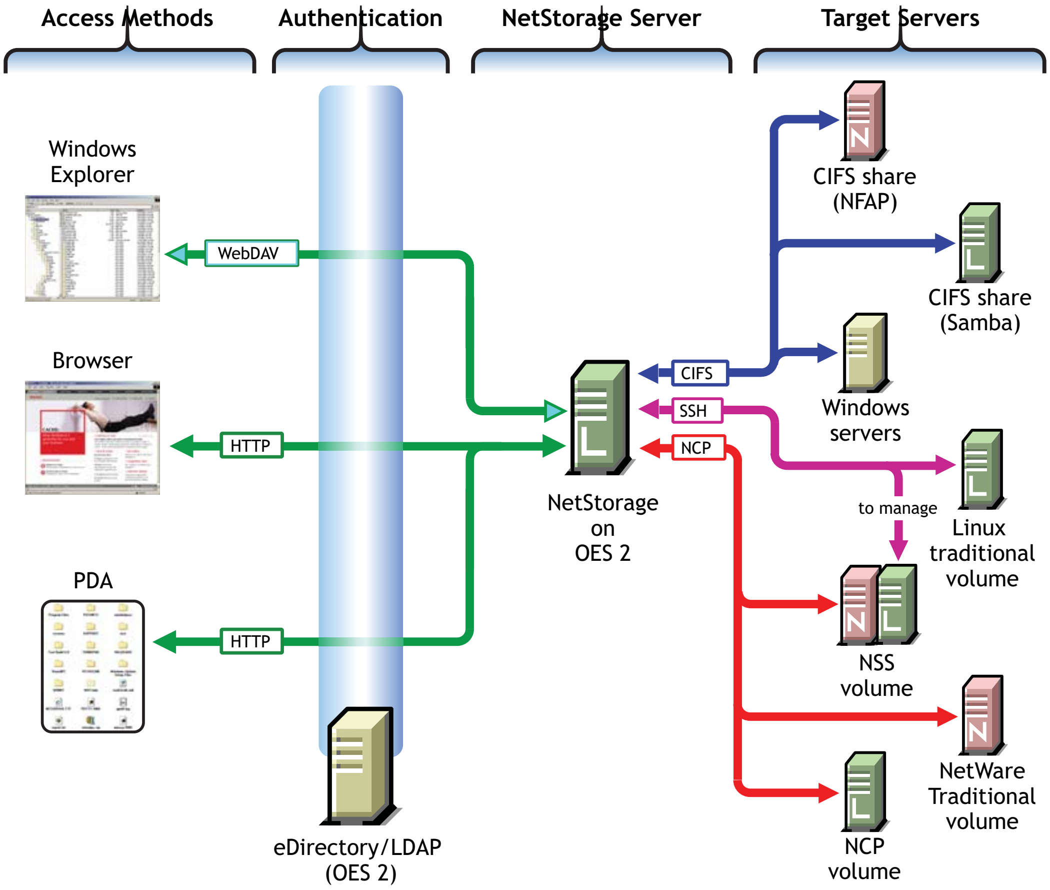
Table 18-2 NetStorage Access Solutions

Access Methods	Authentication	Target File Systems	Solution: NetStorage
Browser or PDA access is critical to those who must travel. However, access method support varies widely among file service providers.	Authentication helps protect information assets, but having diverse authentication methods leads to frustration and lost productivity.	Having diverse file storage services only adds to the complexity and confusion.	Novell NetStorage ties all of these issues together with an easy-to-administer, easy-to-use solution.

Novell NetStorage on Linux

NetStorage on Linux provides local and Web access to files on many systems without requiring the Novell Client (see Figure 18-3).

Figure 18-3 *How NetStorage Works on OES 2*



The following table explains the information illustrated in Figure 18-3.

Table 18-3 *NetStorage on Linux*

Access Methods	Authentication	NetStorage Server	Target Servers
Users have read and write access to files from - **Windows Explorer:** Enabled by the HTTP protocol with WebDAV extensions. - **Browsers:** Users can access files directly by connecting to the NetStorage server. - **PDAs:** PDA users with network connections can access their files as well. Access is granted through login script drive mapping (NCP server required) or through Storage Location Objects.	File service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be running on the OES 2 server.	The NetStorage server receives and processes connection requests and provides access to storage on various servers on the network.	NetStorage on Linux can connect eDirectory users to their files and folders stored in the following locations: - Windows workgroup shares (CIFS or Samba shares) - Linux POSIX volumes through an SSH connection. Linux volumes can also be made available as NCP volumes. Management of NSS volumes on OES 2 through NetStorage requires SSH access to the server. See "When Is SSH Access Required?" on page 96.

18.1.5 Novell AFP

The Novell AFP service lets users on Macintosh workstations access and store files on OES 2 servers with NSS volumes without installing any additional software, such as the Novell Client (see Figure 18-4).

Figure 18-4 *How Novell AFP Works*

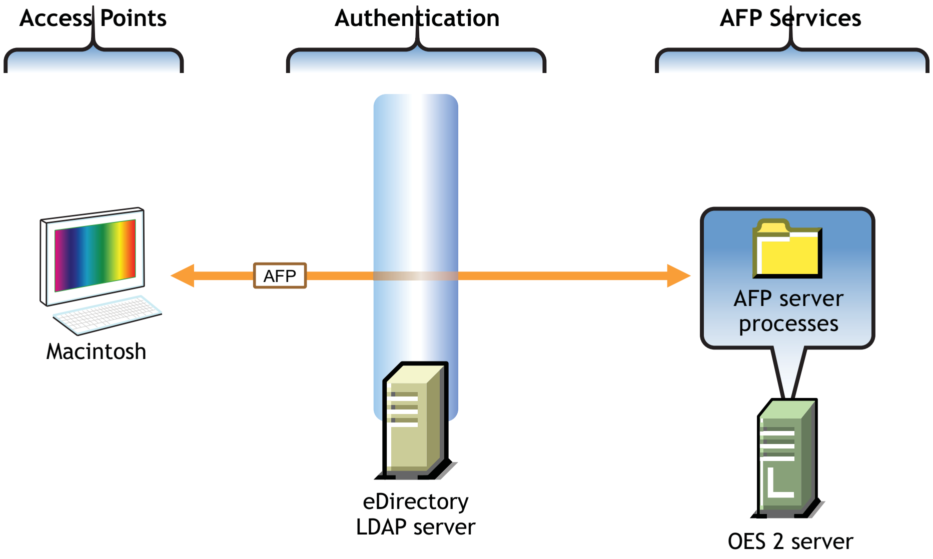


***Table 18-4** AFP Access*

Access Points	Authentication	AFP File Services
eDirectory users on Macintosh workstations have native access to the OES 2 server.	All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES 2 server.	Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to Linux volumes.

18.1.6 Novell CIFS

The Novell CIFS service lets users on Windows workstations access and store files on OES 2 servers with NSS volumes without installing any additional software, such as the Novell Client (see Figure 18-4).

***Figure 18-5** How Novell CIFS Works*

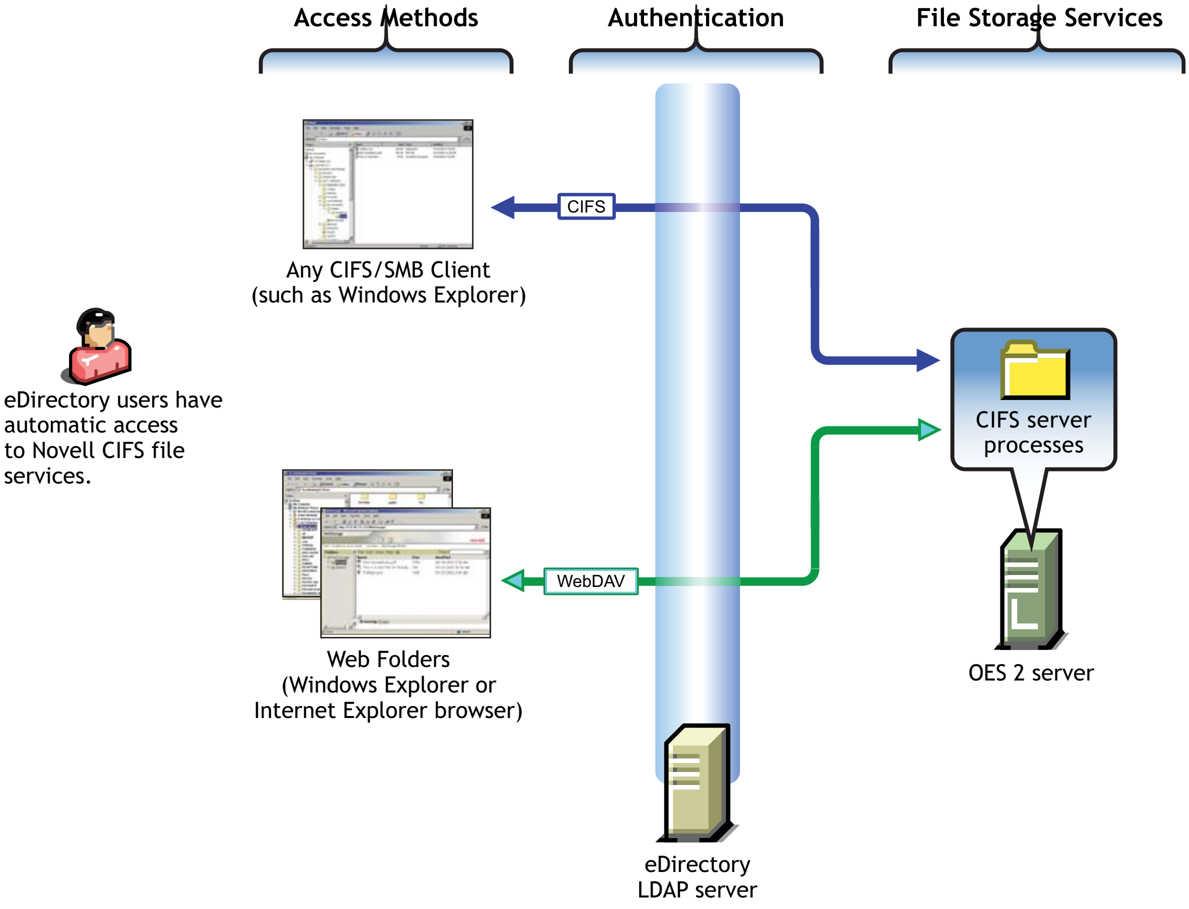


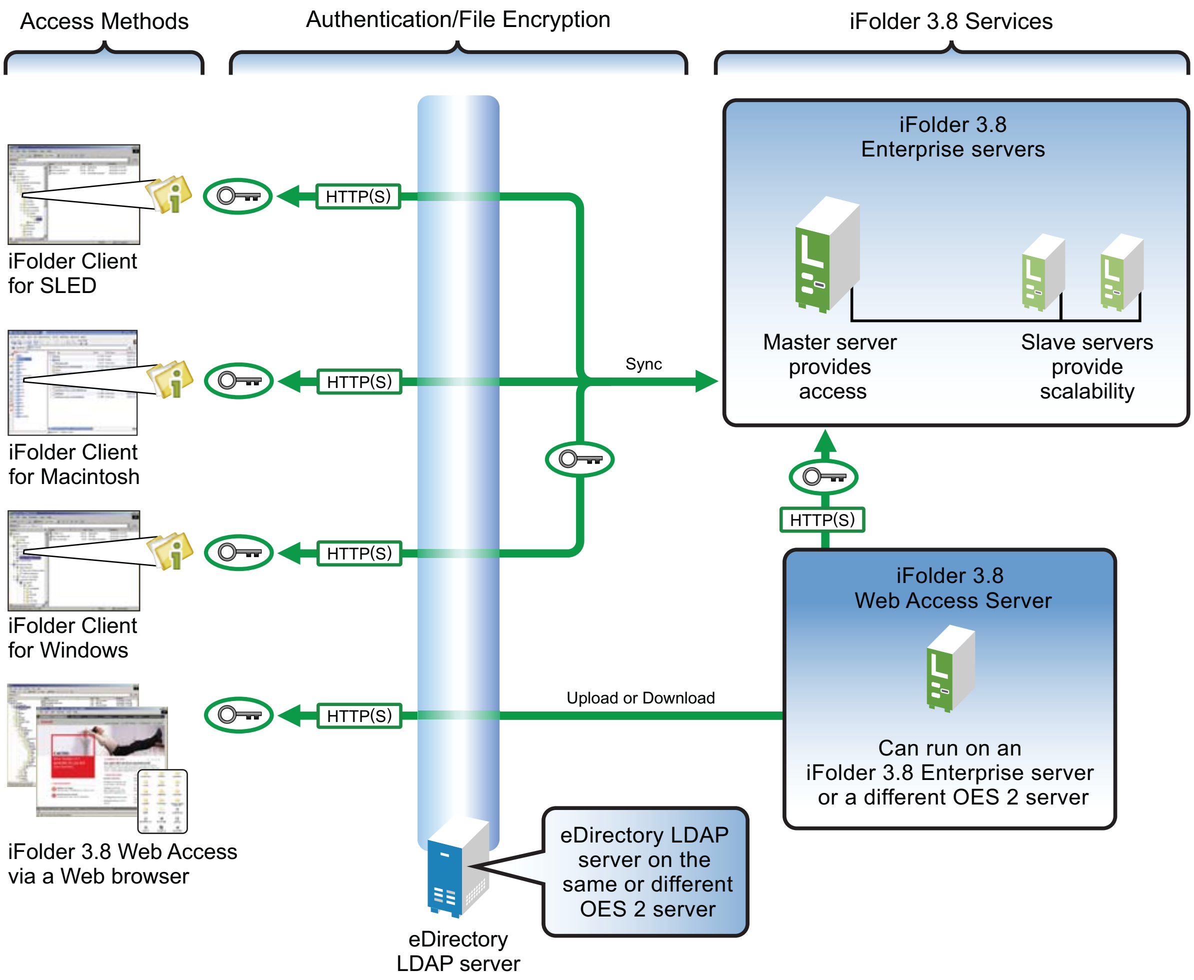
Table 18-5 *CIFS Access*

Access Methods	Authentication	CIFS File Services
eDirectory users on Windows workstations have two native Windows file access options: - **CIFS Client Access:** Windows Explorer users can access and modify files on the OES 2 server just as they would on any workgroup server share. - **Web Folder:** Users can create Web Folders in Windows Explorer or Internet Explorer. Files on the OES 2 server are accessed and maintained with the HTTP-WebDAV protocol.	All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES 2 server.	Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to NSS volumes.

18.1.7 Novell iFolder 3.8

Novell iFolder 3.8 supports multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution (see Figure 18-6).

Figure 18-6 *How Novell iFolder Works*



The following table explains the information illustrated in Figure 18-6.

Table 18-6 *iFolder Access*

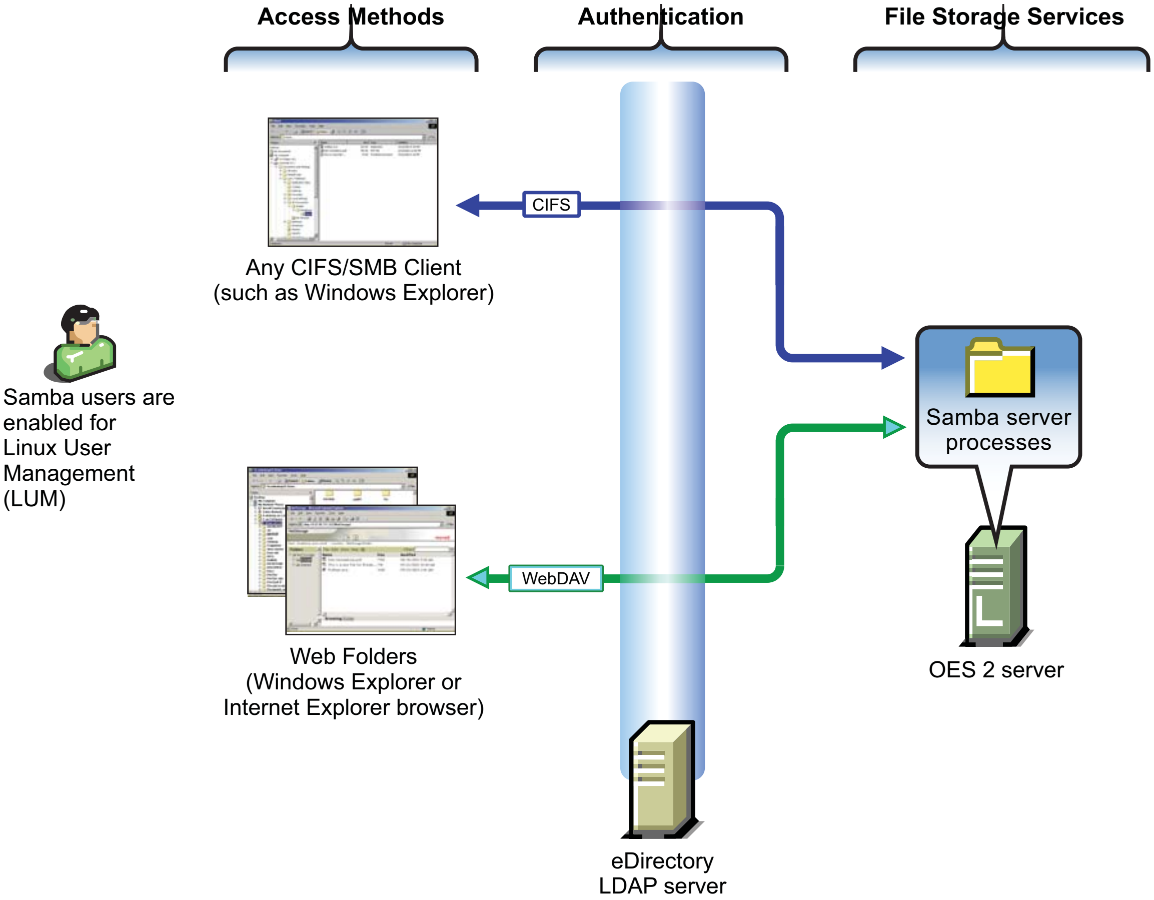
Access Methods	Authentication/File Encryption	Novell iFolder 3.8 Services
Linux, Mac, and Windows workstation users who have the Novell iFolder Client installed can access and modify their files in one or more workstation folders. Changes are automatically synchronized with the iFolder 3.8 Enterprise servers. A Web interface lets users access their files from any computer with an active network or Internet connection.	All file service access is controlled by LDAP- based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES 2 server. Files can be encrypted for transport using SSL connections (HTTPS).	Slave servers can be added as needed, providing the ability to dynamically grow iFolder services without disrupting users. Local and network copies of each file are automatically synchronized by the Novell iFolder Client and Server pieces.

Additional overview information is available in "Overview of Novell iFolder" in the *Novell iFolder 3.8.4 Administration Guide*.

18.1.8 Novell Samba

Samba on an OES 2 server provides Windows (CIFS and HTTP-WebDAV) access to files stored on the OES 2 server (see Figure 18-7).

Figure 18-7 *How Samba on OES Works*



The following table explains the information illustrated in Figure 18-7.

Table 18-7 Samba Access

Access Methods	Authentication	File Storage Services
eDirectory users on Windows workstations have two native Windows file access options (if their eDirectory accounts have been enabled for LUM and Samba): ◆ **CIFS Client Access:** Windows Explorer users can access and modify files on the Samba server just as they would on any workgroup server share. ◆ **Web Folder:** Users can create Web Folders in Windows Explorer or Internet Explorer. Files on the OES 2 server running Samba are accessed and maintained with the HTTP-WebDAV protocol.	All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES 2 server.	Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to Linux volumes.

Samba is an open source initiative. In addition to Linux support, Samba initiatives provide support for other platforms such as Apple Computer's operating systems. More information is available on the Web (http://www.samba.org).

18.2 Planning for File Services

Functional overviews of each file service product are included in Section 18.1, "Overview of File Services," on page 183.

- Section 18.2.1, "Deciding Which Components Match Your Needs," on page 193
- Section 18.2.2, "Comparing Your CIFS File Service Options," on page 194
- Section 18.2.3, "Planning Your File Services," on page 195

18.2.1 Deciding Which Components Match Your Needs

To decide which file service components to install, you should match service features listed in Table 18-8 to your network's file service requirements.

Table 18-8 OES File Services Feature Breakdown

Service	Access Method Features	Back-End Storage Features	Security Features
NCP Server (NetWare Core Protocol)	Novell Client (NCP client)	◆ Any Linux volumes (including NSS) that are defined as NCP volumes ◆ NetWare volumes	◆ eDirectory Authentication

Service	Access Method Features	Back-End Storage Features	Security Features
NetStorage	◆ Any supported browsers ◆ Personal Digital Assistant (PDA) ◆ Remote (browser-based) ◆ Web Folders (on either an Internet Explorer browser or in Windows Explorer) ◆ Windows Explorer	◆ Linux POSIX volumes ◆ NetWare volumes ◆ NCP volumes ◆ NSS volumes ◆ Samba (CIFS) servers ◆ Windows (CIFS) servers	◆ Secure LDAP Authentication
Novell AFP	◆ Macintosh Chooser	◆ NSS volumes	◆ Secure LDAP Authentication
Novell CIFS	◆ Any CIFS client ◆ Remote access (Web Folders in the Internet Explorer browser) ◆ Windows Explorer	◆ NSS volumes	◆ Secure LDAP Authentication
Novell iFolder 3.8	◆ Linux File Managers ◆ Macintosh Chooser ◆ Offline access with file synchronization (between local and network copies) on reconnect ◆ Web browsers ◆ Windows Explorer	◆ Novell iFolder 3.8 Enterprise server file repository on OES 2 server	◆ Files can be encrypted for transport through SSL (HTTPS). ◆ Secure LDAP Authentication
Novell Samba	◆ Any CIFS client ◆ Remote access (Web Folders in the Internet Explorer browser) ◆ Windows Explorer	◆ Linux POSIX file system on OES 2 server ◆ NSS volumes	◆ Secure LDAP Authentication

18.2.2 Comparing Your CIFS File Service Options

OES 2 SP3 offers three file services that use the CIFS protocol: Novell CIFS, Novell Samba, and Samba in Domain Services for Windows (DSfW).

Table 18-9 *Comparing OES 2 CIFS Solutions*

Item	Novell CIFS	Novell Samba	Samba in DSfW
Authentication	A Password policy that allows the CIFS proxy user to retrieve passwords is required.	A Samba-compatible Password policy is required for compatibility with Windows workgroup authentication.	The Domain Services Password policy is required for DSfW users. The domain is set up as a trusted environment. DSfW uses Active Directory authentication methods, such as Kerberos, to ensure that only authorized users can log in to the domain.
File system support	NSS is the only file system supported for this release.	It is recommended (but not required) that you create Samba shares on NSS data volumes. NSS is fully integrated with eDirectory for easier management, and using an NSS volume allows you to take advantage of the rich data security model in NSS. You can use either iManager or the nssmu utility to create an NSS volume on an OES 2 server. For instructions on how to set up an NSS volume, see "Managing NSS Volumes" in the *OES 2 SP3: File Systems Management Guide*.	
LUM and Samba enablement	LUM and Samba enablement are not required.	Users must be enabled for LUM and Samba and assigned to a Samba group.	eDirectory users in the domain (eDirectory partition) are automatically Samba users and are enabled to access Samba shares. See "Creating Users" in the *OES 2 SP3: Domain Services for Windows Administration Guide*. Domain users are set up with the necessary UID and default group (DomainUsers) membership. Every additional eDirectory group created within the domain is automatically Linux-enabled.
Username and password	The same username and password must exist on both the Windows workstation and in eDirectory.	The same username and password must exist on both the Windows workstation and in eDirectory.	eDirectory users in the domain (eDirectory partition) can log into any workstation that has joined the domain. There is no need for a corresponding user object on the workstation.

18.2.3 Planning Your File Services

1 For the file services you plan to install, compute the total additional RAM required (above the basic system requirement).

- **NCP:** There are no additional RAM requirements.
- **NetStorage:** There are no additional RAM requirements.
- **Novell AFP:** There are no additional RAM requirements.

- **Novell CIFS:** There are no additional RAM requirements.
- **Novell iFolder 3.8:** Suggestions for calculating the additional RAM you need are contained in "Server Workload Considerations" in the *Novell iFolder 3.8 Administration Guide*.
- **Samba:** There are no additional RAM requirements.

2 Record the additional required RAM in your planning notes.

3 For the file services you plan to install, compute the total additional disk space required (above the basic system requirement).

- **NCP:** Allocate enough disk space to meet your users' file storage needs. On Linux, this space must exist on partitions you have designated as NCP volumes. On NetWare, all volumes are accessible through NCP.
- **NetStorage:** There are no disk space requirements because NetStorage provides access only to other file storage services.
- **Novell AFP:** Allocate enough disk space for the partition containing the /home directories to meet your users' file storage needs.
- **Novell CIFS:** Allocate enough disk space for the partition containing the /home directories to meet your users' file storage needs.
- **Novell iFolder 3.8:** Suggestions for calculating the additional disk space you need are contained in "Server Workload Considerations" in the *Novell iFolder 3.8 Administration Guide*.
- **Samba:** Allocate enough disk space for the partition containing the /home directories to meet your users' file storage needs.

4 Record the additional required disk space in your planning notes.

5 For the file services you plan to install, refer to the information in the OES 2 installation guides indicated in the following table and note your planning choices on your planning sheet.

File Service Product	Linux Planning References
NCP	"Novell NCP Server / Dynamic Storage Technology" in the *OES 2 SP3: Installation Guide*
NetStorage	"Novell NetStorage" in the *OES 2 SP3: Installation Guide*
Novell AFP	"Novell AFP Services" in the *OES 2 SP3: Installation Guide*
Novell CIFS	"Novell CIFS for Linux" in the *OES 2 SP3: Installation Guide*
Novell iFolder 3.8	"Novell iFolder" in the *OES 2 SP3: Installation Guide*
Samba	"Novell Samba" in the *OES 2 SP3: Installation Guide*

18.3 Coexistence and Migration of File Services

Storing shared data on network servers is only half of the picture. The other half is making it possible for users of Windows, Macintosh, and UNIX/Linux workstations to access the data. In some networks, the installation of special software is permitted on the workstations to provide client access. Others require users to be able to access shared data without installing extra software on the workstation.

This section discusses migration of the following services:

- Section 18.3.1, "Novell Client (NCP)," on page 197
- Section 18.3.2, "NetStorage," on page 197

18.3.1 Novell Client (NCP)

Novell Client for Windows is the long-standing software solution for providing NCP access to NetWare data from Windows workstations. The Novell Client extends the capabilities of Windows desktops to access the full range of Novell services, such as authentication to eDirectory, network browsing and service resolution, and secure file system access. It supports traditional Novell protocols such as NCP, RSA, and NDAP, and it interoperates with open protocols such as LDAP. For more information on the Novell Client for Windows, see the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*.

The Novell Client for Linux provides these same services for Linux workstations. For more information on the Novell Client for Linux, see the *Novell Client 2.0 SP3 for Linux Administration Guide*.

Because NCP is now available on Linux, Novell Client users can attach to OES 2 servers as easily as they have been able to attach to NetWare servers. The NCP Server for Linux enables support for login script, mapping drives to OES 2 servers, and other services commonly associated with Novell Client access.

For more information on NCP Server for Linux, see the *OES 2 SP3: NCP Server for Linux Administration Guide*.

18.3.2 NetStorage

NetStorage provides Web access to the files and directories on OES 2 servers from browsers and Web-enabled devices such as PDAs.

Because NetStorage is a service that facilitates access to file services in various locations but doesn't actually store files, there are no coexistence or migration issues to consider.

For more information about NetStorage, see the *NW 6.5 SP8: NetStorage Administration Guide* or the *OES 2 SP3: NetStorage Administration Guide*.

18.3.3 Novell AFP

Novell AFP provides native AFP protocol access from Macintosh workstations to data on OES 2 servers, offering the same basic AFP connectivity that was previously available only on NetWare. No Novell Client software is required.

For information on migrating AFP services from NetWare to OES 2, see "Migrating AFP from NetWare to OES 2 SP3 Linux " in the *OES 2 SP3: Migration Tool Administration Guide*.

18.3.4 Novell CIFS

Novell CIFS provides native CIFS protocol access from Windows workstations to data on OES 2 servers, offering the same basic CIFS connectivity that was previously available only on NetWare. No Novell Client software is required.

For information on migrating CIFS services from NetWare to OES 2, see "Migrating CIFS from NetWare to OES 2 SP3 Linux" in the *OES 2 SP3: Migration Tool Administration Guide*.

18.3.5 Novell iFolder 3.8

iFolder 3.8 supports multiple iFolders per user, user-controlled sharing, and a centralized network of servers to provide scalable file storage and secure distribution. Users can share files in multiple iFolder folders, and share each iFolder folder with a different group of users. Users control who can participate in an iFolder folder and their access rights to the files in it. Users can also participate in iFolder folders that others share with them.

Novell iFolder 3.8 is available only on OES 2.

For information on migrating from iFolder 2 to iFolder 3.8, see "Migrating iFolder 2.x" in the *OES 2 SP3: Migration Tool Administration Guide*.

18.3.6 Samba

OES 2 includes Samba software to provide Microsoft CIFS and HTTP-WebDAV access to files on the server. Like Novell CIFS, this is useful to those who don't want to use the Novell Client.

There is no migration path from Novell CIFS (NFAP) to Samba.

For more information about Samba in OES 2, see the *OES2 SP3: Samba Administration Guide*.

18.4 Aligning NCP and POSIX File Access Rights

NetWare administrators have certain expectations regarding directory and file security. For example, they expect that home directories are private and that only the directory owners can see directory contents. However, because of the differences in the NetWare Core Protocol (NCP) and POSIX file security models (see Section 22.2.1, "Comparing the Linux and the Novell Trustee File Security Models," on page 227) that is not the case by default on POSIX file systems.

Fortunately, when you install Linux User Management (LUM) in OES 2, there is an option to make home directories private. This option automatically provides the privacy that NetWare administrators are used to seeing. Unfortunately, the option only applies to newly created home directories, so there is more to understand and do if aligning access rights is an issue for you.

Use the information in this section to understand how you can configure POSIX directories to more closely align with the NCP model.

- Section 18.4.1, "Managing Access Rights," on page 199
- Section 18.4.2, "Providing a Private Work Directory," on page 200
- Section 18.4.3, "Providing a Group Work Area," on page 200
- Section 18.4.4, "Providing a Public Work Area," on page 201
- Section 18.4.5, "Setting Up Rights Inheritance," on page 201

18.4.1 Managing Access Rights

NCP directories are, by default, private. When you assign a user or a group as a trustee of a directory or file, those trustees can automatically navigate to the assigned area and exercise whatever access privileges you have assigned at that level and below. You can assign as many trustees with different access privileges as you need.

On the other hand, Linux POSIX directories can be accessed through three sets of permissions defined for each file object on a Linux system. These sets include the read (r), write (w), and execute (x) permissions for each of three types of users: the file owner, the group, and other users. The Linux kernel in OES 2 also supports access control lists (ACLs) to expand this capability. However, ACLs are outside the scope of this discussion. For more information on ACLs, see "Access Control Lists" (http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_acls.html) in the *SLES 10 SP4: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html).

The Linux `chown` command lets you change the file owner and/or group to a LUM user or a LUM-enabled group. For example, `chown -R user1 /home/user1` changes the owner of the `user1` home directory and all its subdirectories and files to user1. For more information, see the chown man page on your OES 2 server.

The Linux `chmod` command provides a very simple and fast way of adjusting directory and file access privileges for the three user types: owner, group, and other (all users). In its simplest form, the command uses three numbers, ranging from 0 through 7, to represent the rights for each of the three user types. The first number sets the rights for the owner, the second number sets the rights for the group, and the third number sets the rights for all others. Each number represents a single grouping of rights, as follows:

Number	Setting	Binary Representation
0	- - -	0 0 0
1	- - x	0 0 1
2	- w -	0 1 0
3	- w x	0 1 1
4	r - -	1 0 0
5	r - x	1 0 1
6	r w -	1 1 0
7	r w x	1 1 1

Those familiar with the binary number system find this method an easy way to remember what each number represents.

For example, the command `chmod 777 /home` would grant read, write and execute rights (7) to owner, group, and other for the /home directory, while `chmod 700 /home` would grant the three rights to only the directory owner, with group and other having no rights. `chmod 750 /home` would grant rwx rights to the owner, r-x rights to the group, and no rights to other users.

For more information about the `chmod` command, see the chmod man page on your OES 2 server.

18.4.2 Providing a Private Work Directory

To make an NCP directory private, you assign a single user as the trustee and make sure that no unexpected users or groups have trustee rights in any of the parent directories.

To provide a private work area on a Linux POSIX volume:

1 Make the user is the directory owner. For example, you could use the `chown` command to change the owner (user),

```
chown -R user: /path/user_dir
```

where *user* is the eDirectory user, *path* is the file path to the work directory, and *user_dir* is the work directory name. The -R option applies the command recursively to all subdirectories and files.

2 Grant only the user read, write, and execute rights (rwx --- ---) to the directory. For example, you could use the `chmod` command as follows,

```
chmod -R 700 /path/user_dir
```

where *path* is the file path to the work directory, and *user_dir* is the work directory name.

3 Check each parent directory in the path up to the `root (/)` directory, making sure that all users (referred to as "other users" in Linux) have read and execute rights (r-x) in each directory as shown by the third group of permissions (. . . . . . r-x). (Owner and group permissions are represented by dots because their settings are irrelevant.)

The reason for checking directories is that in the parent directories the directory owners are "other" users and they need to be able to see the path down to their own private directories.

Because r-x is the default for most directories on Linux, you probably won't need to change the permissions.

18.4.3 Providing a Group Work Area

On an NCP volume, you can provide a group work area by assigning users to a group and then granting the group trustee rights to the directory. As an alternative, if users need different levels of access within the work area, you can assign each user as a trustee and grant only the rights needed.

To provide a group work area on a Linux POSIX volume:

1 Use the `chown` command to set group ownership for the directory. For example, you could enter

```
chown -R :group /path/group_dir
```

where *group* is the group name, *path* is the file path to the work area, and *group_dir* is the group work directory. The `-R` option applies the action to all subdirectories and files in group_dir.

2 Grant the group read, write, and execute rights (. . . rwx . . .). (Owner and other permissions are represented by dots because their settings are irrelevant.)

For example, you could enter

```
chmod -R 770 /path/group_dir
```

where *path* is the file path to the work area, and *group_dir* is the group work directory. The second 7 grants rwx to the group. (The example assumes that the owner of the directory should also retain all rights. Therefore, the first number is also 7.)

3 Check each parent directory in the path up to the `root (/)` directory, making sure that the group has read and execute rights (r-x) in each directory as shown by the second group of permissions (. . . r-x . . .).

   Use the `chmod` command to adjust this where necessary by specifying the number 5 for the group permission. For more information, see "Section 18.4.1, "Managing Access Rights," on page 199."

18.4.4 Providing a Public Work Area

On an NCP volume, you can provide a public work area by assigning [Public] as a trustee and then granting the required trustee rights to the directory.

For the work area itself, you would set permissions for the owner, group, and all others to read, write, and execute rights (rwx rwx rwx) (`chmod 777`).

All others must also have read and execute rights on the system in each parent directory in the path all the way to the root of the Linux system. This means that you set permissions for all parent directories to rwx --- r-x.

To provide a public work area on a Linux POSIX volume:

1 Use the `chown` command to assign all rights (rwx) to other (all users). For example, you could enter

```
chmod -R 707 /path/group_dir
```

   where *path* is the file path to the work area, and *group_dir* is the group work directory. The third 7 grants rwx to the group. (The example assumes that the owner of the directory should also retain all rights and that the group setting is irrelevant.)

2 Check each parent directory in the path up to the `root (/)` directory, making sure that all users (other) have read and execute rights (r-x) in each directory as shown by the third group of permissions (. . . . . . rwx). (Owner and group permissions are represented by dots because their settings are irrelevant.)

   Use the chmod command to adjust this where necessary by specifying the number 5 for the other permission. For more information, see "Managing Access Rights" at the beginning of this section.

18.4.5 Setting Up Rights Inheritance

The final step in aligning POSIX rights to the NCP model is setting the Inherit POSIX Permissions volume flag in the NCP configuration file so that all files and subdirectories created in these areas inherit the same permissions as their parent directory. For instructions, see "Configuring Inherit POSIX Permissions for an NCP Volume" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.

18.5 Novell FTP (Pure-FTPd) and OES 2

FTP file services on OES 11 SP1 servers are provided by Pure-FTPd, a free (BSD), secure, production-quality and standard-conformant FTP server. The OES implementation includes support for FTP gateway functionality as on NetWare and offers a level of integration between eDirectory and Pure-FTP that allows users to authenticate to eDirectory for FTP access to the server.

This section discusses the following topics:

- Section 18.5.1, "New FTP Features Added for SP3," on page 202
- Section 18.5.2, "Configuring Pure-FTPd on an OES 2 Server," on page 202
- Section 18.5.3, "Administering and Managing Pure-FTPd on an OES 2 Server," on page 203
- Section 18.5.4, "Cluster Enabling Pure-FTPd in an OES 2 Environment," on page 207
- Section 18.5.5, "Troubleshooting PureFTPd," on page 208

18.5.1 New FTP Features Added for SP3

The ability to run multiple FTP instances and common home directory support have been added for SP3.

18.5.2 Configuring Pure-FTPd on an OES 2 Server

Edit the `/etc/pure-ftpd/pure-ftpd.conf` file to configure the Pure-FTPd server.

NOTE: All the Pure-FTPd users must be LUM enabled on the server.

The following table lists the recommended configuration parameters for Pure-FTPd.

Table 18-10 *Configuration Parameters*

Parameter	Description
DefaultHomeDirectory /tmp	Default home directory of the user.
ChrootEveryone no	Cage in every user in his home directory.
MaxClientsNumber 10	Maximum numbers of clients that can simultaneously access the server.
PassivePortRange 40000 40020	Port range for passive connection replies. Range must be a minimum of 2*MaxClientsNumber.
MaxClientsPerIP 3	Maximum number of sim clients with the same IP address
NoRename yes|no	Set to *yes* if you do not want the users to rename the files
remote_server yes	Enables remote server navigation for the FTP server ChrootEveryone parameter is required for remote_server to be enabled
disallow_list_oes_server yes	Disables the `site slist` from listing the OES servers
edir_ldap_port 389	LDAP port of the eDirectory server

Parameter	Description
AnonymousOnly no	Enables authenticated connection to pure-ftp server
NoAnonymous yes	Disables anonymous connection
ChrootEveryone no	Allows the user to browse outside the home directory. This configuration is required for remote server navigation

18.5.3 Administering and Managing Pure-FTPd on an OES 2 Server

Starting Pure-FTPd

Start the Pure-FTPd server using the `rcpure-ftpd` command.

Initializing Multiple Instances

Pure-FTPd is loaded by using a configuration file. Multiple instances of Pure-FTPd can be loaded using different configuration files.

By default, an instance of Pure-FTPd using `/etc/pure-ftpd/pure-ftpd.conf` file is loaded at the boot time by init.d script. For loading multiple instances, new configuration files need to be created.

To load a new instance of Pure-FTPd:

1. Create a new configuration file for each instance.

   For example: Copy `/etc/pure-ftpd/pure-ftpd.conf` to a different location. Rename the file to `pure-ftpd1.conf` and move it to `/etc/opt/novell/pure-ftpd1.conf`.

2. Modify the following settings in the configuration file to avoid IP address or port conflicts between the instances:

   - **PIDFile:** Points to the full path of the PID file created by the pure-ftpd instance. PID file is used for unloading a particular instance of pure-ftpd. Hence, ensure that the PID File path is unique for every instance.

     For example: `/var/run/pure-ftp1.pid`, `/var/run/pure-ftp2.pid`.

   - **Bind:** By default, pure-ftpd binds to all the IP addresses on the system and listens to requests over port 21. Modify the settings of the bind such that all the pure-ftpd instances bind to different IP addresses or port combinations.

     also, modify the settings in the `/etc/pure-ftpd/pure-ftpd.conf` to avoid any IP address or port conflict from the second instance.

     For example: If a system has two interfaces with two IP addresses 10.1.1.1 and 10.1.1.2, then the bind setting for two pure-ftpd instances can be *Bind 10.1.1.1,21* and *Bind 10.1.1.2,21*.

3 Load the new instance using `/usr/sbin/pure-config.pl <`*`Full path of the config file`*`>`

For example: `/usr/sbin/pure-config.pl /etc/opt/novell/pureftpd-confs/pure-ftpd1.conf` loads an instance using the config file `/etc/opt/novell/pureftpd-confs/pure-ftpd1.conf`.

Verifying the Load of a New Instance

Use the following methods to verify that the new instance of pure-ftpd is successfully loaded:

- The `ps -eaf | grep pure-ftpd` command lists all the instances of pure-ftpd loaded on the system.
- The PID file as specified using the PIDFile in the configuration file must be created.
- An FTP connection from the client to the server over the IP address being used by the pure-ftpd instance must be created.

Unloading Specific Instances

A new script `pure-ftp-stop.pl` is added to unload an instance of pure-ftpd and all its child processes. Full path of the configuration file used to load the instance of pure-ftpd must be passed to the `pure-ftp-stop.pl` script.

For example: `/usr/sbin/pure-ftp-stop.pl /etc/opt/novell/pureftpd-confs/pure-ftpd1.conf` unloads the instance of pure-ftpd loaded using `/etc/opt/novell/pureftpd-confs/pure-ftp1.conf`.

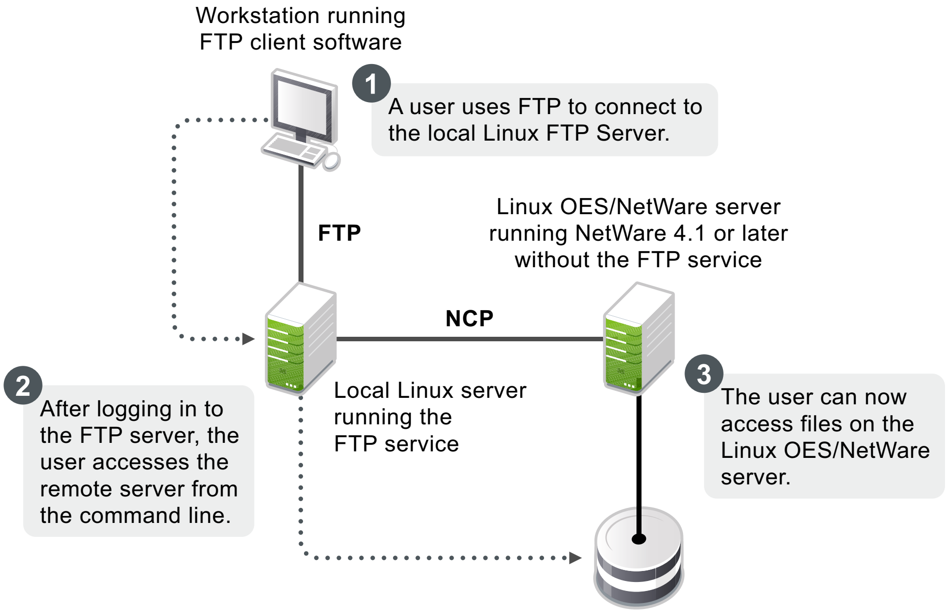
The PIDFile of the pure-ftpd instance is also used for unloading the pure-ftpd instance.

Verifying the Unload of a New Instance

- The PID file specified using the PIDFile in the configuration file must be deleted.
- The number of instances displayed by `ps -eaf | grep pure-ftpd` must reduce.
- An FTP connection request to the server must error out.

Pure-FTPd Remote Access Implementation

After logging in to the eDirectory tree, users can access files and directories on a remote Linux server whether or not the server is running Linux FTP Server software. The remote server can be another Linux OES server or an IBM server if they are in the same tree.


Workstation running
FTP client software
1
A user uses FTP to connect to the local Linux FTP Server.
FTP
Linux OES/NetWare server running NetWare 4.1 or later without the FTP service
NCP
2
After logging in to the FTP server, the user accesses the remote server from the command line.
Local Linux server running the FTP service
3
The user can now access files on the Linux OES/NetWare server.

The NCP protocol lets you transfer files and navigate to and from remote eDirectory servers.

To navigate to remote servers, use the following command:

```
cd //remote server name/volume/directory pathname
```

File operations such as `get`, `put`, and `delete` can be used on the remote server, even without changing the directory path to that server.

For example:

```
get //remote_server_name/volume/directory path/filename
```

The double slash (//) indicates that the user wants to access a remote server. After the double slash, the first entry must be the name of the remote server.

Configuring Pure-FTPd

Configuration file: /etc/pure-ftpd/pure-ftpd.conf

The configuration parameters for remote server navigation are as follows:

Entry	Value	Function
remote_server	yes	Enables remote server navigation for the Pure-FTPd server.
disallow_list_oes_server	yes	Disables SITE SLIST command for listing OES machines.
edir_ldap_port	389	eDirectory LDAP port

The following configuration parameters needs to be set for remote server navigation:

Entry	Value	Reason Why
ChrootEveryone	no	Option yes restricts users to login only to his home directory and cannot navigate to other directories including remote OES servers.
ChrootEveryone	no	Option yes restricts users to login only to his home directory and cannot navigate to other directories including remote OES servers.
AnonymousOnly	no	Option yes allows only anonymous logins.

Path Formats

Table 18-11 *Linux FTP Server path formats*

Task	Command Format
Specifying the volume and directory path name	//server_name/volume_name/directory_path
Navigating to different volumes	cd //server_name/volume_name
Switching back to the home directory	cd ~
Switching to home directory of any user	cd ~user_name
Switching to the root of the server	cd /

NOTE: The Linux FTP Server does not support wildcards at the root of the server.

SITE Command

The `SITE` command enables FTP clients to access features specific to the Linux FTP Server.

NOTE: The `SITE` command is not case sensitive if entered from an FTP client.

The `SITE` command has the following syntax:

```
SITE [SLIST]
```

NOTE: The settings done through `SITE` commands are valid only for the current session.

This command is unique to the Linux FTP service and are not standard FTP commands.

Table 18-12 provides the `SITE` command along with the description:

Table 18-12 *Linux FTP SITE command*

Command	Description
`SLIST`	Lists all the OES servers within the eDirectory tree.

NOTE: All the FTP users needs to be LUM-enabled on the FTP server.

18.5.4 Cluster Enabling Pure-FTPd in an OES 2 Environment

You can configure Pure-FTPd server in active/active mode of Novell Cluster Services.

Prerequisites

- Novell Cluster Services is installed and setup.

  For step-by-step information on setting up Novell Cluster Services, refer to "Installing and Configuring Novell Cluster Services on OES 2 Linux" in the "*OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*."

Active/Active Mode

In active/active cluster mode, multiple instances of FTP server runs on a single node cluster.

Pure-FTPd must be associated with a shared NSS volume and the DefaultHomeDirectory of users must be on the shared NSS volume.

Configuring Active/Active Mode

1. Install pure-ftpd on all the cluster nodes by selecting *Novell FTP* in the OES install. Upgrade pure-ftpd on all the nodes with the test RPM.
2. Enable hard links on the shared NSS volumes.
3. Create a unique configuration file for every FTP server to be associated with a shared NSS volume. Ensure that:
   - The Bind setting in the configuration file is same as the IP Address of the virtual server created for the NSS pool.
   - The PID file must be unique for each FTP instance running on the cluster.
4. Copy the configuration file to the shared volume to `/etc/opt/novell` on the shared volume. Copying the configuration file to the shared volume, the file is automatically moved across the nodes with the volume and is always available to the FTP Server.

   For exmaple: If the shared volume is FTPVol1, the path to copy the configuration file is `/media/nss/FTPVol1/etc/opt/novell/pure-ftpd`.
5. Configure all the FTP servers for DefaultHomeDirectory support. As NSS volume is shared, the DefaultHomeDirectory in the configuration file must be on the shared volume.

   For example: If `FTPVol1` is the shared volume attached to an FTP Server, DefaultHomeDirectory in the configuration file is `/media/nss/FTPVol1/FTPShare`.
6. Update the load and unload scripts of the cluster resource.
   - **Load script:** Add the following command to load the FTP server with the shared volume:

```
/usr/sbin/pure-config.pls <Full Path to configuration file>
```

   For example: If the shared volume is FTPVol1 and the Pure-FTP configuration file is `/etc/opt/novell/pure-ftpd/ftpvol1.conf` on FTPVol1, the pure-ftpd load command in the load script is `exit_on_error /usr/sbin/pure-config.pl /media/nss/FTPVol1/etc/opt/novell/pure-ftpd/ftpvol1.conf`.

   - **Unload script:** Add the following command to unload the FTP server:

```
/usr/sbin/pure-ftp-stop.pl <Full Path to configuration file>
```

   Configuration file path must be same as the one passed to pure-config.pl in the load script.

NOTE: In iManager, load and unload the cluster resources. Pure-ftpd instances must be loaded along with the shared NSS volumes. Migrate the pure-ftpd instances when the associated shared volumes are moved across the cluster nodes.

18.5.5 Troubleshooting PureFTPd

Home Directory Not Found

Error: Home directory not available

Cause: Either the user's home directory is missing or the configured default home directory is not available.

Action: Edit the FTP configuration file to point to the available home directory or create the default directory in the file system.

18.6 NCP Implementation and Maintenance

If you have installed the NCP server for OES, eDirectory/Novell Client users can access files on the OES 2 server with no additional configuration.

The implementation information in the following sections can help you get started with NCP on OES 2 servers.

- Section 18.6.1, "The Default NCP Volume," on page 208
- Section 18.6.2, "Creating NCP Home and Data Volume Pointers," on page 208
- Section 18.6.3, "Assigning File Trustee Rights," on page 209
- Section 18.6.4, "NCP Caveats," on page 209
- Section 18.6.5, "NCP Maintenance," on page 209

18.6.1 The Default NCP Volume

The NCP Server for OES enables NCP access to NCP and NSS volumes defined on the OES 2 server. When you install the NCP server, the installation creates one NCP volume named `SYS:` that maps to the `/usr/novell/sys` folder on the OES server.

This NCP volume contains `LOGIN` and `PUBLIC` directories that, in turn, contain a small subset of the files traditionally found on a NetWare server in the directories with the same names.

18.6.2 Creating NCP Home and Data Volume Pointers

Initially, there are no NCP home directories or data volumes available to Novell Clients that attach to an OES 2 server.

For existing eDirectory users: If you want users to have NCP home or data directories on the server, you must decide where you want these directories to reside on the server's partitions and then create NCP volumes by using the NCPCON utility at the terminal prompt.

For example, if you wanted to create an NCP volume (pointer) named `HOME` and mount it to the `/usr` folder on the Linux server, you would enter the following command at the command prompt:

```
ncpcon create volume HOME /usr
```

After issuing this command, when a Novell Client attaches to the OES 2 server, the `HOME:` volume appears along with the `SYS:` volume created by the installation.

For new eDirectory users: If you create an NCP or NSS volume on the server prior to creating users, then you have the option of specifying that volume in iManager as the location of the home directory for the new users.

IMPORTANT: NCP Volume pointers are always created with uppercase names (`HOME:`, `SYS:`, etc.) regardless of the case specified when the volume pointers are created.

18.6.3 Assigning File Trustee Rights

You can use the same methods for assigning file trustee rights on NCP volumes on OES 2 servers that you use when assigning them on NetWare. For example, the Novell Client can be used by anyone with the Access Control right on the volume, or the root user can use the ncpcon utility > `rights` command at a command prompt to administer NCP trustee rights. See "Managing File System Trustees, Trustee Rights, and Attributes on NCP Volumes"in the *OES 2 SP3: NCP Server for Linux Administration Guide*. (The ncpcon `rights` command is related to but not the same as the rights utility used to manage trustees on NSS volumes.)

18.6.4 NCP Caveats

Starting with OES 2 SP2, cross-protocol file locking (CPL) is enabled by default on all new servers with NCP installed. For more information, see Section 1.5.5, "Cross-Protocol File Locking Change," on page 19.

18.6.5 NCP Maintenance

Because NCP provides Novell Client access to files on NetWare and OES 2 servers, the service is covered by maintenance tasks that apply to file systems on these servers. For information on maintaining file services, see the "storage/file systems (http://www.novell.com/documentation/oes2/storage.html)" section in the online documentation.

18.7 NetStorage Implementation and Maintenance

The following sections are provided only as introductory information. For more information about using NetStorage, see the *OES 2 SP3: NetStorage Administration Guide*.

- Section 18.7.1, "About Automatic Access and Storage Locations," on page 210
- Section 18.7.2, "About SSH Storage Locations," on page 210
- Section 18.7.3, "Assigning User and Group Access Rights," on page 210
- Section 18.7.4, "Authenticating to Access Other Target Systems," on page 211
- Section 18.7.5, "NetStorage Authentication Is Not Persistent by Default," on page 211
- Section 18.7.6, "NetStorage Maintenance," on page 211

18.7.1 About Automatic Access and Storage Locations

The inherent value of NetStorage lies in its ability to connect users with various servers and file systems. Some connections are created automatically depending on the OES platform where NetStorage is installed. Other connections must be created by the network administrator.

In summary, NetStorage provides automatic access to:

- NSS volumes on the same server that use the default mount point (/media/nss)
- User Home directories that are specified in eDirectory on NCP or NSS volumes.
- Drive mapping locations in login scripts of the user logging in (if the NCP Server for Linux is running on the server)

To provide access to file systems not listed above, you must create Storage Location objects in eDirectory. For instructions on creating Storage Locations, see "Creating a Storage Location Object" in the *OES 2 SP3: NetStorage Administration Guide*.

18.7.2 About SSH Storage Locations

If you plan to use SSH storage locations, be aware that by default any users who are enabled for Samba cannot access data stored at the SSH locations. Additional steps are required to grant simultaneous access to Samba and SSH. For more information, see Section 12.4, "SSH Services on OES 2," on page 95.

18.7.3 Assigning User and Group Access Rights

Because NetStorage provides access to other file storage systems, the users and groups that access the other systems through NetStorage must be created and granted file and directory access on those systems.

For example:

- eDirectory users must exist in the eDirectory tree where the OES server resides and have access rights to the files and directories on the OES server.
- Windows users must exist on the Windows systems and have the required access rights to the files and directories on those systems.
- If your users will access Samba files on an OES 2 server, they must be enabled for LUM and Samba access on the OES 2 server. For more information, see "Services in OES 2 That Require LUM-Enabled Access" on page 156.

IMPORTANT: The usernames and passwords used to authenticate to the NetStorage (OES) server through eDirectory must match the usernames and passwords defined on the target systems.

18.7.4 Authenticating to Access Other Target Systems

The OES installation establishes a primary authentication domain for NetStorage. To access any storage location, users must exist somewhere in this primary domain. When it receives an authentication request, NetStorage searches for the username in the context you specified during OES installation and in all its subcontexts.

Authentication to other file systems is often controlled by other authentication domains. For example, you might create a storage location on the OES 2 server that points to a legacy NetWare server that resides in a different eDirectory tree. To access this storage location, users must authenticate to the other tree.

This means that you must specify an additional context in the NetStorage configuration as a non-primary authentication domain.

When defining a non-primary authentication domain, you must

- Ensure that the username and password in the non-primary domain matches the username and password in the primary domain.
- Specify the exact context where User objects reside. NetStorage doesn't search the subcontexts of non-primary authentication domains.

For more information about managing NetStorage authentication domains, see "Authentication Domains" in the *OES 2 SP3: NetStorage Administration Guide*.

18.7.5 NetStorage Authentication Is Not Persistent by Default

By default, users must reauthenticate each time they access NetStorage in a browser. This is true even if another browser window is open and authenticated on the same workstation.

The reason for this is that persistent cookies are not enabled by default.

This setting can be changed. For more information, see "Persistent Cookies" in the *OES 2 SP3: NetStorage Administration Guide*.

18.7.6 NetStorage Maintenance

Your NetStorage installation can change as your network changes and evolves by providing access to new or consolidated storage locations. For information about the kinds of tasks you can perform to keep your NetStorage implementation current, see the *OES 2 SP3: NetStorage Administration Guide*.

18.8 Novell AFP Implementation and Maintenance

To use the Novell implementation of AFP file services on your OES 2 server, you must install the service by using the instructions in the *OES 2 SP3: Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in "Installing AFP after the OES 2 SP3 Installation" in the *OES 2 SP3: Novell AFP For Linux Administration Guide*.

- Section 18.8.1, "Implementing Novell AFP File Services," on page 212
- Section 18.8.2, "Maintaining Novell AFP File Services," on page 212

18.8.1 Implementing Novell AFP File Services

NOTE: If you are new to OES, we recommend the *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare* for an introduction to creating and working with eDirectory objects and OES 2 file services, including Novell AFP.

All eDirectory users can access the AFP file services on an OES 2 server as they would any Macintosh server.

18.8.2 Maintaining Novell AFP File Services

Information on maintaining your AFP installation is found in the *OES 2 SP3: Novell AFP For Linux Administration Guide*.

18.9 Novell CIFS Implementation and Maintenance

To use the Novell implementation of CIFS file services on your OES 2 server, you must install the service by using the instructions in the *OES 2 SP3: Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in "Installing and Configuring a CIFS Server through YaST" in the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

- Section 18.9.1, "Implementing Novell CIFS File Services," on page 212
- Section 18.9.2, "Maintaining Novell CIFS File Services," on page 212

18.9.1 Implementing Novell CIFS File Services

NOTE: If you are new to OES, we recommend the *OES 2 SP3: Getting Started with OES 2 and Virtualized NetWare* for an introduction to creating and working with eDirectory objects and OES 2 file services, including Novell CIFS.

All eDirectory users can access the CIFS file services on an OES 2 server as they would any Windows workgroup server.

For instructions on implementing Novell CIFS, see "Planning and Implementing CIFS" in the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

18.9.2 Maintaining Novell CIFS File Services

Information on maintaining your CIFS installation is found in the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

18.10 Novell iFolder 3.8 Implementation and Maintenance

IMPORTANT: iFolder 3.8 documentation is no longer published in HTML format. Therefore, linking directly to the iFolder 3.8 documentation is no longer possible. You must download the PDF version of the iFolder 3.8.4 documentation and manually find the sections referenced in this section.

The following implementation pointers are provided only as introductory information. To begin using Novell iFolder, see the *Novell iFolder 3.8 Administration Guide*.

- Section 18.10.1, “Managing Novell iFolder 3.8,” on page 213
- Section 18.10.2, “Configuring Novell iFolder 3.8 Servers,” on page 213
- Section 18.10.3, “Creating and Enabling Novell iFolder 3.8 Users,” on page 213
- Section 18.10.4, “Novell iFolder 3.8 Maintenance,” on page 213

18.10.1 Managing Novell iFolder 3.8

You manage Novell iFolder through the iFolder Management Console, which you can access directly or through iManager. For more information, see “Installing and Configuring iFolder Services” in the *Novell iFolder 3.8 Administration Guide*.

18.10.2 Configuring Novell iFolder 3.8 Servers

Before you let users log in to the Novell iFolder 3.8 server, be sure you complete all the setup tasks in “Installing and Configuring iFolder Services” (including “Configuring the iFolder Web Admin Server” if applicable) in the *Novell iFolder 3.8 Administration Guide*.

18.10.3 Creating and Enabling Novell iFolder 3.8 Users

To provide user access to Novell iFolder 3.8:

1. Provision eDirectory User objects for iFolder 3.8.
2. Enable the User Account Policies for iFolder access.
3. (Optional) Enable Account Quotas (space limits) for the user accounts.
4. Create iFolders for users.
5. Distribute the iFolder Client to users.

For more information, see “Locating the Users in the Search Results” in the *Novell iFolder 3.8 Administration Guide*.

18.10.4 Novell iFolder 3.8 Maintenance

As the Novell iFolder service load increases, you might need to increase the server capacity or add additional servers. For help, see “Deploying iFolder Server ” in the *Novell iFolder 3.8 Administration Guide*.

18.11 Samba Implementation and Maintenance

To use the Novell implementation of Samba file services on your OES 2 server, you must install the service by using the instructions in the *OES 2 SP3: Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in “Installing Samba for OES 2” in the *OES2 SP3: Samba Administration Guide*.

- Section 18.11.1, “Implementing Samba File Services,” on page 214
- Section 18.11.2, “Maintaining Samba File Services,” on page 214

18.11.1 Implementing Samba File Services

All users whose accounts have been enabled for Samba access can access the OES 2 server as they would any Windows server.

For instructions on implementing Samba, see "Installing Samba for OES 2" in the *OES2 SP3: Samba Administration Guide*.

18.11.2 Maintaining Samba File Services

Information on maintaining your Samba installation is found in the *OES2 SP3: Samba Administration Guide*.

19 Search Engine (QuickFinder)

Open Enterprise Server 2 includes the Novell QuickFinder Server. QuickFinder lets you add search functionality to any Web site or internal intranet. It can index and find matches within a wide variety of data types. It also supports rights-based searches so that users see only what they have rights to see, depending on the type of index created and the file system indexed.

QuickFinder replaces the NetWare Web Search Server that was available in NetWare 6.5 SP3 and earlier. When you upgrade a NetWare server running NetWare Web Search Server to NetWare 6.5, Web Search Server is automatically upgraded to QuickFinder. The upgrade identifies all the configuration settings and indexes from Web Search and enables them to be used by QuickFinder.

When indexing a file system, the QuickFinder engine indexes only what it has rights to see. On NetWare, it has full access to all mounted volumes. On Linux, it has rights to only the files that the `wwwrun` user and the `www` group have rights to see.

For more information, see the topics in "Search Engine (http://wwwtest.provo.novell.com/documentation/oes2/search-engine.html#search-engine)" in the OES 2 online documentation or refer to the *OES 2 SP3: Novell QuickFinder Server 5.0 Administration Guide*.

20 Print Services

Open Enterprise Server 2 includes Novell iPrint, a powerful and easy-to-implement printing solution that provides print-anywhere functionality to network users. iPrint lets Windows, Linux, and Macintosh users quickly locate network printers through a Web browser, easily install and configure a located printer through a native printer installation method, and print to installed printers from any location through an IP connection.

This section contains the following information:

20.1 Overview of Print Services

Novell iPrint lets Linux, Macintosh, and Windows users

- Quickly locate network printers through a Web browser.
- Easily install and configure a located printer through a native printer installation method.
- Print to installed printers from any location (including the Web) through an IP connection.

The information in this section provides a high-level overview of Novell iPrint print services. It is designed to acquaint you with basic iPrint functionality so you understand the configuration steps you need to perform to provide iPrint print services, and understand how iPrint functions from the user’s perspective.

20.1.1 Using This Overview

If you already know that you want to provide OES print services for your users and you understand how iPrint works, skip the overviews and continue with Section 20.2, “Planning for Print Services,” on page 220.

If you want to learn more about iPrint, continue with this overview section.

20.1.2 iPrint Components

A Novell iPrint installation consists of various components, most of which are represented by objects in your eDirectory tree:

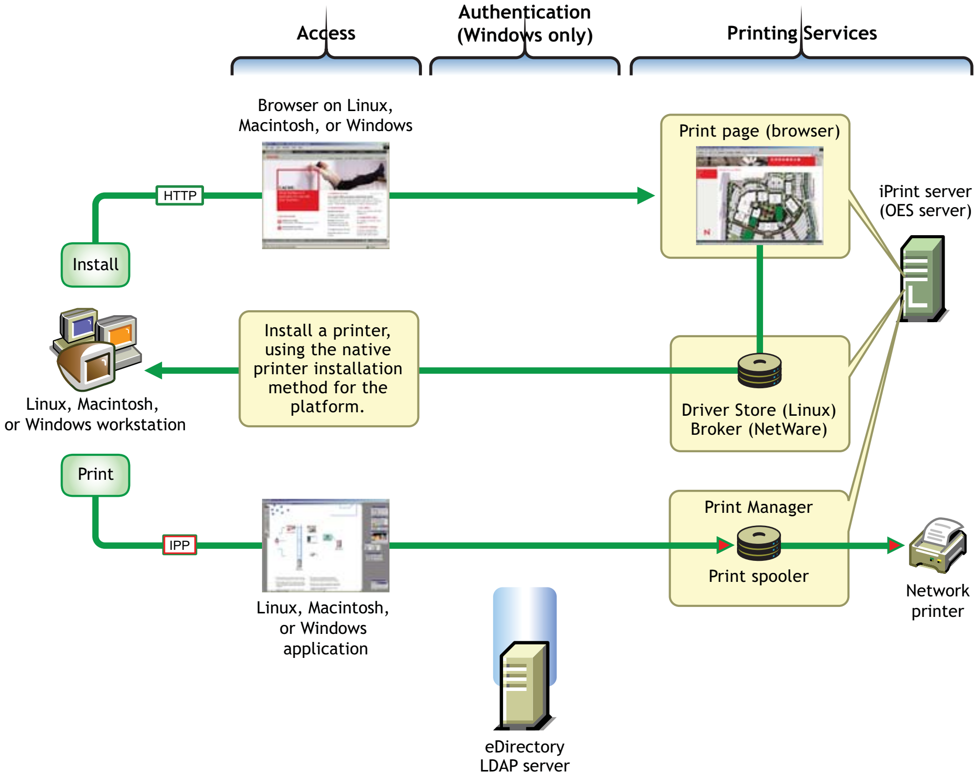
- **Print Driver Store (Linux):** This is a repository that stores the drivers on an OES 2 server for your network printers. It is the first component you configure and is represented by an eDirectory object that you create.
- **Print Broker (NetWare):** This is a repository that stores the drivers on an NetWare 6.5 SP8 server for your network printers. It is the first component you configure and is represented by an eDirectory object that you create.
- **Printer Drivers:** These are the platform-specific printer drivers and PostScript* Printer Description (PPD) files that are stored in the Driver Store or Broker and are installed on workstations when users select a target printer. Printer drivers and PPD files exist as file structures within the Driver Store and Broker and are not represented by objects in eDirectory.
- **Printer Objects:** These are eDirectory objects you create that store information about the printers available through iPrint. The information stored in an object is used each time its associated printer is added to a workstation's list of available printers.
- **Print Manager:** This is a daemon that runs on OES 2 or an NLM that runs on the NetWare 6.5 SP8 server. It receives print jobs from users and forwards them to the target printer when it is ready. It is represented by and controlled through an eDirectory object that you can configure.
- **iPrint Client:** This is a set of browser plug-ins. On Macintosh and Windows workstations it is automatically installed the first time it interacts with iPrint. On Linux workstations, it must be installed manually. The client is required on each platform to navigate through the iPrint Web pages, select a target printer, and install the print driver.

For more information on iPrint, see "Print Services (http://wwwtest.provo.novell.com/documentation/oes2/print-services.html#print-services)" in the OES online documentation.

20.1.3 iPrint Functionality

Figure 20-1 describes how iPrint functions from a user workstation perspective.

Figure 20-1 How iPrint Works



The following table explains the information illustrated in Figure 20-1.

Table 20-1 iPrint Functionality

Access	Authentication	Printing Services
The iPrint Client must be installed on each workstation accessing iPrint services. A user needing to use a printer for the first time accesses the organization's print page on the Web. When the user selects the target printer, its platform-specific driver is automatically installed and configured. After printer installation, users can print to the printer from any application.	You can require authentication for Windows users if needed. The option to require authentication is not available for Linux and Macintosh users. Although shown separately, eDirectory could be installed on the OES 2 server.	Users with the iPrint Client installed and access to the OES 2 server can install printer drivers and print to iPrint printers. By default, iPrint generates a printer list for the printers hosted on the server. A customized Web page lets users browse to the target printer by using location lists and maps that you have previously created for the site where the printer is located.

20.2 Planning for Print Services

Consider the following information as you plan your iPrint installation:

- We recommend that you record your decisions in planning notes for future reference.
- iPrint has no additional RAM requirements.
- Most iPrint installations (even in large enterprises) do not require additional disk space for associated print job spooling.

  However, if you anticipate very heavy print usage and want to plan for additional disk space in that regard, the iPrint spooler area is located in the `/var` partition or directory structure on OES 2 servers. On NetWare servers, you designate the location when creating the Print Manager object.
- To finish planning your iPrint installation, refer to the information in "Novell iPrint" in the *OES 2 SP3: Installation Guide*

20.3 Coexistence and Migration of Print Services

If you select iPrint during the OES server installation, the iPrint software components are automatically installed on the server. Although the Common UNIX Printing System (CUPS) software is also installed with SLES 10, CUPS is disabled to avoid port 631 conflicts.

For information on upgrading from NetWare queue-based printing, Novell Distributed Print Services (NDPS), or previous versions of iPrint, see "Installing iPrint Software" in the *NW 6.5 SP8: iPrint Administration Guide*.

For more information on configuring iPrint on OES, see "Installing and Setting Up iPrint on Your Server" in the *OES 2 SP3: iPrint for Linux Administration Guide*.

In OES SP2, migrating iPrint services from a NetWare server to an OES 2 server is supported by the OES 2 Migration Tool. For more information, see "Migrating iPrint from NetWare or OES 2 Linux to OES 2 SP3 Linux" in the *OES 2 SP3: Migration Tool Administration Guide*.

20.4 Print Services Implementation Suggestions

This section provides only summary implementation information. For complete iPrint documentation, see the *OES 2 SP3: iPrint for Linux Administration Guide*.

- Section 20.4.1, "Initial Setup," on page 220
- Section 20.4.2, "Implementation Caveats," on page 221
- Section 20.4.3, "Other Implementation Tasks," on page 221

20.4.1 Initial Setup

After your OES 2 server is installed, you must do the following to complete your iPrint installation:

1. Create a Driver Store on OES 2 or a Broker on NetWare 6.5 SP8 to store the print drivers.

   These eDirectory objects store the drivers for your network printers on Linux and NetWare servers, respectively. Each Printer object you create for your network needs to reference a printer driver in Driver Store/Broker. When users subsequently install printers, the correct drivers for the platform running on their workstation are downloaded from the Driver Store and installed.

You create the Driver Store through iManager. For specific instructions, see “Creating a Driver Store” in the *OES 2 SP3: iPrint for Linux Administration Guide*

2 Add a printer driver to the Driver Store or Broker for each printer/platform combination needed.

For example, If you have Windows XP, Windows 2000, and Novell Linux Desktop (NLD) workstations on your network and you have four different printer types, you need to add four printer drivers for each platform (a total of 12 printer drivers) to the Driver Store or Broker.

You add printer drivers to the store through iManager. For specific instructions, see “Updating Printer Drivers” in the *OES 2 SP3: iPrint for Linux Administration Guide*

3 Create a Print Manager object.

The Print Manager receives print jobs from users and forwards them to the target printer when it is ready. The Print Manager must be running for you to create Printer objects.

The Print Manager is an object you create in eDirectory and is usually started and stopped through iManager.

You create the Print Manager object through iManager. For specific instructions, see “Creating a Print Manager” in the *OES 2 SP3: iPrint for Linux Administration Guide*

4 Create Printer objects.

You must create a Printer object for each printer you want users to access through iPrint. These objects store information about the printer that is used each time the printer is installed on a workstation.

You create Printer objects through iManager. For specific instructions, see “Creating a Printer” in the *OES 2 SP3: iPrint for Linux Administration Guide*

5 (Optional) Create location-based, customized printing Web pages.

By default, each iPrint installation includes the creation of a Default Printer List Web page that users can access to install iPrint printers.

You have the option of enhancing the browsing experience by creating location-based printing Web pages that feature either lists of printers by location, maps of the buildings showing each printer, or a combination of both.

If your organization is located at multiple sites or even in a building with multiple floors, providing location-based print Web pages can greatly simplify printing for your users.

Your iPrint installation contains the iPrint Map Designer to help you easily create location maps with clickable printer icons. For more information, see “Setting Up Location-Based Printing” in the *OES 2 SP3: iPrint for Linux Administration Guide*

6 Provide instructions to users for accessing iPrint printers.

After performing the steps above, your network is ready for iPrint functionality. You need only tell users how to access your printing Web pages; Novell iPrint does the rest.

20.4.2 Implementation Caveats

There are a few implementation caveats relating to iPrint on Linux. See “iPrint” on page 69.

20.4.3 Other Implementation Tasks

In addition to the tasks described in Section 20.4.1, “Initial Setup,” on page 220, there are additional tasks you might want or need to consider. To see a list of potential tasks, refer to the “Print Services (http://wwwtest.provo.novell.com/documentation/oes2/print-services.html#print-services)” links in the OES online documentation.

20.5 Print Services Maintenance Suggestions

As you add printers to your network or move them to different locations, be sure to update your iPrint installation to reflect these changes.

After your installation is completed and users are printing, you can monitor print performance by using the information located in "Using the Print Manager Health Monitor" in the *OES 2 SP3: iPrint for Linux Administration Guide*

For more information on iPrint and its functionality within OES, see the "Print Services (http://wwwtest.provo.novell.com/documentation/oes2/print-services.html#print-services)" links in the online documentation.

21 Web Services

The Web and application services in Open Enterprise Server 2 support the creation and deployment of Web sites and Web applications that leverage the widespread availability of Internet-based protocols and tools.

With the proper Web components in place, a server can host dynamic Web sites where the content changes according to selections made by the user. You can also run any of the hundreds of free Web applications that can be downloaded from the Internet. Web and application services make it easy to build your own dynamic Web content and create customized Web database applications.

See the topics in “Web Services (http://wwwtest.provo.novell.com/documentation/oes2/web-services.html#web-services)” in the OES online documentation.

Apache

Apache Web Server 2.0 is the most popular Web server on the Internet.

For additional information, see Apache.org Web site (http://www.apache.org).

Tomcat

Tomcat is used to run basic Java servlet and JavaServer Pages (JSP) applications.

For information, see the Apache Jakarta Tomcat 5.5 Web site (http://tomcat.apache.org/tomcat-5.5-doc/index.html).

22 Security

This section contains the following topics:

22.1 Overview of OES Security Services

This section provides specific overview information for the following key OES components:

For more authentication and security topics, see the OES online documentation (http://wwwtest.provo.novell.com/documentation/oes2/security.html#security).

22.1.1 Application Security (AppArmor)

Novell AppArmor provides easy-to-use application security for both servers and workstations. You specify which files a program can read, write, and execute.

AppArmor enforces good application behavior without relying on attack signatures and prevents attacks even if they are exploiting previously unknown vulnerabilities.

For more information, see the Novell AppArmor Documentation Web site (http://www.novell.com/documentation/apparmor/index.html).

22.1.2 NSS Auditing Engine

OES 2 SP3 includes the NSS Auditing Engine, which is installed by default with NSS.

The auditing engine provides an interface for auditing client applications, such as Novell Sentinel and various third-party products to access. Information about the auditing engine SDK is available on the Novell Web site (http://developer.novell.com/wiki/index.php/NSS_Auditing_SDK).

Using the SDK, client applications can be developed to audit various NSS file system operations on files and directories, including:

- delete
- create
- open
- close
- rename
- link
- metadata modified
- trustee add/delete
- inherited rights modified

Novell Sentinel Log Manager 90-Day Free Trial

Novell Sentinel Log Manager runs on a 64-bit SLES 11 host. You can download the suite from the Novell Download Web site (http://download.novell.com/Download?buildid=o8BgsbCidWg~). For installation and usage instructions, see the Novell Log Management Readme and Release Notes included as a link on the download page.

Third-Party Partner Applications

The following Novell partners are currently developing applications for use with the NSS Auditing Engine:

- Blue Lance
- NetVision
- Symantec

22.1.3 Encryption (NICI)

The Novell International Cryptography Infrastructure (NICI) is the cryptography service for Novell eDirectory, Novell Modular Authentication Services (NMAS), Novell Certificate Server, Novell SecretStore, and TLS/SSL.

Key Features

NICI includes the following key features:

- Industry standards: It implements the recognized industry standards.
- Certified: It is FIPS-140-1 certified on selected platforms.
- Cross-platform support: It is available on both OES platforms.
- Governmental export and import compliance: It has cryptographic interfaces that are exportable from the U.S. and importable into other countries with government-imposed constraints on the export, import, and use of products that contain embedded cryptographic mechanisms.
- Secure and tamper-resistant architecture: The architecture uses digital signatures to implement a self-verification process so that consuming services are assured that NICI has not been modified or tampered with when it is initialized.

Never Delete the NICI Configuration Files

In the early days of NICI development, some NICI problems could be solved only by deleting the NICI configuration files and starting over. The issues that required this were solved years ago, but as is often the case, the practice persists, and some administrators attempt to use this as a remedy when they encounter a NICI problem.

No one should ever delete the NICI configuration files unless they are directly told to do so by a member of the NICI development team. And in that rare case, they should be sure to back up the files before doing so. Failure to do this makes restoring NICI impossible.

More Information

For more information on how to use NICI, see the *Novell International Cryptographic Infrastructure (NICI) 2.7.6 Administration Guide*.

22.1.4 General Security Issues

In addition to the information explained and referenced in this section, the OES online documentation contains links to "General Security Issues" (http://www.novell.com/documentation/oes2/security.html#b1349evx).

22.2 Planning for Security

This section discusses the following topics. For additional planning topics, see the Security section in the OES online documentation (http://wwwtest.provo.novell.com/documentation/oes2/security.html#security).

- Section 22.2.1, "Comparing the Linux and the Novell Trustee File Security Models," on page 227
- Section 22.2.2, "User Restrictions: Some OES 2 Limitations," on page 229

22.2.1 Comparing the Linux and the Novell Trustee File Security Models

The Novell Trustee and Linux (POSIX) security models are quite different, as presented in Table 22-1.

Table 22-1 *POSIX vs. NSS/NCP File Security Models*

Feature	POSIX / Linux	Novell Trustee Model on OES 2
Administrative principles	Permissions are individually controlled and managed for each file and subdirectory. Because of the nature of the POSIX security model, users usually have read rights to most of the system. To make directories and files private, permissions must be removed. For more information on making existing directories private, see Section 18.4.2, "Providing a Private Work Directory," on page 200.	Trustee assignments are made to directories and files and flow down from directories to everything below unless specifically reassigned.

Feature	POSIX / Linux	Novell Trustee Model on OES 2
Default accessibility	Users have permissions to see most of the file system. The contents of a few directories, such as the `/root` home directory, can only be viewed by the `root` user. Some system configuration files can be read by everyone, but the most critical files, such as `/etc/fstab`, can only be read and modified by `root`.	Users can see only the directories and files for which they are trustees (or members of a group that is a trustee).
Home directories—an example of default accessibility	By default, all users can see the names of directories and files in home directories. During LUM installation, you can specify that newly created home directories will be private. For more information on making existing home directories private, see Section 18.4.2, "Providing a Private Work Directory," on page 200.	By default, only the system administrator and the home directory owner can see a home directory. Files in the directory are secure. If users want to share files with others, they can grant trustee assignments to the individual files, or they can create a shared subdirectory and assign trustees to it.
Inheritance from parents	Nothing is inherited. Granting permission to a directory or file affects only the directory or file.	Rights are inherited in all child subdirectories and files unless specifically reassigned. A trustee assignment can potentially give a user rights to a large number of subdirectories and files.
Privacy	Because users have permissions to see most of the file system for reasons stated above, most directories and files are only private when you make them private.	Directories and files are private by default.
Subdirectory and file visibility	Permissions granted to a file or directory apply to only the file or directory. Users can't see parent directories along the path up to the root unless permissions are granted (by setting the UID, GID, and mode bits) for each parent. After permissions are granted, users can see the entire contents (subdirectories and files) of each directory in the path.	When users are given a trustee assignment to a file or directory, they can automatically see each parent directory along the path up to the root. However, users can't see the contents of those directories, just the path to where they have rights.

When an NCP volume is created on a Linux POSIX or NSS volume, some of the behavior described above is modified. For more information, see the *OES 2 SP3: NCP Server for Linux Administration Guide*, particularly the "NCP on Linux Security" section.

22.2.2 User Restrictions: Some OES 2 Limitations

Seasoned NetWare administrators are accustomed to being able to set the following access restrictions on users:

- Account balance restrictions
- Address restrictions
- Intruder lockout
- Login restrictions
- Password restrictions
- Time restrictions

Many of the management interfaces that set these restrictions (iManager, for example), might seem to imply that these restrictions apply to users who are accessing an OES 2 server through any protocol.

This is generally true, with two important exceptions:

- Maximum number of concurrent connections in login restrictions
- Address restrictions

These two specific restrictions are enforced only for users who are accessing the server through NCP. Connections through other access protocols (for example, HTTP or CIFS) have no concurrent connection or address restrictions imposed.

For this reason, you probably want to consider not enabling services such as SSH and FTP for LUM when setting up Linux User Management. For more information on SSH and LUM, see Section 12.4, "SSH Services on OES 2," on page 95.

For more information on Linux User Management, see "Linux User Management: Access to Linux for eDirectory Users" on page 153. For more information on the services that can be PAM-enabled, see Table 16-2 on page 157.

22.3 Configuring and Administering Security

For a list of configuration and administration topics, see the Security section in the OES online documentation (http://wwwtest.provo.novell.com/documentation/oes2/security.html#security).

22.4 Resolving Nessus Security Scan Issues

22.4.1 Port dns (53/tcp): DNS Server Zone Tranfer Information Disclosure (AXFR)

Nessus Plug in: 10595

Port: DNS service on port 53

Synopsis: The remote name server permits zone transfers.

Description: A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a server's primary application, for example, proxy.example.com, payroll.example.com, b2b.example.com, etc.

Information like this is of great use to an attacker, who may use it to gain information about the topology of the network and spot new targets.

Resolution: Limit DNS zone transfers to only the servers that need the information. The Security Chapter for DNS includes the required information to restrict zones, allow-update and queries and the security factors. See "Security Considerations for DNS" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

22.4.2 Port dns (53/udp):DNS Server Recursive Query Cache Poisoning Weakness

Nessus Plug in: 10539

Port: DNS on port 53

Synopsis: The remote name server allows recursive queries to be performed by the host running nessusd.

Description: It is possible to query the remote name server for third party names.

If this is your internal name server, then the attack vector may be limited to employees or guest access if allowed. If you are probing a remote name server, then it allows anyone to use it to resolve third party names, such as www.novell.com.This allows attackers to perform cache poisoning attacks against this name server.

If the host allows these recursive queries via UDP, then the host can be used to "bounce" denial-of-service attacks against another network or system.

Resolution: Restrict recursive queries to the hosts that should use this name server, such as those of the LAN connected to it.

The Security Chapter for Novell DNS includes the required information to restrict zones, allow-update and queries and the security factors. See "Security Considerations for DNS" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

22.4.3 Port dns (53/udp): DNS Server Cache Snooping Remote Information Disclosure

Nessus Plug in: 12217

Port: DNS on port 53

Synopsis: The remote DNS server is vulnerable to cache snooping attacks.

Description: The remote DNS server responds to queries for third-party domains that do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

NOTE: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants, and potential users on a guest network or WiFi connection if supported.

Resolution: The Security Chapter for Novell DNS includes the required information to restrict zones, allow-update and queries and the security factors. See "Security Considerations for DNS" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

22.4.4 Port dns (53/udp): Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Nessus Plug in: 33447

Port: DNS on Port 53

Synopsis: The remote name resolver (or the server it uses upstream) may be vulnerable to DNS cache poisoning.

Description: The remote DNS resolver does not use random ports when making queries to third party DNS servers. This problem might be exploited by an attacker to poison the remote DNS server more easily, and therefore divert legitimate traffic to arbitrary sites.

Resolution: Nessus might report this if the OES server is configured to use a non-OES DNS server that has the above vulnerability. Configure DNS with Novell-DNS instead of the third-party server that is vulnerable.

22.4.5 Port ftp (21/tcp): Anonymous FTP Enabled

Nessus Plug in: 10079

Port: FTP service on port 21

Synopsis: Anonymous logins are allowed on the remote FTP server.

Description: This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Resolution: Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

22.4.6 Port ftp (21/tcp):Multiple Vendor Embedded FTP Service Any Username Authentication Bypass

Nessus Plug in: 10990

Port: FTP service on port 21

Synopsis: A random username and password can be used to authenticate to the remote FTP server.

Description: The FTP server running on the remote host can be accessed using a random username and password. Nessus has enabled some countermeasures to prevent other plug ins from reporting vulnerabilities incorrectly because of this.

Resolution: Contact the FTP server's documentation so that the service handles authentication requests properly.

22.4.7 Port ldap: LDAP NULL BASE Search Access

Nessus Plugin: 10722

Port: LDAP on 389, DSfW LDAPS on 1636, msft-gc on 3268

Synopsis: The remote LDAP server may disclose sensitive information.

Description: The remote LDAP server supports search requests with a null, or empty, base object. This allows information to be retrieved without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user may be able to query your LDAP server using a tool such as LdapMiner.

NOTE: There are valid reasons to allow queries with a null base. For example, it is required in version 3 of the LDAP protocol to provide access to the root DSA-Specific Entry (DSE), with information about the supported naming context, authentication types, and the like. It also means that legitimate users can find information in the directory without any a prior knowledge of its structure.

For these reasons, this finding may be a false-positive.

Resolution: If the remote LDAP server supports a version of the LDAP protocol before v3, consider whether to disable NULL BASE queries on your LDAP server LDAP NULL BASE search access might be required by many OES services.

For more details see, TID 7000737 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7000737).

22.4.8 Port smb (139/tcp) : Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials

Neesus Plug in : 56210

Synopsis: It is possible to obtain the host SID for the remote host, without credentials.

Description: By emulating the call to LsaQueryInformationPolicy(), it is possible to obtain the host SID (Security Identifier), without credentials. The host SID can then be used to get the list of local users.

Resolution: Novell-Cifs sends a dummy response with an SID value of 0. Therefore, this is not a security vulnerability.

22.4.9 Port ssh (22/tcp): SSH Protocol Version 1 Session Key Retrieval

Nessus Plug in: 10882

Port: SSH service on port 22

Synopsis: The remote service offers an insecure cryptographic protocol.

Description: The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe, so they should not be used.

Resolution: Disable compatibility with SSH 1.*x*.

22.4.10 Port (524/tcp): Novell NetWare ncp Service NDS Object Enumeration

Nessus Plug in: 10988

Port: NCP server on port 524

Synopsis: Remote directory server leaks information.

Description: This host is a Novell NetWare (eDirectory) server, and has browse rights on the PUBLIC object. It is possible to enumerate all NDS objects, including users, with crafted queries. An attacker can use this to gain information about this host.

Resolution: This feature is required by many OES services for their normal operation.

If this is an external system, block Internet access to port 524.

22.4.11 Port www (443/tcp): SSL Certificate signed with an unknown Certificate Authority

Nessus Plug in: 51192

Port: Apache (443), LDAPS (636), DSfW LDAPS (1636), msft-gc-ssl (3269), wbem (5989), NRM (8009), iMonitor (8030)

Synopsis: The SSL certificate for this service is signed by an unknown certificate authority.

Description: The X.509 certificate of the remote host is not signed by a known public certificate authority. If the remote host is a public host in production, this nullifies the use of SSL because anyone could establish a man-in-the-middle attack against the remote host.

Resolution: Purchase or generate a proper certificate for this service. For more information about generating certificates using the Novell Certificate Server, see "Using eDirectory Certificates with External Applications" in the *Novell Certificate Server 3.3.4 Administration Guide*.

22.4.12 Port www (443/tcp): SSL Version 2 (v2) Protocol Detection

Nessus Plug in: 20007

Port: Apache port www (443)

Synopsis: The remote service encrypts traffic using a protocol with known weaknesses.

Description: The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

Resolution: Consult the Apache documentation to disable SSL 2.0 and use SSL3.0 or TLS 1.0 instead.

22.4.13 Port www (tcp): SSL Weak Cipher Suites Supported

Nessus Plug in: 26928

Port: Apache (443), NRM (8009), LDAPS (636), DSfW LDAPS (1636), msft-gc-ssl (3269)

Synopsis: The remote service supports the use of weak SSL ciphers.

Description: The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

NOTE: This is considerably easier to exploit if the attacker is on the same physical network.

Resolution:

1. Change the weak SSLCipherSuite setting for Apache in the `/etc/apache2/vhosts.d/vhost-ssl.conf` file from:

   ```
   SSLCipherSuite
   ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
   ```

   to

   ```
   SSLCipherSuite
   ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:!MEDIUM:!LOW:+SSLv2:!EXP:!eNULL
   ```

2. Restart Apache by entering the following at the terminal prompt:

   rcapache2 restart

22.4.14 Port www (tcp): SSL Medium Strength Cipher Suites Supported

Nessus Plug in: 42873

Port: Apache (443), NRM (8009), LDAPS (636), DSfW LDAPS (1636), msft-gc-ssl (3269)

Synopsis: The remote service supports the use of medium strength SSL ciphers.

Description: The remote host supports the use of SSL ciphers that offer medium-strength encryption (key lengths at least 56 bits and less than 112 bits).

NOTE: This is considerably easier to exploit if the attacker is on the same physical network.

Resolution: Open the `/etc/opt/novell/httpstkd.conf` file in a text editor, then do the following:

1. Find the following section.

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;    Cipher strength determines the bit strength for the SSL key
;    that is required to access Novell Remote Manager(NRM).
;       The default will be all
;
;    If you modify the setting it will be necessary to restart NRM.
;
;       Options: all, low, medium, high
;
;       all - allows any negotiated encryption level.
;       low - allows less than 56-bit encryption
;       medium - allows 56-bit up to 112-bit encryption
;       high - allows 112-bit or greater encryption
;
;       Example:
;       cipher high
;
;
;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
cipher all
```

2. Change `cipher all` to `cipher high`.
3. Save the file.
4. Restart httpstkd by entering `rcnovell-httpstkd restart` at a terminal prompt.

22.4.15 Port/Service: smb (139/tcp)

Build: Oes2Sp3 server Jan'12 patch

Nessus Plug in: 56708

Plugin Name: SMB Signing Disabled

Synopsis: Signing is disabled on the remote SMB server.

Description: Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

Solution: Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called `server signing`.

See also, http://support.microsoft.com/kb/887429, http://technet.microsoft.com/en-us/library/cc786681%28WS.10%29.aspx, http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Risk Factor: Medium

CVSS Base Score: 5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Vulnerability Publication Date: 2012/01/17

Plugin Publication Date: 2012/01/19

Plugin Last Modification Date: 2012/01/19

Risk factor : Medium

CVE: CVE-1999-0532

Other references: OSVDB:492

Nessus ID: 10595

22.5 Links to Product Security Considerations

The following product documentation contains additional security information:

***Table 22-2** Security Consideration Links*

Product/Technology	Security Considerations Section Link
AppArmor	Novell AppArmor Administration Guide (http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html)
Archive and Version Services	"Security Considerations for Archive and Version Services" in the *OES 2 SP3: Novell Archive and Version Services 2.1 Administration Guide for Linux*
Domain Services for Windows	*OES 2 SP3: Novell Domain Services for Windows Security Guide*
Dynamic Storage Technology	"Security Considerations" in the *OES 2 SP3: Dynamic Storage Technology Administration Guide*
eDirectory	"Security Considerations" in the *Novell eDirectory 8.8 SP7 Administration Guide*
File Systems	*OES 2 SP3: File Systems Management Guide* (information throughout the guide)
Identity Manager 3.6	"Security Best Practices (http://www.novell.com/documentation/idm36/idm_security/data/front.html)" in the Identity Manager 3.6 Documentation (http://www.novell.com/documentation/caribou/index.html)
iPrint for OES 2	"Setting Up a Secure Printing Environment" in the *OES 2 SP3: iPrint for Linux Administration Guide*
Linux User Management	"Security Considerations" in the *OES 2 SP3: Novell Linux User Management Administration Guide*
Novell AFP	"Security Guidelines for AFP" in the *OES 2 SP3: Novell AFP For Linux Administration Guide*
Novell CIFS	"Security Guidelines for CIFS" in the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

Product/Technology	Security Considerations Section Link
Novell Client for Windows	"Managing File Security and Passwords" in the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*
Novell Client for Linux	"Managing File Security" in the *Novell Client 2.0 SP3 for Linux Administration Guide*
Novell Remote Manager for OES 2	"Security Considerations" in the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*
Novell Storage Services	"Securing Access to NSS Volumes, Directories, and Files" and "Security Considerations" in the *OES 2 SP3: NSS File System Administration Guide for Linux*
Novell iFolder 3.8	*Novell iFolder 3.8 Security Administration Guide*
OES 2 Installation	"Security Considerations" in the *OES 2 SP3: Installation Guide*
OES 2 Migration Tools	"Security Considerations for Data Migration" in the *OES 2 SP3: Migration Tool Administration Guide*
OpenWBEM	"Ensuring Secure Access" in the *OES 2 SP3: OpenWBEM Services Administration Guide*
QuickFinder	"Security Considerations for QuickFinder Server" in the *QuickFinder Server 5.0 Administration Guide*
SuSEfirewall2	"Masquerading and Firewalls" (http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_fire.html) in the *SLES 10 SP4 Installation and Administration* guide (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html)

22.6 Links to Anti-Virus Partners

See the Partners and Communities page on Novell.com (http://www.novell.com/products/openenterpriseserver/partners_communities.html).

23 Certificate Management

By default, all SUSE Linux Enterprise Server (SLES) 10 servers include self-generated server certificates to secure data communications with the servers. These certificates are self-signed and do not comply with the X.509 RFCs. They are provided only as a stop-gap and should be replaced as soon as possible by a certificate from a trusted Certificate Authority.

Unfortunately, many organizations ignore the vulnerabilities to mischievous or even malicious attacks that are created by not replacing these temporary certificates. Some of the reasons for this are

- Many administrators lack the knowledge required.
- Certificate maintenance can require a significant investment of time and effort.
- Obtaining third-party certificates for each server is expensive.

The problems are compounded by the fact that X.509 certificates are designed to expire regularly and should be replaced shortly before they do.

Open Enterprise Server 2 includes solutions that address each of these issues at no additional expense.

This section discusses the certificate management enhancements available in OES 2 and how simple and straightforward it is to take advantage of these.

- Section 23.1, "Overview," on page 239
- Section 23.2, "Setting Up Certificate Management," on page 242
- Section 23.3, "If You Don't Want to Use eDirectory Certificates," on page 244

23.1 Overview

The following sections outline how OES 2 lets you automate certificate management for OES 2 and all HTTPS services:

- Section 23.1.1, "SLES Default Certificates," on page 239
- Section 23.1.2, "OES 2 Certificate Management," on page 240
- Section 23.1.3, "Multiple Trees Sharing a Common Root," on page 241

23.1.1 SLES Default Certificates

By default, HTTPS services on SLES 10 are configured to use two files that are located in `/etc/ssl/servercerts` and are protected so that only `root` and some specific groups can read them:

- **serverkey.pem:** This contains the server's raw private key.
- **servercert.pem:** This contains the server's certificates.

OES 2 services, such as Apache, OpenWBEM, and Novell Remote Manager, are also configured to use these certificates.

23.1.2 OES 2 Certificate Management

OES 2 enhances certificate management as follows:

- "Installation of eDirectory Certificates" on page 240
- "What Is Installed Where" on page 240
- "Novell Certificate Server" on page 241
- "Server Self-Provisioning" on page 241
- "PKI Health Check" on page 241

Installation of eDirectory Certificates

As you install eDirectory and OES 2, by default all HTTPS services are configured to use eDirectory certificates. This means that eDirectory is established as the Certificate Authority for the tree you are installing into, and it will generate keys and certificates for the server and replace the installed SLES certificates with the eDirectory certificates.

What Is Installed Where

Key and certificate files are installed in the following locations:

Table 23-1 *File Locations*

Location	Details
`/etc/ssl/certs`	This is the default location of trusted root certificates for clients on the server. Most of the applications on the server are configured to use this directory. For example, the LDAP client uses one or more of the trusted certificates in this directory when establishing a secure LDAP connection. The OES 2 installation copies the eDirectory tree CA's certificate (`eDirCACert.pem`) here, thereby establishing the CA as a trusted root. Everyone (other) has rights to read the contents of this directory.
`/etc/ssl/servercerts`	The standard location for the server's raw private key (`serverkey.pem`) and certificates (`servercert.pem`). Applications on the server, including OES 2 applications, are configured to point to the files in this directory. Only `root` and some specific groups can read the files in this directory.

Location	Details
`/etc/opt/novell/certs`	This directory contains the eDirectory CA certificate in both DER and PEM formats for use by applications that need them. The files are named `SSCert.der` and `SSCert.pem`, respectively. For example, when PKI Health Check runs, it installs the CA certificate in the Java Keystore in DER format if the certificate needs replacing.

Novell Certificate Server

The component that generates eDirectory keys and certificates is the Novell Certificate Server.

This certificate server provides public key cryptography services that are natively integrated into Novell eDirectory. You use the server to can mint, issue, and manage both user and server certificates to protect confidential data transmissions over public communications channels such as the Internet.

For complete information on the Novell Certificate Server, see the *Novell Certificate Server 3.3.4 Administration Guide*.

Server Self-Provisioning

When activated, Server Self-Provisioning lets server objects in eDirectory create their own certificates. You must activate this option if you want PKI Health Check to automatically maintain your server certificates.

For more information on this feature, see "X.509 Certificate Self-Provisioning" in the *Novell Certificate Server 3.3.4 Administration Guide*.

PKI Health Check

The PKI health check runs whenever the certificate server starts.

If you have enabled Server Self-Provisioning, the health check routine automatically replaces server certificates when any of the following are detected:

- The certificates don't exist.
- The certificates have expired.
- The certificates are about to expire.
- The IP or DNS information on the certificates doesn't match the server configuration.
- The Certificate Authority (CA) that issued the certificate is different from the CA currently configured.

For more information on this feature, see "PKI Health Check" in the *Novell Certificate Server 3.3.4 Administration Guide*.

23.1.3 Multiple Trees Sharing a Common Root

The Organizational CA can be configured to act as a sub-CA. This lets multiple trees share a common root certificate. The root certificate can be stored in a physically protected tree. It can also integrate with a third-party PKI. For more information, see "Subordinate Certificate Authority" in the *Novell Certificate Server 3.3.4 Administration Guide*.

23.2 Setting Up Certificate Management

Use the information in the following sections to help you set up certificate management as you install OES 2.

- Section 23.2.1, "Setting Up Automatic Certificate Maintenance," on page 242
- Section 23.2.2, "Eliminating Browser Certificate Errors," on page 242

23.2.1 Setting Up Automatic Certificate Maintenance

To set up your server so that HTTPS services use eDirectory certificates, you must specify the *Use eDirectory Certificates for HTTP Services* option while installing or upgrading eDirectory.

This installs eDirectory keys and certificates on the server, but it does not configure the server to automatically replace the certificates when they expire. Automatic maintenance requires that Server Self-Provisioning be enabled as follows:

1. On the server you are configuring, in iManager > Roles and Tasks, click the *Novell Certificate Access > Configure Certificate Authority* option.
2. Click *Enable server self-provisioning*.

   This causes automatic certificate replacement for the conditions described in "PKI Health Check" on page 241.

   IMPORTANT: If you enable Server Self-Provisioning in an OES 2 tree and you have created a CRL configuration object but not yet configured any CRL distribution points, the PKI Health Check might replace the default certificates every time it runs.

   To avoid this, you can either

   - Finish configuring the CA's CRL capability by creating one or more CRL Distribution Points by using iManager's *Configure Certificate Authority* task.

     or

   - Delete any CRL Configuration objects, for example CN=One - Configuration.CN=CRL Container.CN=Security.
3. If you also want the CA certificate to be replaced if it changes or expires, click the *Health Check - Force default certificate creation/update on CA change* option.

23.2.2 Eliminating Browser Certificate Errors

Because the Internet Explorer and Mozilla Firefox browsers don't trust eDirectory certificate authorities by default, attempts to establish a secure connection with OES 2 servers often generate certificate errors or warnings.

These are eliminated by importing the eDirectory tree CA's self-signed certificate into the browsers.

Complete the instructions in the following sections as applicable to your network.

- "Exporting the CA's Self-Signed Certificate" on page 243
- "Importing the CA Certificate into Mozilla Firefox on Linux" on page 243
- "Importing the CA Certificate into Mozilla Firefox on Windows" on page 243
- "Importing the CA Certificate into Internet Explorer 6 and 7 on Windows" on page 243

Exporting the CA's Self-Signed Certificate

1. Launch Novell iManager.
2. Log into the eDirectory tree as the Admin user.
3. Select the *Roles and Tasks* menu, then click *Novell Certificate Server* > *Configure Certificate Authority*.
4. Click the *Certificates* tab, then select the self-signed certificate.
5. Click *Export*.
6. Deselect *Export Private Key*.

   The *Export Format* changes to DER.
7. Click *Next*.
8. Click *Save the Exported Certificate* and save the file to the local disk, noting the filename and location if they are indicated.
9. Click *Close* > *OK*.
10. Find the file you just saved. By default it is usually on the desktop.
11. Complete the instructions in the follow sections that apply to your browsers.

Importing the CA Certificate into Mozilla Firefox on Linux

1. Launch Firefox.
2. Click *Edit* > *Preferences* > *Advanced*.
3. Select the *Encryption* tab.
4. Click *View Certificates*.
5. Select the *Authorities* tab, then click *Import*.
6. Browse to the certificate file you downloaded in "Exporting the CA's Self-Signed Certificate" on page 243 and click *Open*.
7. Select *Trust this CA to identify Web sites*, then click *OK* > *OK* > *Close*.

   Firefox now trusts certificates from the servers in the tree.

Importing the CA Certificate into Mozilla Firefox on Windows

1. Launch Firefox.
2. Click *Tools* > *Options* > *Advanced*.
3. Select the *Security* tab.
4. Click *View Certificates*.
5. Select the *Authorities* tab, then click *Import*.
6. Browse to the certificate file you downloaded in "Exporting the CA's Self-Signed Certificate" on page 243 and click *Open*.
7. Select *Trust this CA to identify Web sites*, then click *OK* > *OK* > *OK*.

   Firefox now trusts certificates from the servers in the tree.

Importing the CA Certificate into Internet Explorer 6 and 7 on Windows

1. Launch Internet Explorer.
2. Click *Tools* > *Internet Options*.

3 Select the *Content* tab.

4 Click *Certificates*.

5 Click *Import*.

The Certificate Import Wizard launches.

6 Click *Next*.

7 Click *Browse*,

8 In the *Files of Type* drop-down list, select *All Files(*.*)*, browse to the file you downloaded in "Exporting the CA's Self-Signed Certificate" on page 243, then click *Open*.

9 Click *Next*.

10 Click *Next*.

Choose the default, *Automatically select the certificate store based on the type of certificate.*

11 Click *Finish* > *Yes* > *OK*.

Internet Explorer now trusts certificates from the servers in the tree.

23.3 If You Don't Want to Use eDirectory Certificates

For most organizations, the eDirectory certificate solution in OES 2 is an ideal way to eliminate the security vulnerabilities mentioned at the beginning of this chapter. However, some administrators, such as those who have third-party keys installed on their servers, probably want to keep their installed certificates in place.

You can prevent the use of eDirectory certificates for HTTPS services by making sure that the option to use them is not selected on the first eDirectory configuration page. This might or might not require that you change the eDirectory installation option, depending on your scenario.

Table 23-2 outlines the default setting for each scenario.

Table 23-2 *Default eDirectory Certificate for HTTPS Settings*

Scenario	Certificate Option Setting	Default Result	If you Change the Default Setting
New install	Selected	All HTTPS services on the server are configured to use eDirectory certificates.	All HTTPS services on the server are configured to use the YaST-generated temporary certificates.
Add-on to SLES 10 or post-install	Selected	All HTTPS services on the server are configured to use eDirectory certificates.	The current service certificates and configurations are retained.
Upgrade from OES 1	Selected	All HTTPS services are configured to use eDirectory certificates.	The current service certificates and configurations are retained.
Upgrade from OES 2 or OES 2 SP1	The same option is used as when OES 2 was installed	HTTPS service settings are retained.	No effect. Once the option to use eDirectory certificates has been used, the behavior can only be changed in eDirectory through iManager.

A Adding Services to OES 2 Servers

You can add services to Open Enterprise Server 2 servers after they are installed.

OES 2 is a set of services that can be either added to an existing server or installed at the same time as SUSE Linux Enterprise Server 10 SP1. After OES 2 services are added, we refer to the server as an OES 2 server.

To add OES 2 services to an OES 2 server, follow the instructions in “Installing or Configuring OES 2 SP3 on an Existing Server” in the *OES 2 SP3: Installation Guide*.

B Changing an OES 2 SP3 Server’s IP Address

The instructions in this section let you change the IP address assigned to an OES 2 SP3 server and the services it hosts.

B.1 Caveats and Disclaimers

The instructions in this section assume that only the IP address of the server is changing. They do not cover changing the DNS hostname of the server.

B.2 Prerequisites

B.2.1 General

Before starting the process, be sure you know the following:

❐ **Old IP Address:** The server’s IP address you are changing.

❐ **New IP Address:** The IP address the server will use after the change.

❐ **Old Master Server Address:** The IP address of the eDirectory™ server specified when the server was installed.

By default this is also the LDAP server address for OES services installed on the server.

❐ **New Master Server Address:** The IP address of the eDirectory server that the server should point to after the change. The old and new addresses might be the same, but you will be required to enter both.

❒ **Address of the Subnet for the New IP Address:** This is a subnet address, not the subnet mask. For example, 192.168.2.0, not 255.255.255.0.

B.2.2 iPrint

If your network users connect to their printers through the print manager on this server, you might want to consider setting up iPrint Client Management (ICM) prior to the change. ICM lets you centrally configure the iPrint configuration for your users. For more information, see "Using iPrint Client Management" in the *OES 2 SP3: iPrint for Linux Administration Guide*.

B.2.3 Clustering

If the server is running Novell Cluster Services:

1 Check your plans against the prerequisites for clusters in "IP Address Requirements" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

2 Follow the instructions in "Changing the IP Addresses of Cluster Resources" in the same guide.

B.3 Changing the Server's Address Configuration

1 Log into the server you are reconfiguring as the `root` user.

2 Download and save the `ipchangesp3.sh` script file (http://www.novell.com/documentation/oes2/scripts/ipchangesp3.sh) to the `root` (/) partition of the server you are reconfiguring.

3 Open the YaST Control Center.

4 In *Network Devices* select *Network Card*.

5 Confirm that the Old IP address you listed in Section B.2.1, "General," on page 247 is in fact the IP address currently configured for the network card. You need this later in the process.

6 Using the various dialog boxes associated with the network card configuration, change the card configuration to the new IP address settings you listed in Section B.2.1, "General," on page 247, changing each of the following as necessary:

- IP Address
- Subnet Mask
- Router (Gateway)

7 Close YaST, then continue with Section B.4, "Reconfiguring the OES Services," on page 248.

B.4 Reconfiguring the OES Services

1 Open a terminal prompt.

2 At the terminal prompt, change to the root (/) directory, make the script executable, then run the script by entering the following commands:

```
cd /
chmod 744 ipchangesp3.sh
./ipchangesp3.sh oldip newip oldmasterip newmasterip
```

where *oldip* is the old IP address, *newip* is the new IP address, *oldmasterip* is the IP address of the eDirectory server specified when the server was installed, and *newmasterip* is the IP address of the new eDirectory server identified in Prerequisites above.

The oldmasterip and the newmasterip can be the same IP address, but they must both be included in the command.

IMPORTANT: By default, the master eDirectory address is also the LDAP server address for OES services installed on the server.

All services that are configured with the old master address as their LDAP address are reconfigured to use the new master address. On the other hand, if you specified a different LDAP server address for any of the installed services, and if that LDAP server's address is also changing, you need to manually reconfigure the services.

To see the IP addresses that your services were originally configured to use, use a text editor to open the files in `/etc/sysconfig/novell/`.

As the script runs, it changes all of the OES configuration files and does everything else that can be done automatically to change the IP address for all OES services.

3 Type the Admin password when prompted.

   You might need to wait a few minutes for the LDAP server to restart.

4 When the script finishes, restart the server by entering the following command at the terminal prompt:

```
shutdown -r now
```

B.5 Repairing the eDirectory Certificates

1. Start iManager and click through the warnings about a DNS name mismatch.
2. In the Login dialog box, type the Admin username and password, type the newmasterip address in the *Tree* field, then click *Login*.
3. Click *Novell Certificate Server* > *Repair Default Certificates*.
4. In *Create Server Certificate* > *Step 1 of 3*, browse to and select the server object for the server you are changing.
5. Click *OK* > *Next*.
6. In *Step 2 of 3*, click *Next*.
7. Click *Finish*, then close the dialog box.

B.6 Completing the Server Reconfiguration

Some OES services require reconfiguration steps to be done manually.

Complete the steps in the following sections as they apply to the server you are changing.

- Section B.6.1, "QuickFinder," on page 250
- Section B.6.2, "DHCP," on page 250
- Section B.6.3, "DSfW," on page 250
- Section B.6.4, "iFolder," on page 252
- Section B.6.5, "iPrint," on page 253
- Section B.6.6, "NetStorage," on page 253

B.6.1 QuickFinder

1 If the IP address you have changed is listed as an alias for the virtual search server, modify the list by deleting the entry for the old address and adding an entry for the new one.

For instructions, see “Deleting a Virtual Search Server” and “Creating a Virtual Search Server” in the *OES 2 SP3: Novell QuickFinder Server 5.0 Administration Guide*.

2 Regenerate the QuickFinder™ index by completing the instructions in see “Creating Indexes” in the *OES 2 SP3: Novell QuickFinder Server 5.0 Administration Guide*.

B.6.2 DHCP

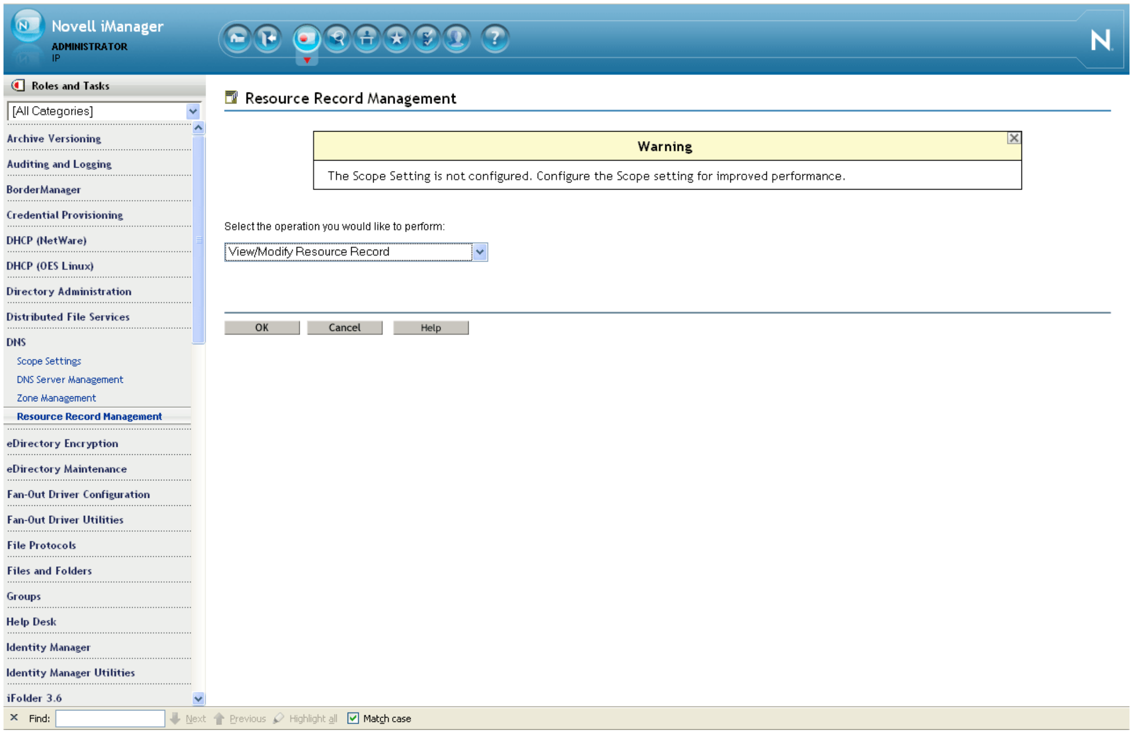
1 Make sure the DHCP configuration in eDirectory has a subnet declared for the new IP address.

For instructions, see “Administering and Managing DHCP” in the *OES 2 SP3: Novell DNS/ DHCP Administration Guide*.

B.6.3 DSfW

After the IP address is changed, execute the following instructions:

1 Open *iManager* > *DNS* > *Resource Record Management*. Select *View and Modify Resource Record* from the drop-down list, then click *OK* to open the Modify Resource Record window.



Resource Record Management

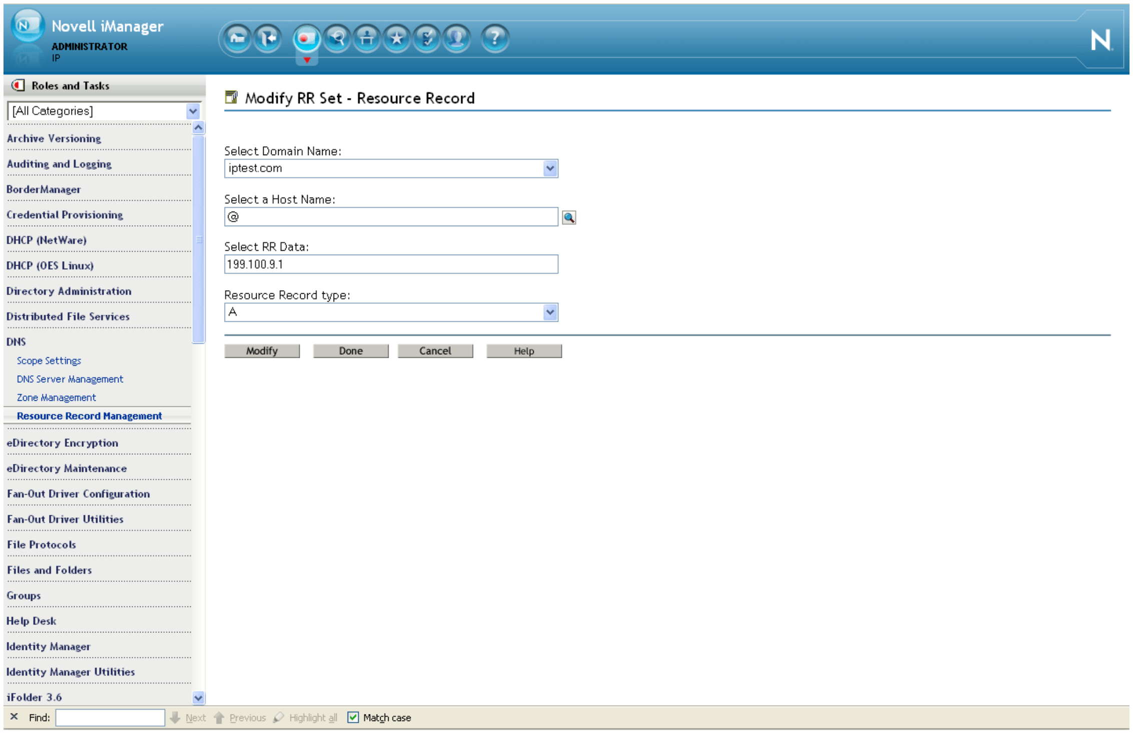
Warning

The Scope Setting is not configured. Configure the Scope setting for improved performance.

Select the operation you would like to perform:

View/Modify Resource Record

2 Select the domain name from the drop-down list, then click *Search*. This is the domain name whose IP address is to be changed (In this example, it is the ‘A’ record).



Modify RR Set - Resource Record

Select Domain Name: iptest.com

Select a Host Name: @

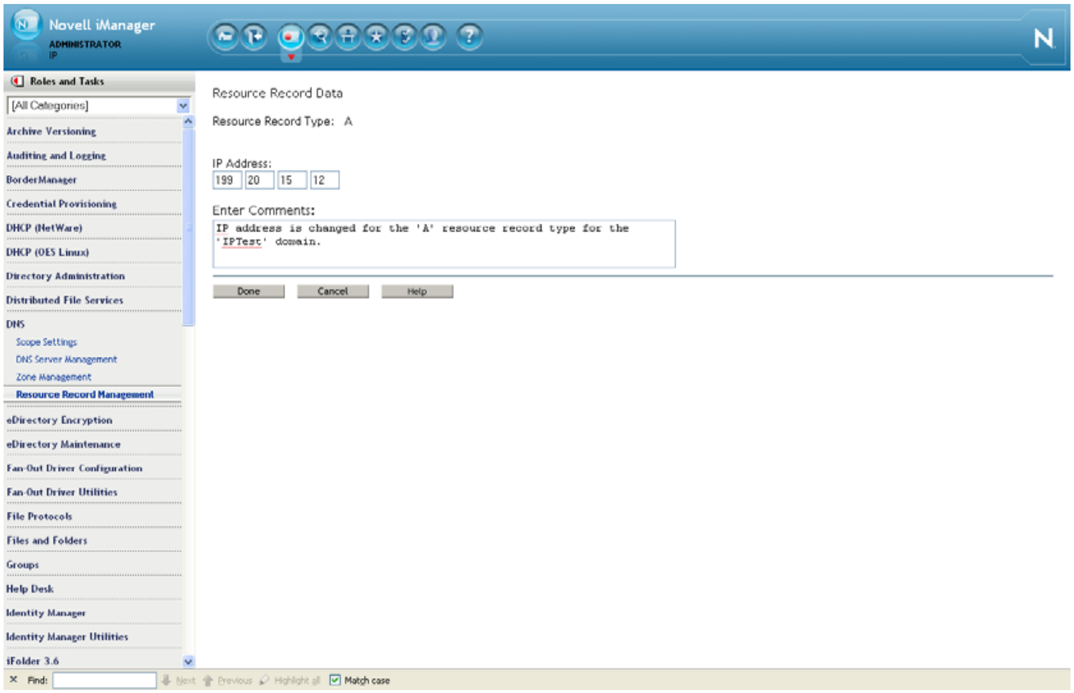
Select RR Data: 199.100.9.1

Resource Record type: A

2a Specify the *Host Name* using the search feature.

2b Select the '@ ' record and click *Modify* to change the IP address with the new IP address.

Select the hostname A record and click *Modify* to change the IP address with the new IP address.



Resource Record Data

Resource Record Type: A

IP Address:
199 20 15 12

Enter Comments:
IP address is changed for the 'A' resource record type for the 'IPTest' domain.

2c Click *Done*. A message indicates that the A record has been successfully modified.

3 Execute the following steps to rename and move the Reverse Lookup object:

3a Click *iManager* > *Directory Administration* >*Rename Object*. Search and select the Reverse Lookup object from eDirectory.

3b In the New Object Name field, specify the name of the Reverse Lookup object with the new IP address.

For example: If the object name is `135_103_92_100_in-addr_arpa.OESSystemObjects.nmfrd`, rename it with the new IP address. So if the new IP address is 100.92.103.136, the new name of the Reverse Lookup object will be `136_103_92_100_in-addr_arpa.OESSystemObjects.nmfrd`.

3c Click *iManager* > *Directory Administration* >*Modify Object*. Search and select the Reverse Lookup object from eDirectory.

3d From the *Other* tab, select the valued attribute named `dnip:zonedomainname` and change the value to new name of the Reverse Lookup object. Click *Save*.

4 Restart the DNS server.

5 Change the following:

5a Update the `/etc/resolve.conf` file if the server was acting as the DNS server for the domain.

NOTE: If you are performing the IP address change on the Forest Root Domain that is hosting the DNS server, make sure you update the `/etc/resolve.conf` file for all the servers referencing this domain controller.

B.6.4 iFolder

See "Managing Server IP Change " in the *Novell iFolder 3.8.4 Administration Guide*.

B.6.5 iPrint

1 Using your favorite text editor, open the following configuration file:

```
/etc/opt/novell/iprint/conf/DN_of_PSMipsmd.conf.
```

where *DN_of_PSM* is the name of the Print Manager in eDirectory.

2 Change any entries that list the old IP address to the new IP address.

3 Restart the Print Manager by entering the following command at a terminal prompt:

```
rcnovell-ipsmd restart
```

IMPORTANT: Users that have accessed printers through the modified Print Manager will lose access to their printers.

If you have set up iPrint Client Management on the server, you can automate the reconfiguration process. If not, users must reinstall the printers.

For more information on iPrint Client Management, see "Using iPrint Client Management" in the *OES 2 SP3: iPrint for Linux Administration Guide*.

B.6.6 NetStorage

1 At a terminal prompt, enter the following commands:

```
/opt/novell/xtier/bin/xsrvcfg -D
```

```
/opt/novell/xtier/bin/xsrvcfg -d newip -c AuthenticationContext
```

where *newip* is the new IP address used throughout this section and *AuthenticationContext* is the eDirectory context for NetStorage users. NetStorage searches the eDirectory tree down from this container. If you want NetStorage to search the entire eDirectory tree, specify the root context.

```
rcnovell-xregd restart
rcnovell-xsrvd restart
rcapache2 restart
```

B.7 Modifying a Cluster

If the server is running Novell Cluster Services™, complete the instructions in "Modifying the Cluster Configuration Information" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

B.8 Reconfiguring Services on Other Servers That Point to This Server

If you have services on other servers that point to the old IP address for this server, be sure to reconfigure those services to point to the new IP address.

C Updating/Patching OES 2 Servers

One of a network administrator's biggest challenges is keeping installed software up-to-date on all servers and workstations.

You can install product updates as they are made available through the ZENworks Linux Management update channel. For instructions on setting up the ZENworks Linux Management update channel for each OES 2 server and running the patch process, see "Updating (Patching) an OES 2 SP3 Server" in the *OES 2 SP3: Installation Guide*.

D Backup Services

The following sections briefly outline the backup services available in Open Enterprise Server 2. For more information, see the topics listed under "Backup (http://wwwtest.provo.novell.com/documentation/oes2/backup.html#backup)" in the OES 2 online documentation.

- Section D.1, "Services for End Users," on page 257
- Section D.2, "System-Wide Services," on page 257

D.1 Services for End Users

OES 2 offers a number of services to automatically back up your network users' data files.

- **Archive and Version Services:** If you implement Archive and Version Services on your network, your users can instantly restore any previous version of a modified, renamed, or deleted network file on an NSS volume without requiring assistance from the IT staff.
- **iFolder 3.8:** By implementing Novell iFolder 3.8, you empower your users to have their local files automatically follow them everywhere—online, offline, all the time—across computers. Users can share files in multiple iFolders, and share each iFolder with a different group of users. Users control who can participate in an iFolder and their access rights to the files in it. Users can also participate in iFolders that others share with them.
- **Salvage and Purge:** By default, all NSS volumes have the Salvage system enabled at the time they are created. With Salvage enabled, deleted files are retained on the volume for a short time, during which users can restore (salvage) them. File are eventually purged from the system, either manually, or by the system when the Purge Delay setting times out or space is needed on the volume.

D.2 System-Wide Services

OES 2 offers both Novell Storage Management Services and services that are available as part of the SUSE Linux Enterprise Server 10 distribution.

- Section D.2.1, "Links to Backup Partners," on page 257
- Section D.2.2, "Novell Storage Management Services (SMS)," on page 258
- Section D.2.3, "SLES 10 Backup Services," on page 258

D.2.1 Links to Backup Partners

See the Partners and Communities page on Novell.com (http://www.novell.com/products/openenterpriseserver/partners_communities.html).

D.2.2 Novell Storage Management Services (SMS)

- "Understanding SMS" on page 258
- "SMS Coexistence and Migration Issues" on page 258

Understanding SMS

Novell Storage Management Services (SMS) is not a backup application. Rather, it provides a standard framework and the necessary interfaces that can be used in developing a complete backup/restore solution. SMS helps back up file systems (such as NSS) on NetWare 6.5 SP8 and OES 2 servers to removable tape media or other media for offsite storage.

SMS is implemented as two independent components that provide functional abstractions:

- Storage Management Data Requestor (SMDR) defines the API framework, provides remote connectivity, and abstracts the details of communication between servers.
- Target Service Agent (TSA) provides an implementation of SMS APIs for a particular target. The TSA provides transparency by abstracting details of the specific service being backed up.

  For example, various applications use the file system TSA to back up and restore NSS file system data and metadata (trustee assignments, file attributes, and name spaces).

SMS Coexistence and Migration Issues

In OES 2, the SMS API framework is available on SLES 10 so that there is a single consistent interface to back up file systems on NetWare, file systems on Linux, and Novell applications such as GroupWise and Novell iFolder. The API set has been enhanced to include new functionality for OES.

Most of the SMS coexistence and migration issues are of concern only to backup application developers. However, administrators should be aware that SMS-based applications must be used to back up and restore NSS file system data on OES servers. Although NSS is exposed as a Virtual File System-compliant file system, the Linux interfaces are inadequate to back up NSS file system attributes, rich ACLs, trustees, and multiple data streams.

For additional information, see "Coexistence and Migration Issues" in the *OES 2 SP3: Storage Management Services Administration Guide for Linux*.

D.2.3 SLES 10 Backup Services

Two SLES 10 services might be of interest.

- **DRDB:** This lets you to create a mirror of two block devices at two different sites across an IP network. When used with HeartBeat 2 (HB2), DRBD supports distributed high-availability Linux clusters. For more information, see "Installing and Managing DRBD Services" (http://www.novell.com/documentation/sles10/stor_admin/data/drdb.html) in the *SLES 10 SP4: Storage Administration Guide* (http://www.novell.com/documentation/sles10/stor_admin/data/bookinfo.html).
- **rsync:** This is useful when large amounts of data need to be backed up regularly or moved to another server, such as from a staging server to a Web server in a DMZ. For more information, see "Introduction to rsync" (http://www.novell.com/documentation/sles10/book_sle_reference/data/sec_net_sync_rsync.html) in the *SLES 10 SP4: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html).

E Quick Reference to OES 2 User Services

Use Table E-1 as a quick reference for providing your network users with instructions for accessing each Novell Open Enterprise Server 2 service.

Table E-1 *OES User Services Quick Reference*

services	Access Method or URL	Notes
iPrint	http://*server_ip_address_or_dns_name/ipp* https://*server_ip_address_or_dns_name:443/ipp*	
NetStorage	For browser access, use: http: or https://*server_ip_or_dns*/netstorage For WebDAV access, use: http: or https://*server_ip_or_dns*/oneNet/NetStorage	The WebDAV URL is case sensitive.
Novell Client	1. Install the Novell Client on a supported Windows workstation. 2. Log in to eDirectory. 3. Access NCP volumes on NetWare or Linux that you have the appropriate file trustee rights to.	
Novell AFP	In the Chooser, click Go and browse to the server.	
Novell CIFS	Map a network drive in Windows Explorer. Create a Web Folder in Internet Explorer.	
Novell iFolder 3.x Web Access server	https://*server_ip_address_or_dns_name*/ifolder	"ifolder" is the default name, but this can be customized by the administrator.
Novell Remote Manager	http://*server_ip_address_or_dns_name*:8008	Any LUM-enabled user can see their directories and files on OES 2 servers.
Samba	Map a network drive in Windows Explorer. Create a Web Folder in Internet Explorer.	

F OES 2 SP3 Browser Support

As a general rule, Open Enterprise Server SP3 management tools support the following browsers as they are available on the workstation platforms listed in "Client/Workstation OS Support" on page 263:

- Mozilla Firefox3.6.2
- Microsoft Internet Explorer 8 (latest SP)
- Apple Safari 4.*x*

Table F-1 provides service-specific links and information about browser support in Novell® OES.

Table F-1 *Browser Support in OES*

Management Tool	Supported Browser Information Link
iManager 2.7	- "Using a Supported Web Browser" in the *Novell iManager 2.7.6 Administration Guide* There are rendering differences for some iManager plug-ins between Internet Explorer 6 (IE) and Mozilla-based browsers. For example, options that are accessed through tabs in IE are sometimes accessed through drop-down lists in Firefox. Also, iManager plug-ins might not work properly if the highest priority Language setting for your Web browser is set to a language other than one of iManager's support languages. To avoid problems, set the first language preference to a supported language.
iMonitor	- "System Requirements" in "Using Novell iMonitor" in the *Novell eDirectory 8.8 SP7 Administration Guide*
IP Address Manager (NetWare)	Same as Novell Remote Manager
iPrint	- "Supported Browsers for iPrint" in the *OES 2 SP3: iPrint for Linux Administration Guide*
Novell iFolder 3.8	- "Web Browser" in the *Novell iFolder 3.8.4 Administration Guide*
Novell Remote Manager	- "System Requirements" in the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide* - "System Requirements" in the *NW 6.5 SP8: Novell Remote Manager Administration Guide*
OpenSSH Manager (NetWare)	- "Added Functionality" in the *NW 6.5 SP8: OpenSSH Administration Guide*
QuickFinder Server Manager	- "Managing QuickFinder Server" in the *OES 2 SP3: Novell QuickFinder Server 5.0 Administration Guide*

Management Tool	Supported Browser Information Link
TCP/IP Configuration (NetWare)	Same as Novell Remote Manager

G Client/Workstation OS Support

As a general rule, Open Enterprise Server 2 services can be accessed and administered from workstations running the following operating systems:

- SUSE Linux Enterprise Desktop 10 SP3 (32- and 64-bit)
- SUSE Linux Enterprise Desktop 11.x (32- and 64-bit)
- OpenSUSE11.x 32- and 64-bit (iFolder and iPrint clients only)
- Microsoft Windows XP SP3 32-bit
- Microsoft Windows Vista Home Basic Sp1 (32- and 64-bit) (iPrint client only)
- Microsoft Windows Vista Business SP1
- Microsoft Windows Vista Business 64-bit SP1
- Microsoft Windows Vista Ultimate SP1
- Microsoft Windows Vista Ultimate 64-bit SP1
- Microsoft Windows Vista Enterprise SP1
- Microsoft Windows Vista Enterprise 64-bit SP1
- Microsoft Windows 7 Home Premium (32- and 64-bit) (iPrint client only)
- Microsoft Windows 7 Ultimate (32- and 64-bit)
- Microsoft Windows 7 Professional (32- and 64-bit)
- Macintosh OS X 10.5 (non-administrative only)
- Macintosh OS X 10.6 (non-administrative only)

For specific information on a given service, consult the service documentation.

H OES 2 Service Scripts

Novell Open Enterprise Server 2 services rely on specific service scripts located in /etc/init.d. The scripts used by OES 2, some of which are standard Linux scripts, are listed in Table H-1.

IMPORTANT: For managing OES 2 services, we strongly recommend using the browser-based tools outlined in Section 12.1, "Overview of Management Interfaces and Services," on page 85. The browser-based tools provide error checking not available at the service-script level, and they ensure that management steps happen in the sequence required to maintain service integrity.

Table H-1 *OES Service Scripts in /etc/init.d*

Services Associated with Scripts	Script Name	Notes
Apache Web server	`apache2`	The rcapache2 symbolic link, which is by default part of the path, can be used to start, stop, and restart the Apache Web Server, rather than referencing the init script directly.
Archive and Version Services	`novell-ark`	This lets you to start, stop, restart and display the status of the Archive and Version Service.
CASA	micasad	This is the CASA daemon.
Distributed File Services	`novell-dfs`	This lets you start and stop the VLDB service.
DNS (Novell eDirectory enhanced)	novell-named	This works in connection with `named` to provide Novell eDirectory DNS services.
DNS (SUSE Linux Enterprise Server 10 base)	named	This is the SLES 10 DNS service daemon.
Dynamic Storage Technology	novell-shadowfs	This script starts and stops the shadowfs daemon and the kernel module fuse.
eDirectory	`ndsd`	This lets you start and stop eDirectory. It executes the `/usr/sbin/ndsd` binary.
eDirectory SNMP support	`ndssnmpsa`	
eDirectory LDAP support	`nldap`	This lets you load and unload the LDAP library that Novell eDirectory uses to provide LDAP support. It is not actually a service.
FTP	pure-ftpd	This is used by the Novell FTP Pattern.

Services Associated with Scripts	Script Name	Notes

iPrint	`cups`
	`novell-idsd`
	`novell-ipsmd`	

iPrint	cups	iPrint uses this daemon.
Linux User Management	namcd nscd	These daemons are required by Linux User Management and work together to ensure good performance. The namcd daemon caches user and group names and IDs from eDirectory, speeding subsequent lookups of cached users and groups. The nscd daemon caches host names and addresses.
Logging	syslog	This is used for logging by many OES 2 services.
Novell AFP	novell-afptcpd	This script starts and stops the afptcpd daemon, which is the Novell AFP service daemon
Novell CIFS	novell-cifs	This script starts and stops the cifsd daemon, which is the Novell CIFS service daemon
NetStorage (actually XTier)	novell-xregd novell-xsrvd	NetStorage runs inside the novell-xsrvd XTier Web Services daemon, and also utilizes Tomcat services for certain other functions. novell-xregd is the init script for starting and stopping XTier's registry daemon. It is part of the `novell-xtier-base` RPM and is enabled by default for run levels 2, 3, and 5. novell-xsrvd is the init script for starting and stopping XTier's Web services daemon. It is also part of the `novell-xtier-web` RPM and is enabled for run levels 2, 3, and 5.
Novell Cluster Services (NCS)	novell-ncs	NCS uses some shell scripts and utilities that come with the heartbeat package. For example, NCS uses a binary called send_arp to send out ARP packets when a secondary address is bound. NCS never runs the heartbeat daemons. In fact, NCS and heartbeat are mutually exclusive when it comes to execution, and heartbeat must always be configured to not run (chkconfig heartbeat off) when NCS is loaded on the server.

Services Associated with Scripts	Script Name	Notes
Novell Remote Manager	novell-httpstkd	This script runs by default on every OES 2 server and enables access to NRM for Linux through a browser. Use this script followed by the status option to view current status. Or use stop, start, or restart options to alter the run state of the NRM daemon as needed.
Novell Storage Services	novell-nss	This script runs by default on every OES 2 server with NSS volumes and enables access to the NSS runtime environment. To see if the NSS kernel modules and NSS admin volume are running, enter `service novell-nss status`, `/etc/init.d/novell-nss status`, or `rcnovell-nss status` at a command prompt. If they are not running, use the `start` option to start them. You cannot stop NSS.
Novell Remote Manager e-mail notifications	postfix	Novell Remote Manager uses this to send notifications as configured.
NTP	ntp	This is the SLES 10 Network Time Protocol daemon.
OpenWBEM CIMOM	`owcimomd`	This is used to start the OpenWBEM CIMOM daemon, which is an integral part of the iManager plug-ins for LUM, Samba, NSS, SMS, and NCS. iPrint and NRM also use OpenWBEM. Novell Remote Manager on OES 2 gets its server health information from CIMOM.
Patching	novell-zmd	This is the GUI patch updater daemon.
Red Carpet	rcd	This is the rug command line daemon.
Samba	nmb	This is the Samba NetBIOS naming daemon.
Samba CIFS support	smb	This script runs the Samba daemon.
SLP support	slpd	This lets you start and stop OpenSLP, which is a key component for eDirectory and certain other services and clients.
Storage Management Services	novell-smdrd	This lets you start and stop the SMDR daemon precess. It also loads and unloads the NSS zapi kernel module used by SMS to back up the NSS volumes.
Tomcat	novell-tomcat5	This script sets up the SLES 10 Tomcat specifically for OES 2 services, such as the Welcome pages.

I System User and Group Management in OES 2 SP3

This section discusses the users and groups that are used by Open Enterprise Server. Administrative users are discussed in Appendix J, "Administrative Users in OES 2 SP3," on page 293.

I.1 About System Users and Groups

"Regular" network users rely on network services. System users and groups support those services.

Some NetWare administrators are concerned about the number of system users and groups on an OES server. They wonder what functions system users perform, why there are "so many" of them, and how they impact licensing and network security.

The answers to these and other questions are found in the sections that follow.

I.1.1 Types of OES System Users and Groups

The users and groups that support OES services can be grouped into the three types shown in Table I-1.

Table I-1 *Types of System Users and Groups with Examples*

System User or Group Type	Purpose	Examples
Proxy User	Perform very specific service-related functions, such as ◆ Retrieving passwords and service attributes ◆ Writing Service information in eDirectory. ◆ Providing a user ID (uid) that the associated service daemon uses to run.	◆ cifsProxyUser-*servername* ◆ *LUM_Proxy_user*
System Group	◆ Facilitate the management of system users ◆ Provide access rights to service data on the server or in the eDirectory tree.	◆ DHCP ◆ DNSDHCP
System User	The daemons associated with the respective services run as these users.	◆ wwwrun ◆ iprint

I.1.2 OES System Users and Groups by Name

Table I-2 lists the users and groups that OES services depend on and use.

Table I-2 *System User and Groups Listing*

System User or Group	Object Type	Associated Service
(Archive Versioning Proxy) The install admin is always assigned.	Proxy User	Archive and Versioning Services
arkuser	System User	Archive and Versioning Services
CifsProxyUser-*servername*	Proxy User	CIFS
DHCP LDAP Proxy	Proxy User	DHCP
dhcpd	System User	DHCP
DHCPGroup	System Group	DHCP
DNS Proxy	Proxy User	DNS
DNSDHCP-GROUP	System Group	DNS
hacluster	System User	Heartbeat
iFolderProxy	Proxy User	iFolder 3
iprint	System User	iPrint
Iprint (POSIX) iprintgrp (eDirectory)	System Group	iPrint

System User or Group	Object Type	Associated Service
LUM proxy (optional)	Proxy User	Linux User Management
named	System User	DNS
ncsclient	System User	NCS
ncsgroup	System Group	NCS
NetStorage Proxy	Proxy User	NetStorage
novell_nobody	System User	CIMOM
novell_nogroup	System Group	CIMOM
novlxregd	System User	XTier
novlxsrvd	System User	XTier
novlxtier	System Group	XTier
OESCommonProxy_*hostname*	System User	CIFS, DNS, DHCP, iFolder, NetStorage, Clustering (NCS), Linux User Management (optional)
server_name-SambaProxy	Proxy User	Samba (Novell)
server_name-W-SambaUserGroup	System Group	Samba (Novell)
*server_name*admin	Proxy User	NSS
www	System Group	Apache Tomcat QuickFinder
wwwrun	System User	Apache

I.2 Understanding Proxy Users

The subject of OES proxy users is somewhat complex. Therefore, it's a good idea to understand the basics before planning your implementation strategy.

IMPORTANT: The information in the following sections only answers security questions and provides general information. It is not intended to be used for the manual configuration of proxy users.

- Section I.2.1, "What Are Proxy Users?," on page 272
- Section I.2.2, "Why Are Proxy Users Needed on OES?," on page 272
- Section I.2.3, "Which Services Require Proxy Users and Why?," on page 272
- Section I.2.4, "What Rights Do Proxy Users Have?," on page 274

I.2.1 What Are Proxy Users?

As the name implies, proxy users are user objects that perform functions on behalf of OES services.

Proxy user accounts do not represent people, rather they are eDirectory objects that provide very specific and limited functionality to OES services. Generally, this includes only retrieving service-related information, such as user passwords and service attributes, but sometimes proxy users also write service information in eDirectory.

Many but not all OES services rely on proxy users to run on Linux (see "Which Services Require Proxy Users and Why?" on page 272). Proxy user creation and/or configuration is therefore an integral part of configuring OES.

None of the OES services require that you specify proxy user information during the OES installation, but some, such as DNS/DHCP, CIFS, and iFolder, give you the option to do so. Others, such as NCS and NSS create proxy users without user input, while Archive and Versioning Services always uses the install admin as its proxy user.

I.2.2 Why Are Proxy Users Needed on OES?

OES provides the Novell services that were previously only available on NetWare.

To make its services available on Linux, Novell had to accommodate a fundamental difference between the way services run on NetWare and the way they run on Linux.

- **NetWare Services:** The NetWare operating system and eDirectory are tightly integrated. This allows the services (NLMs) on NetWare to assume the identity of a server object in eDirectory, thus gaining access to the other objects and information in eDirectory that are needed for the services to run.
- **OES Services:** eDirectory also runs very well on OES, and it provides the infrastructure on which OES services rely, but it is not integrated with the Linux operating system.

  On Linux servers there is no concept of a service, such as Apache or iFolder running as a server object. Instead, each service runs using a User ID (uid) and a Group ID (gid) that the Linux server recognizes as being valid.

I.2.3 Which Services Require Proxy Users and Why?

The following services utilize a proxy user.

Table I-3 *Proxy Users Functions Listed by Service*

Associated Service	Example Proxy User Name	Services That the User Provides
AFP	n/a	Starting with SP3, AFP no longer requires a proxy user.
Archive Versioning	admin The install admin is always specified.	The service runs as this user.
CIFS	OESCommonProxy_*hostname* Or CifsProxyUser-*servername*	Retrieves CIFS user information.

Associated Service	Example Proxy User Name	Services That the User Provides
Clustering (NCS)	OESCommonProxy_*hostname* Or installing admin user	For SP3, NCS has separated out the proxy user (eDirectory communication) functionality so that the clustering administrator and the proxy user can be two separate users. For more information, see "OES Common Proxy User" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.
DHCP	OESCommonProxy_*hostname* Or DHCP_LDAP_Proxy	Lets the service access DHCP objects in eDirectory.
DNS	OESCommonProxy_*hostname* Or DNS_Proxy	Lets the service access DNS objects in eDirectory.
iFolder 3	OESCommonProxy_*hostname* Or iFolderProxy **IMPORTANT:** The Common Proxy user cannot be used if iFolder is running on a cluster node.	Connects to the eDirectory server and retrieves the following information: ◆ modifytimestamp ◆ cn ◆ mail ◆ sn ◆ GUID ◆ givenName ◆ member
Linux User Management	OESCommonProxy_*hostname* Or *LUM_proxy*	Searches the tree for LUM users.
NetStorage	OESCommonProxy_*hostname* Or *NetStorage_Proxy* The LDAP Admin user is specified by default, but another user can be created prior to installing and then specified.	Performs LDAP searches for users logging into NetStorage.
NSS	*server_name*admin	Reads user objects and maintains the volume, pool, and other storage system objects. This user performs some of the same functions as proxy users do for other services. However, unlike other OES services that can share proxy users, NSS requires a unique proxy user for each server.

Associated Service	Example Proxy User Name	Services That the User Provides
Samba (Novell)	*server_name*-SambaProxy	Searches the LDAP tree (eDirectory) for Samba users.

I.2.4 What Rights Do Proxy Users Have?

Each OES service's YaST installation automatically adds the required rights to the proxy user specified for the service.

Unless otherwise specified, each of the following users has the standard set of user rights in eDirectory:

- **Self:**

  Login Script:

  ```
  Read Write, Not inheritable
  ```

  Print Job Configuration:

  ```
  Read Write, Not inheritable
  ```

  [All Attribute Rights]:

  ```
  Read, Inheritable
  ```

- **[Public]**

  Message Server:

  ```
  Read, Not inheritable
  ```

- **[Root]**

  Group Membership

  ```
  Read, Not inheritable
  ```

  Network Address

  ```
  Read, Not inheritable
  ```

In addition, each proxy user is granted additional rights as summarized in Table I-4.

Table I-4 *Proxy Users Rights*

Associated Service	Example Proxy User Name	Default Rights Granted
AFP	n/a	Starting with SP3, AFP no longer requires a proxy user.
Archive Versioning	*Archive Versioning Proxy*	◆ This user has Read and Write rights to the archived volume.
CIFS	CifsProxyUser-*servername*	◆ This proxy user has the right to retrieve CIFS user information.

Associated Service	Example Proxy User Name	Default Rights Granted
Clustering (NCS)	OESCommonProxy_*hostname* Or installing admin user	◆ The proxy user has rights (granted through membership in the NCS_Management group) to communicate with eDirectory on behalf of the clustering service.
DHCP	DHCP_LDAP_Proxy	◆ No rights are assigned directly, but membership in the DHCPGroup, which does have assigned rights, provides the rights it needs.
DNS	DNS_Proxy	◆ No rights are assigned directly, but membership in the DNS-DHCPGroup, which does have assigned rights, provides the rights it needs.

iFolder 3	iFolderProxy	◆ Additional eDirectory rights include:
		[Entry Rights]
		`Browse`
		LDAP ACL representation:
		`1#subtree#iFolderProxy#`
		[All Attributes Rights]
		`Read, Compare`
		LDAP ACL representation:
		`3#subtree#iFolderProxy#`

Linux User Management	*LUM_proxy*	◆ If created, this proxy user has Search rights on Unix Config & Unix Workstation Objects.

NetStorage	NetStorage_Proxy	◆ Additional eDirectory rights:
		[Entry Rights]
		`Browse`
		LDAP ACL representation:
		`1#subtree#NetStorage_Proxy#`
		[All Attributes Rights]
		`Read, Compare`
		LDAP ACL representation:
		`3#subtree#NetStorage_Proxy#`

NSS	*server_name*admin	◆ Additional eDirectory rights: Supervisor right to the container it was created in.

Associated Service	Example Proxy User Name	Default Rights Granted
Samba (Novell)	*server_name*-SambaProxy	◆ The Universal Password policy associated with the Samba users grants this proxy user the right to retrieve user passwords. ◆ Additional eDirectory rights: Rights to itself – Supervisor attribute right Rights to the OU where it is located All Attribute rights – Read Write Entry rights – Browse Create samba* – Create Read Write

I.3 Common Proxy User - New in SP3

- Section I.3.1, "Common Proxy User FAQ," on page 276
- Section I.3.2, "Managing Common Proxy Users," on page 278

I.3.1 Common Proxy User FAQ

- "Why Would I Want to Specify Common Proxy Users?" on page 276
- "Why Has a Proxy User Been Added to Novell Cluster Services?" on page 277
- "Which Services Can and Cannot Leverage the Common Proxy User?" on page 277
- "Can a Common Proxy User Service Multiple Servers?" on page 278
- "Can I Change the Common Proxy User Name and Context?" on page 278
- "Can I Assign the Common Proxy User After Services Are Installed?" on page 278
- "What About Upgraded Servers Using a Common Proxy?" on page 278
- "Are There Important Limitations to Keep in Mind?" on page 278

Why Would I Want to Specify Common Proxy Users?

The implementation of a common proxy user in OES 2 SP3 addresses the following administrative needs:

- **Limit the Number of Proxy Users:** By default, the number of proxy users in an eDirectory tree can quickly become quite large. And even though proxy users don't consume user license connections, many administrators are disconcerted by the sheer number of objects to manage and track.

  Common proxy users reduce the default number of proxy users from one per service to basically one per OES 2 SP3 server.

- **Accommodate Password Security Policies:** Many organizations have security policies that require periodic password changes. Some administrators are overwhelmed by having to manually track all proxy users, change their passwords, and restart the affected services after every change.

  Common proxy users can have their passwords automatically generated and changed at whatever interval is required. Services are restarted as needed with no manual intervention required.

- **Prevent Password Expiration:** When proxy user passwords expire, OES 2 services are interrupted, leading to network user frustration and administrator headaches.

  Automatic password management for common proxy users ensures that services are never disrupted because of an expired password.

Why Has a Proxy User Been Added to Novell Cluster Services?

For SP3 the eDirectory communication functionality that was previously performed by the designated NCS administrator, has been separated out so that it can now be performed by a system user if so desired.

This aligns NCS functionality with other OES services that use proxy (system) users for similar functions. For more information, see "OES Common Proxy User" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

Which Services Can and Cannot Leverage the Common Proxy User?

- "Services That Can Leverage the Common Proxy User" on page 277
- "Services That Cannot Leverage the Common Proxy User" on page 277

Services That Can Leverage the Common Proxy User

The following OES services are automatically configured at install time by default to use your Common Proxy User (if specified):

- Novell CIFS
- Novell Cluster Services
- Novell DNS
- Novell DHCP
- Novell iFolder
- Novell NetStorage

The following OES service can be configured at install time to use your Common Proxy User (if specified):

- Linux User Management (having a proxy user is optional)

Services That Cannot Leverage the Common Proxy User

The following services that use proxy users do not leverage the Common Proxy user for the reasons listed:

Service	Reason
Archive and Version Services	This service uses the installing administrator as in the past.
Novell AFP	The need for an AFP proxy user has been eliminated in OES 2 SP3 due to a new NMAS method used for client authentication.
Novell Samba	Samba proxy password requirements are not a good fit with the Common Proxy user.
Novell Storage Services	This requires full rights to administer NSS and continues to require a system-named user with a system-generated password.

Can a Common Proxy User Service Multiple Servers?

No.

The common proxy user is designed and configured to be the common proxy for the OES services on a single server. Each subsequent new server needs a separate and distinct proxy created for its services.

Can I Change the Common Proxy User Name and Context?

Yes.

However, best practice suggests that eDirectory object names and locations within the tree reflect the object purpose and scope of influence or function. For this reason, the default Common Proxy User name is OESCommonProxy_*hostname*, where hostname is the name of the OES server being installed, and the default eDirectory context is the same as for the server for which the common proxy is created.

IMPORTANT: If you specify a different context from the server, the Organizational Unit that you specify must already exist in eDirectory. Otherwise, the server installation will fail, and you'll need to start over.

Can I Assign the Common Proxy User After Services Are Installed?

Yes. See "Assigning the Common Proxy to Existing Services" on page 279.

What About Upgraded Servers Using a Common Proxy?

You can change the services running on an OES 2 server that has been upgraded to OES 2 SP3 to leverage a Common Proxy user. See "Assigning the Common Proxy to Existing Services" on page 279.

Are There Important Limitations to Keep in Mind?

Yes.

iFolder must not be configured to use a Common Proxy on a cluster node.

I.3.2 Managing Common Proxy Users

Common proxy users are eDirectory objects and can therefore be managed via iManager. However, after the initial setup is complete, there should generally be no reason for OES administrators to directly manage Common Proxy users.

Use the information in the following sections to understand and implement common proxy user management.

- "Always Use LDAP Port 636 to Communicate with eDirectory" on page 279
- "Assigning the Common Proxy to Existing Services" on page 279
- "Changing Proxy Passwords Automatically" on page 279

Always Use LDAP Port 636 to Communicate with eDirectory

The Common Proxy user management scripts communicate with eDirectory using port 636 only. See the instructions in "Installing OES 2 SP3 as a New Installation" in the *OES 2 SP3: Installation Guide*).

Assigning the Common Proxy to Existing Services

You can assign the common proxy user to any of the services listed in "Services That Can Leverage the Common Proxy User" on page 277 using the `move_to_common_proxy.sh` script on your OES 2 SP3 server. In fact, if you have upgraded from SP2 and the server doesn't have a common proxy user associated with it, simply running the script will create and configure the proxy user and assign the services you specify.

1. In the `/opt/novell/proxymgmt/bin` folder, run the following command:

```
./move_to_common_proxy.sh service1,service2
```

where the service entries are OES service names.

Example scenario:

- You have upgraded server myserver, which is located in o=novell and uses IP address 10.10.10.1, from SP2 to SP3.
- The secure LDAP port for the server is 636.
- You are installing the server as the eDirectory Admin user, and your LDAP user FQDN is cn=admin,o=novell.
- Your Admin password is 123abc.
- You want to create a common proxy user and assign it as the common proxy for the Novell DNS and DHCP services running on the server.
- Therefore, you enter the following commands:

```
cd /opt/novell/proxymgmt/bin
```

```
./move_to_common_proxy.sh -d cn=admin,o=novell -w 123abc -i 10.10.10.1 -p 636 -
s novell-dhcp,novell-dns
```

User cn=OESCommonProxy_*myserver*.o=novell is created with a system-generated password and assigned the Common Proxy Policy password policy. The DNS and DHCP services are configured to be serviced by the Common Proxy user.

NOTE: Running the `move_to_common_proxy.sh` script automatically enables automatic changing of proxy user passwords. This feature is explained in the next section, Changing Proxy Passwords Automatically.

Changing Proxy Passwords Automatically

You can configure your server so that your proxy users are regularly assigned new system-generated passwords by doing the following:

1. Open the file `/etc/opt/novell/proxymgmt/proxy_users.conf` in a text editor.
2. List the FQDN of each proxy user on the server that you want to automatic password management set up for.

   For example you might insert the following entries:

   cn=OESCommonProxyUser_myserver,o=novell

cn=myproxy,o=novell

IMPORTANT: Users listed here must not be listed in the `proxy_users.conf` file on any other servers in the tree.

3. Save the file.
4. Enter the following commands:

```
cd /opt/novell/proxymgmt/bin
```

```
change_proxy_pwd.sh -A Yes
```

By default, the crontab job will run every 30 days.

I.4 Planning Your Proxy Users

Because of the prominent role played by the proxy users on your OES network, it is important that you understand your implementation options and the implications for each option. You can then plan an overall proxy user implementation strategy.

- Section I.4.1, "About Proxy User Creation," on page 280
- Section I.4.2, "There Are No Proxy User Impacts on User Connection Licenses," on page 284
- Section I.4.3, "Limiting the Number of Proxy Users in Your Tree," on page 284
- Section I.4.4, "Password Management and Proxy Users," on page 286

I.4.1 About Proxy User Creation

The first step in planning your proxy user implementation strategy is understanding the do's and don'ts of proxy user creation.

- "Creation Options" on page 280
- "Do Not Manually Configure Proxy Users" on page 283
- "Avoid Assigning an Admin User As a Proxy User" on page 284

Creation Options

Table I-2 presents information about the creation options for each OES proxy user.

Table I-5 *Proxy User Creation Options*

Associated Service	Service Proxy User Name if Applicable	Creation Information
AFP	n/a	Beginning with OES 2 SP3, the need for an AFP proxy user has been eliminated.
Archive Versioning	admin	The admin account that installs the server is automatically assigned as the Archive and Versioning proxy user. This is not configurable. Thefore, the new Common Proxy User feature doesn't apply.

Associated Service	Service Proxy User Name if Applicable	Creation Information
CIFS	OESCommonProxy_*hostname* Or CifsProxyUser-*servername*	◆ **Common Proxy User:** If a Common Proxy User is specified, CIFS will be automatically configured to use it by default, but you have the option to change this. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the CIFS YaST install automatically does the following: ◆ Creates a proxy user named cifsProxyUser-*servername* in the same context as the server. ◆ Generates a password, and stores it in either CASA or in an encrypted file on the server, depending on which option you select. Alternatively, you can modify any of the defaults, including the password. Or if you have already created a proxy user, you can specify that as well.
Clustering (NCS)	OESCommonProxy_*hostname* Or installing admin user	◆ **Common Proxy User:** If the Common Proxy User is specified, it is granted membership in the NCS_Management group, which enables it to communicate with eDirectory on behalf of the clustering service. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the system automatically uses the installing administrator, which is granted membership in the NCS_Management group, which enables it to communicate with eDirectory on behalf of the clustering service.
DHCP	OESCommonProxy_*hostname* Or installing administrator	◆ **Common Proxy User:** If a Common Proxy User is specified, DHCP will be automatically configured to use it by default, but you have the option to change this. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the admin account that installs the server is assigned as the DHCP proxy user. If you want to assign an alternate user account, it must already exist in the tree and be able to access the DHCP server object.
DNS	OESCommonProxy_*hostname* Or installing administrator	◆ **Common Proxy User:** If a Common Proxy User is specified, DNS will be automatically configured to use it by default, but you have the option to change this. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the admin account that installs the server is assigned as the DNS proxy user. If you want to assign an alternate user account, it must already exist in the tree and have Read, Write, and Browse rights in the contexts where the DNS Locator, Root Server, and Group Object are created.

Associated Service	**Service Proxy User Name if Applicable**	**Creation Information**
Domain Services for Windows (DSfW)	OESCommonProxy_*hostname* Or DNS	◆ **Common Proxy User:** If a Common Proxy User is specified, DSfW will be automatically configured to use it by default, but you have the option to change this. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the admin account that installs the server is assigned as the DNS proxy user. Alternatively, you can modify any of the defaults, including the password, or if you have already created a proxy user, you can specify that as well. The user must have the Read right to the LDAP service.
iFolder 3	OESCommonProxy_*hostname* Or iFolderProxy **IMPORTANT:** The Common Proxy user cannot be used if iFolder is running on a cluster node.	◆ **Common Proxy User:** If a Common Proxy User is specified, iFolder will be automatically configured to use it by default, but you have the option to change this. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the system automatically creates a proxy user named iFolderProxy. Alternatively, you can modify any of the defaults, including the password, or if you have already created a proxy user, you can specify that as well. The user must have the Read right to the LDAP service.
Linux User Management	OESCommonProxy_*hostname* Or *LUM_proxy* (optional)	By default, no LUM proxy user is created. ◆ **Common Proxy User:** If a Common Proxy User is specified, you have the option of specifying that it be used as the LUM proxy user. If you do this, LUM is automatically configured to use it. ◆ **No Common Proxy User:** If you create a proxy user for LUM, it will be assigned rights to search the LDAP tree for LUM objects. If you assign a previously created user as the LUM proxy user, it must have the Read right to the LDAP service.
NetStorage	OESCommonProxy_*hostname* Or Installing administrator	◆ **Common Proxy User:** If the Common Proxy User is specified, NetStorage will be configured to use it by default, but you have the option to change this. You must manually configure the proxy user with the rights specified in NetStorage in Table I-4 on page 274. For more information, see “Changing the NetStorage Default Configuration ” in the *OES 2 SP3: NetStorage Administration Guide*. ◆ **No Common Proxy User:** If a Common Proxy User is not specified, the system automatically uses the installing administrator. Alternatively, you can modify any of the defaults, including the password, or if you have already created a different proxy user, you can specify that as well. The user must have the Read right to the LDAP service.

Associated Service	Service Proxy User Name if Applicable	Creation Information
NSS	*server_name*admin	This admin account must have full rights to administer NSS and must be unique to each server. The Common Proxy User does not apply to NSS.
Samba (Novell)	*server_name*-SambaProxy	By default, the Samba proxy user is created in the container specified as the Base Context for Samba Users and is named *servername*-sambaProxyUser. A password is automatically generated for the default proxy user, or you specify a different 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. Because of the Samba proxy password requirements, the Common Proxy User cannot be used with Novell Samba.

Do Not Manually Configure Proxy Users

Best practices for most OES installation scenarios dictate that either the Common Proxy user be used or that proxy users be created in eDirectory prior to installing OES. For more information, see "Common Proxy User - New in SP3" on page 276 and "Limiting the Number of Proxy Users in Your Tree" on page 284.

IMPORTANT: The information in the preceding and following sections only answers security questions and provides general information. It is not intended to be used for the manual configuration of proxy users.

Manually created proxy users must be configured for OES-rootservice use only by the YaST based install, not manually.

Avoid Assigning an Admin User As a Proxy User

We recommend that you always use the special-purpose proxy user accounts described in this and the accompanying sections rather than specifying admin users as proxy users. Best practice dictates that proxy users have strictly limited functionality that supports only their specific system-level responsibilities. Proxy users should not be used for any other purposes.

Although specifying an admin user as the proxy user appears to be an easy way of setting up OES services (and is the install default in some cases if the Common Proxy user option isn't selected), there are potential problems. Mixing actual users with system-level functionality always creates some risk.

The following is a real-life example of risks that can occur when admin users are assigned as proxy users:

Novell Support received a call from an administrator who was getting locked out due to intruder detection after changing the administrator password. The lockout happened several times each day and seemed to be coming from the OES 2 servers. The support technician checked LUM and all of the services he could think of, and didn't see the admin credentials anywhere.

Further investigation revealed that the administrator credentials had been used to install OES 2 on multiple servers, and the credentials were also used as the proxy user credentials for some of the OES services. Consequently, the credentials were stored in CASA for use when the OES services came up.

Because the Admin password had changed, the CASA credentials had expired and service authentication requests were failing, resulting in the intruder detection lockout.

I.4.2 There Are No Proxy User Impacts on User Connection Licenses

Novell policy dictates that proxy users that function only as proxy users, are simply system users. Therefore, proxy users do not consume user connection licenses.

I.4.3 Limiting the Number of Proxy Users in Your Tree

Table I-6 outlines various options for limiting the number of proxy users in your tree and summarizes the security and manageability considerations of each approach.

Table I-6 *Options for Limiting the Number of Proxy Users*

Approach	Security Considerations	Manageability Considerations
Per Service per Server (default)	For CIFS, iFolder 3, and Samba this is the most secure option. By default, the passwords for these are system-generated and not known by anyone. For LUM there is no option to have a system-generated password. For DNS, DHCP, and NetStorage, the install admin's credentials are used by default. This has separate security implications as outlined in "Avoid Assigning an Admin User As a Proxy User" on page 284.	This approach requires no proxy user planning. Services are installed at the same time as the OES server. This is a good option for small organizations or installations where only a few services are used. This is not a good option if security policies dictate that all passwords must be reset periodically.
Per Server	This confines any security vulnerabilities to individual servers and is the scenario for which the Common Proxy User was developed.	This requires that a proxy user for the server is created before the server is installed. If the Common Proxy User is not leveraged, then for the first server in the tree, eDirectory and iManager must be installed with the server. After the server installation finishes, a proxy user can be created. And finally the services can be installed and configured to use the proxy user for the server. This approach is useful when each OES server is managed by a separate administrator, or for enterprises where branch users access a server in the branch office. Knowing the proxy user password is not required unless additional services will be installed or password policies require periodic changing, in which cases the install admin must know the proxy user's password.
Per Partition	This confines any security vulnerabilities to individual partitions.	This is useful when users are co-located with the OES servers in a single partition, and cross-partition access of users to services is rare. This is a good approach for organizations where eDirectory administration is done at a partition level. This requires that a proxy user for the first server in the partition is created before services are installed in the partition. The install admin must know the proxy user's password.

Approach	Security Considerations	Manageability Considerations
Per Service	This confines any security vulnerabilities to individual services. It also ensures that proxy user rights are not overloaded but are distributed so that there is a single proxy user for each type of service	For example, you might have one proxy user for CIFS, one for DNS/DHCP, one for iFolder, one for iPrint etc. This is useful in trees where the users and servers are not co-located, and different services are administered by different administrators. This requires that a proxy user for the service is created before the service is installed in the tree. The install admin must know the proxy user's password.
Per Tree	This exposes all OES services and servers in the tree to any security vulnerabilities.	A proxy user for the tree must be created before any OES services are installed in the tree. This is suitable for organizations that have ◆ Centralized eDirectory administration ◆ Users that are not confined to the partition or subtree where the OES servers reside, but instead access different OES servers from all over the tree. The install admin must know the proxy user's password.

I.4.4 Password Management and Proxy Users

Proxy user passwords must be stored on the individual OES servers where the services are installed because proxy users must be able to log in to eDirectory to perform their required functions.

- "Auto-Generated vs. Manually Specified Passwords" on page 286
- "Passwords Are Stored on the Server" on page 286
- "Avoid Password Expiration Problems" on page 287
- "Changing Proxy Passwords Automatically" on page 288

Auto-Generated vs. Manually Specified Passwords

- **Auto-Generated Passwords:** These offer the highest security because the passwords are known only to the system.

  The Common Proxy User, CIFS Proxy User, iFolder Proxy User (YaST calls this the *LDAP proxy user*), and Samba Proxy User all use auto-generated passwords by default.
- **Manually Specified Passwords:** Although you can change the auto-generated passwords for the various proxy users, this is not recommended because it is less secure and requires that someone keep track of the passwords. Also, manually specified passwords can easily lead to problems, such as service disruption. For a related example of the problems this can cause, see "Avoid Assigning an Admin User As a Proxy User" on page 284.

Passwords Are Stored on the Server

Of course all proxy user passwords are stored in eDirectory. Table I-7 explains where they are stored on the server and how they can be reset if needed.

Table I-7 Password Storage Locations

Associated Service	Where the Password Is Stored Locally	How the Password Can Be Reset
Archive and Versioning	The service-specific password is stored in CASA.	You must use the script provided by Archive and Versioning Services to change the password on the server.
CIFS	If the service-specific proxy user is used, the password is stored in either CASA or in an encrypted file, depending on the configuration option specified during service installation.	You can use iManager to reset the password in CASA or in the encrypted file, or the CASAcli tool if it is stored in CASA.
Common Proxy User	This password is stored in CASA.	We recommend that you only use the change_proxy_pwd.sh script to manage Common Proxy User passwords.
DHCP	If the service-specific proxy user is used, the service-specific password is stored in CASA if it is available. If CASA is not available, it is stored in the `/etc/dhcpd.conf` file.	If the password is stored in CASA, you can set it using the CASAcli tool. If not, edit the `/etc/dhcpd.conf` file.
DNS	If the service-specific proxy user is used, the service-specific password is stored in CASA if it is available. If CASA is not available, it is stored in an encrypted file.	
iFolder 3	If the service-specific proxy user is used, the service-specific password is stored in the iFolder store with PKI cryptography.	It can be changed either from a terminal prompt using the iFolder command line utilities or through the iFolder Admin Console.
Linux User Management	If the service-specific proxy user is used, the service-specific is stored in CASA.	This can be changed in iManager through the Linux User Management plug-in.
NetStorage	If the service-specific proxy user is used, the service-specific password is stored in the XTier registry.	This can be changed in iManager through the NetStorage plug-in.
NSS		This password is system-generated at install time and cannot be reset.
Samba (Novell)	The service-specific password is stored in Samba.	You can change the password by using the `smbpasswd` command.

IMPORTANT: Although the YaST based install can sometimes be used successfully to reconfigure some OES services, Novell neither recommends nor supports that practice.

Avoid Password Expiration Problems

Many organizations require that all network users have password policies to enforce regular password expiration and change.

Such policies create complications for the proxy user design. Proxy user passwords are stored on the local system to enable the OES services to log in to eDirectory. Every time a password change is forced in eDirectory, services stop working until the password is sychronized on the server.

These problems can be avoided by:

- Not assigning proxy users a password policy that enforces password expiration.
- Not using real user credentials for proxy users. See "Avoid Assigning an Admin User As a Proxy User" on page 284.

If password expiration policies cannot be avoided, or a security policy dictates that proxy user passwords must be changed periodically, we strongly urge you to implement an automatic password change routine as explained in"Changing Proxy Passwords Automatically" on page 288.

Otherwise you should probably do the following.

- Ensure that the responsible administrator knows or has a record of each proxy user's password and is aware of when each password expires.
- Before passwords expire, change them in eDirectory and reset them on the server. See the information in Table I-7.

Changing Proxy Passwords Automatically

You can configure your server so that your proxy users are regularly assigned new system-generated passwords by doing the following:

1. Open the file `/etc/opt/novell/proxymgmt/proxy_users.conf` in a text editor.
2. List the FQDN of each proxy user on the server that you want to automatic password management set up for.

   For example you might insert the following entries:

   cn=OESCommonProxyUser_myserver.o=novell
   cn=myproxy.o=novell

   IMPORTANT: Users listed here must not be listed in the `proxy_users.conf` file on any other servers in the tree.
3. Save the file.
4. Enter the following commands:

   ```
   cd /opt/novell/proxymgmt/bin
   ```

   ```
   change_proxy_pwd.sh -A Yes
   ```

   By default, the crontab job will run on the fifteenth (15th) day of each month.

I.5 Implementing Your Proxy User Plan

The proxy users in OES can be configured at different levels within eDirectory, depending on your needs.

IMPORTANT: If you plan to use the Common Proxy User, you can ignore this note.

The brief instructions that follow assume that you are installing into an existing tree and not leverageing the Common Proxy User.

For new trees, you will need to install and configure eDirectory on the first server without configuring any other OES services.

After the server is installed and you have created the required proxy users and passwords, then you can install the OES services and configure them to use the proxy users you have created.

The exception to this is installing all services without changing the default configuration settings (see Table I-5 on page 280). In most cases a default configuration assigns the install admin as the proxy user for the service.

I.5.1 Tree-Wide Proxy Users

Do the following:

1. Create a proxy user in the eDirectory tree where the OES servers will be installed, and set the password.

   Consider naming the user to reflect its purpose. For example, name the proxy user oes_service_proxy_user.
2. Use this proxy user and password while configuring the services on all of the OES servers in that tree.

I.5.2 Service-Specific Proxy Users

Do the following:

1. Create a proxy user in the eDirectory tree for each type of OES service and set the passwords.

   Consider naming the user to reflect its purpose. For example, name the CIFS proxy user, cifs_proxy_user.
2. Use these proxy users and passwords appropriately for each of the OES services on all OES servers.

I.5.3 Partition-Wide Proxy Users

Do the following:

1. Create one proxy user object per eDirectory partition in the OES tree, and set the password.

   Consider naming the user to reflect its purpose. For example, name the proxy user for the London regional office, london_office_proxy_user.
2. Use this proxy user and password for configuring all of the OES services on all the OES servers in that partition.

I.5.4 Server-Wide Proxy User

NOTE: The Common Proxy User is specifically designed as the default for this scenario.

Do the following:

1. Create one proxy user object per OES server (preferably in the same container as the server) and set the password.
2. Use this proxy user and password as the proxy user for all the services on that particular OES server.

I.5.5 Individual Proxy User Per-Server-Per-Service

This is the installation default if the Common Proxy User is not utilized as explained in Table I-6, "Options for Limiting the Number of Proxy Users," on page 285.

I.6 Proxy Users and Domain Services for Windows

Proxy users are not used in DSfW.

The Services part of the Trusted Computed Base has the rights to read users' supplemental credentials for authentication. A separate Kerberos process reads user passwords and performs the authentication. Another event handler in eDirectory creates the supplemental credentials for the user whenever the password is changed for that user.

However, the DNS Proxy User is closely associated with DSfW and can leverage the Common Proxy User available in SP3.

I.7 System Users

SLES and OES create system users on the local Linux system to provide user IDs (uids) to service processes. These users have rights to local files, such as configuration files.

The services that rely on system users do not have passwords because they don't need to log in. They simply use their associated user IDs.

When NSS is installed, some of these users are moved to eDirectory and LUM enabled. This is done to provide access to NSS data, to keep the user IDs the same across multiple servers, and to facilitate clustering and shared volumes.

Table I-2 lists the various system users that are used by OES services.

Table I-8 *System User Purposes*

System User or Group Name	Associated Service	Purpose
arkuser	Archive and Versioning Services	The service uses PostgreSQL as its metadata store, and PostgreSQL must run as a low-privileged user. `arkuser` is that low-privileged user.
dhcpd	DHCP	DHCP accesses local resources through this or an alternatively specified user. If the DHCP lease and configuration files are stored on NSS, the user must be moved to eDirectory and LUM enabled. `dhcpd` is used by default, but any local user can be used.
hacluster	Heartbeat	This user is created by Heartbeat, but it not used by Heartbeat nor by Novell Cluster Services.
iprint	iPrint	The iPrint daemons run as this user. If iPrint is moved to NSS, this user is created in eDirectory and the local user is removed.

System User or Group Name	Associated Service	Purpose
named	DNS	This system user lets DNS access local resources. In case of clusters, DNS data is on NSS volume, and so the user has to be created in eDirectory as well. `named` is used by default, but any local user can be used.
ncsclient	NCS	Used by NCS to access the adminfs file system.
novell_nobody	CIMOM	This user is created by CIMOM but is not currently used.
novlxregd	XTier	The XTier Registry Daemon (novell-xregd) runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.
novlxsrvd	XTier	The XTier Server Daemon (novell-xsrvd) runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.
wwwrun	Apache	The Apache daemon runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.

I.8 System Groups

These are groups in the local Linux system that provide a group ID (gid) to an OES process.

When NSS is installed, some of these groups are moved to eDirectory and LUM enabled. This is done to provide access to NSS data and to keep group IDs the same across multiple servers.

Table I-2 lists the system groups that are used by OES services.

Table I-9 *System Group Purposes*

System User or Group Name	Associated Service	Purpose
Iprint (POSIX) iprintgrp (eDirectory)	iPrint	The iPrint daemons use the group ID (gid) of this group to run. If iPrint is moved to NSS, the iprintgrp group is created in eDirectory.
ncsgroup	NCS	`ncsclient` is a member of this group.
novell_nogroup	CIMOM	This group is created by CIMOM but is not currently used.

System User or Group Name	Associated Service	Purpose
novlxtier	XTier	The XTier daemons use the group id (gid) of this group to run. Apache (wwwrun) is a group member because it needs XTier socket access. When NSS is installed on the Linux server, this group is removed from the local system and created in eDirectory. This is required because members of this group must have access to NSS data, and all NSS access is controlled through eDirectory.
server_name-W-SambaUserGroup	Samba (Novell)	All users granted Samba access are originally assigned to this group, which disables SSH access for them on the server. For more information, see "The Samba connection:" on page 97.
shadow	QuickFinder	Used by QuickFinder and other Web services.
www	Apache Tomcat QuickFinder	Apache (wwwrun) and tomcat (novlwww) use the group ID (gid) of this group to run. QuickFinder requires that all users who manage the service (including the eDirectory Admin user) belong to this group. User `novlxsrvd` is in the group because it needs access to an Apache domain socket. When NSS is installed on the Linux server, this group is removed from the local system and created in eDirectory. This is required because members of this group must have access to NSS data, and all NSS access is controlled through eDirectory.

I.9 Auditing System Users

It is the nature of the Linux operating system and the POSIX security model that the `root` user has access to all system information stored on the local server. Due to this fact, some organizations choose to monitor the activities of privileged users.

If you are interested in monitoring such activities, two Novell products can assist you.

- **Novell Sentinel:** Universal Password events can be monitored using Novell Sentinel. You enable this by modifying the NMAS Login Policy Object. For instructions, see Auditing NMAS Events (http://www.novell.com/documentation/nmas33/admin/data/bwmt40o.html). Then refer to the Novell Sentinel Documentation (http://www.novell.com/documentation/sentinel6/) for further instructions.
- **Privileged User Manager:** This product lets you monitor root user activities on the OES server by collecting data, analyzing keystrokes, and creating indelible audit trails. For more information, see the Novell Privileged User Manager Documentation (http://www.novell.com/documentation/privilegedusermanager22/index.html).

J Administrative Users in OES 2 SP3

Every OES network requires at least one administrative-level user to manage regular network users and system users.

Table J-1 *Administrative Users and Groups*

Administrative User or Group	Associated Service	Object Type	Purpose
Admin	eDirectory	Admin User	The eDirectory administrator that has all rights to manage the Tree. The default is Admin.
Container Admin	eDirectory	Admin User	These administrators are usually responsible for administering within a partition or subtree. They might be assigned only enough rights to install servers, or they might be assigned to specific roles in iManager.
admingroup	eDirectory	Admin Group	Provides LUM-enabling for the eDirectory administrator.
iFolderAdmin	iFolder 3	Service Admin	This is the default iFolder service administrator account. By default, the Tree Admin is specified.
QuickFinderAdmin	QuickFinder	Service Admin	This is the QuickFinder administrator. The default is the Tree Admin.

K Coordinating Password Policies Among Multiple File Services

K.1 Overview

OES 2 SP3 includes native file services for Windows and Macintosh workstations:

Macintosh Workstations	Windows Workstations
◆ Novell AFP	◆ Novell CIFS ◆ Novell Samba ◆ Domain Services for Windows (DSfW) DSfW is not classified as a file service, but it includes a customized version of Samba that is different from Novell Samba.

Each of these services requires that users who access them have Password policies that meet specific requirements. Users can be governed by only one Password policy at a time, so if any of your network users require access to more than one of the file services, you need to coordinate the Password policies that govern the users to ensure that they can access the different file services.

K.2 Concepts and Prerequisites

Prerequisites for AFP, CIFS, and Samba access are explained in the following sections:

K.2.1 Prerequisites for File Service Access

The following are the prerequisites for user access to AFP, CIFS, and Samba services:

- The eDirectory context under which users are searched for must be configured during service configuration.
- The users need to be governed by Password policies that enable Universal Password for them.
- There must be at least one writable replica of NMAS version 3.2 or later having the user object trying to access the AFP or CIFS server. NMAS 3.2 is already present on OES 2 servers, as well as on servers with eDirectory 8.8.2 installed. On OES 1 and NetWare servers with a lone writable replica of a AFP or CIFS user, NMAS should be upgraded by upgrading to the Novell Security Services 2.0.6 on eDirectory 8.7.3 SP10 or eDirectory 8.8.2.
- The file access services will provide access/visibility to the users as per the trustee rights they have on the volumes and files.

In addition, Samba (on both DSFW and non-DSFW servers) has the following additional requirements:

- The users must be LUM-enabled on the server.
- The users must be members of a LUM-enabled group on the server holding the volumes.
- Samba users must be created in a container or partition that has a <Samba-qualified password policy> assigned to it.

K.2.2 eDirectory contexts

- **AFP:** Requires that user contexts be specified during the YaST configuration. These are the contexts under which the user objects will be searched for during an authentication. In a name-mapped (existing tree) install, if the context resides in a DSfW domain, the context can be specified either in the domain name format (Active Directory format) or in the X.509 format.
- **CIFS:** The eDirectory contexts of users can be specified either in the domain name format (Active Directory format) or in the X.509 format.
- **Samba:** Depends on LUM to search for the user in eDirectory and therefore doesn’t require an eDirectory context.

K.2.3 Password Policies and Assignments

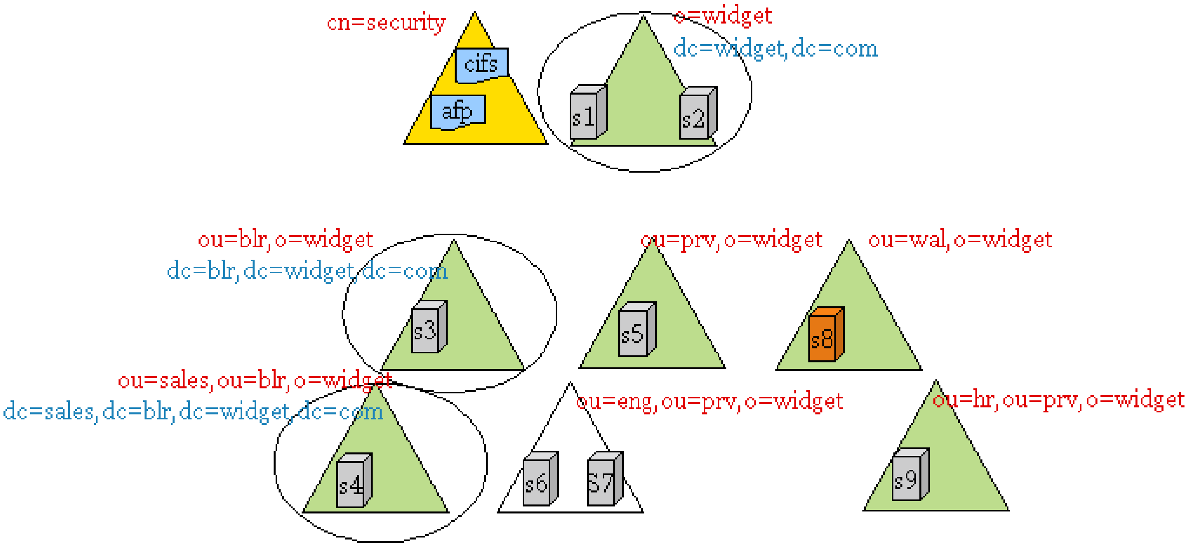
- **Samba:** Creates a default password policy, but does not attach this policy to any user.
- **DSFW:** The password policy in a DSfW environment is modeled after Active Directory Password policies. There is a single Password policy at the domain level, and it is configured during provisioning. eDirectory allows you to set policies at the user or container level. However, this is not recommended in a DSfW environment.

K.3 Examples

K.3.1 Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree

- "Tree Setup" on page 297
- "OES/NetWare Servers" on page 297
- "File Services" on page 297
- "User Access to Services" on page 298
- "Rights Required for Installation and Administration" on page 298

Figure K-1 *Example 1*



Tree Setup

The WIDGETS_INC tree has the following configuration:

- o=widget, ou=blr,o=widget, and ou=sales,ou=blr,o=widget are eDir partitions as well as name mapped domains.
- ou=prv, o=widget, ou=wal,o=widget, ou=hr,ou=prv,o=widget are partitions (but not domains)
- ou=end,ou=prv,o=widget refers to the top of a subtree but not a partition. It is a container under the ou=prv,o=widget partition.

OES/NetWare Servers

- S1-S6 and S9 are OES servers
- S7 and S8 are NetWare servers

File Services

- S1, S2, S3, and S4 are DSfW servers and serve volumes over Samba and NCP
- S5 serves its volumes over AFP and NCP
- S6 serves its volumes over CIFS and NCP

- S7 serves its volumes over AFP, CIFS, and NCP
- S8 serves its volumes over NetWare CIFS, NetWare AFP, and NCP
- S9 serves its volumes over AFP, Samba, and NCP

NOTE: Although Novell CIFS and Samba can both be installed on the same machine, they cannot run together because of a port conflict. The administrator can configure either Samba or Novell CIFS on a single machine, but not both.

User Access to Services

Users from all over the tree can access services running on S1-S9. In order for users to be able to access AFP/CIFS services, the search contexts (eDirectory contexts) for these services should be configured to the subtrees under which those users can be found.

Rights Required for Installation and Administration

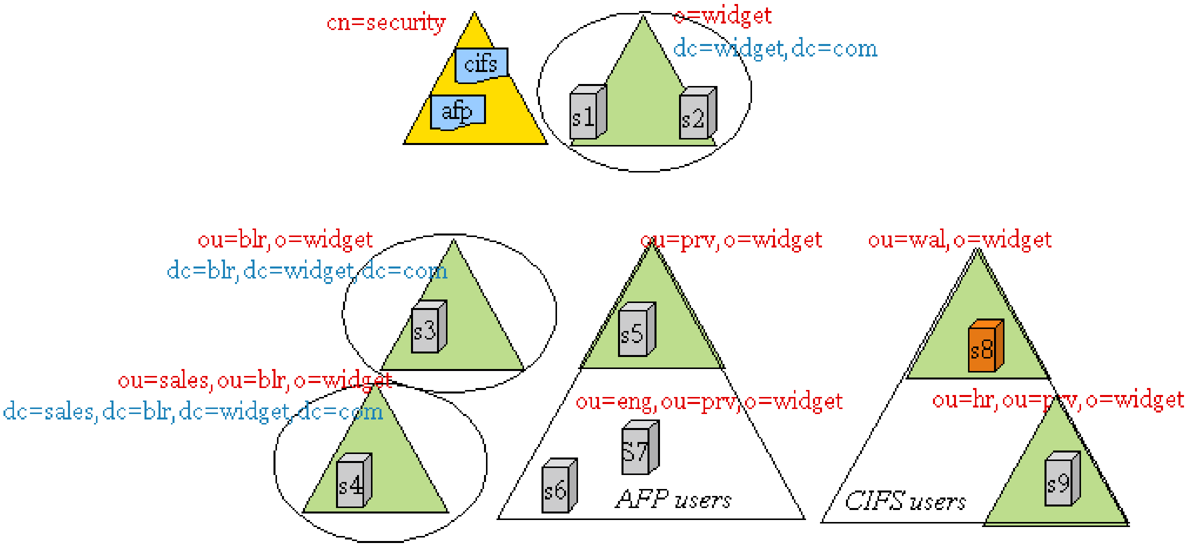
Installation and configuration in iManager must be done by an OES administrator. This is typically a container administrator in eDirectory who has supervisory privileges over the container where the server is being installed. This need not be the tree administrator.

K.3.2 Example 2: Mutually Exclusive Users

- "File Services" on page 298
- "Users" on page 299

In this scenario, the setup of the tree and file services is similar to that in Example 1, but the users are local to the context where a particular service is installed.

Figure K-2 *Example 2*



File Services

- S1, S2, S3, and S4 are DSfW servers and serve their volumes over Samba and NCP

- S5, S6, and S7 serve their volumes over AFP and NCP
- S8 and S9 serves their volumes over CIFS and NCP

Users

For example, u1 is a user under the container ou=prv,o=widget and is expected to access AFP services on S5, S6, and S7. Similarly, u2 is a user under the container ou=wal,o=widget and is expected to access CIFS services on S8 and S9.

K.4 Deployment Guidelines for Different Servers and Deployment Scenarios

- Section K.4.1, "Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services," on page 299
- Section K.4.2, "Deployment Scenario 2: Mutually /Exclusive Users," on page 301
- Section K.4.3, "Deployment Scenario 3: Simple deployments," on page 301
- Section K.4.4, "Modifying User Password Policies after AFP/CIFS/Samba/DSfW Is Installed," on page 301
- Section K.4.5, "Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.," on page 301
- Section K.4.6, "Enabling File Access for DSfW Servers Across Domains," on page 302

K.4.1 Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services

- "First Server in a New Tree (Example1)" on page 299
- "Subsequent Servers in a Tree (Example 1)" on page 300

First Server in a New Tree (Example1)

- "Not recommended—non-name-mapped (new tree) S1 (DSfW) server" on page 299
- "Non-DSFW Server" on page 300

Not recommended—non-name-mapped (new tree) S1 (DSfW) server

Installation is the same as for the Forest Root Domain (FRD). The tree is named as per domain naming standards. Samba is installed as part of DSFW installation. Neither AFP nor Novell CIFS can be installed/configured on this server because they are not compatible with the DSFW server.

In order for users to access NSS volumes on this server through Samba, the users need to fit the following constraints:

- They must be LUM-enabled
- Cross domain access is necessary for users from outside of the DSFW domain corresponding to this server to access the volumes on this server. This can be achieved by adding those contexts to the LUM context for the LUM workstation object that represents the domain controller.
- Winbind translates user principles to UIDs for non-NSS volumes. LUM enabling is not required for non-NSS volume access.

Non-DSFW Server

If the first server in the tree is a non-DSFW server, then any combination of AFP, Novell CIFS, or Samba can be installed on this server. Because the tree is being newly created, the users, the proxy users (system users), and the Password policies will not be present. Use the following procedure for installation:

1. Install and configure the server with eDirectory, NSS, and other core services, but without selecting file access services.
2. Use auto-created common proxy user in eDirectory configuration for the OES services.
3. Use iManager to create a system user (proxy user) to be used for the OES services.
4. Use the Yast install to configure the Novell AFP and Novell CIFS services as follows:

   4a Use an auto-generated common proxy user for all the services.

   4b Specify the contexts under which to search for the AFP or CIFS users.
5. If the AFP/CIFS/Samba user objects are present on NetWare servers, upgrade Novell Security Services version 2.0.6 in order to upgrade to NMAS 3.2 on NetWare.

Subsequent Servers in a Tree (Example 1)

- "S2, S3, S4" on page 300
- "S5" on page 300
- "S6" on page 300
- "S7" on page 300
- "S8" on page 300
- "S9" on page 301

S2, S3, S4

Administrators need to decide whether these servers should be installed on a new domain or as additional domain controllers during capacity planning and deployment design. Follow the *OES 2 SP3: Domain Services for Windows Administration Guide* to deploy S3 and S4 in the tree.

S5

1. Use an auto-generated common proxy user for all the services.

S6

Use the same procedure as for S5.

S7

Use the same procedure as for S5 and S6.

S8

- AFP and CIFS on NetWare don't require proxy users or password policies for service access.

- NMAS needs to be upgraded to 3.2+, if this server hosts the only writable replica for a partition with AFP or CIFS users.
- If this NetWare box is migrated to OES2 SP2, the AFP and CIFS users are enabled for Universal Password. They need to either use a plain text authentication method, or log in through NCP (Novell Client) to synchronize their NDS passwords to the Universal Password. AFP can auto-synchronize the Universal Password if the default DHX authentication method is used.

S9

- Use the same procedure as for S5.
- Either use a common proxy user for all the services (AFP), or allow auto-generation of the proxy user/password for each AFP.

K.4.2 Deployment Scenario 2: Mutually /Exclusive Users

In some trees, AFP, CIFS, and Samba might be employed, but the users are partitioned in such a way that each user has access to AFP, to CIFS or to Samba, but not to all of them.

S1, S2, S3, S4

DSfW servers with Samba. All the users are under dc=blr,dc=widgets,dc=com.

- You can use the default Password policy provided by Domain Services for Windows for all the users in this subtree.
- You can create and use a single proxy user/password under dc=blr,dc=widgets,dc=com for all the servers providing Samba.

K.4.3 Deployment Scenario 3: Simple deployments

Simple deployments require very little planning.

Auto-generated proxy users by each service might be a good idea.

K.4.4 Modifying User Password Policies after AFP/CIFS/Samba/DSfW Is Installed

After a new password policy is assigned to a Samba or DSfW user, rerun the YaST–based configuration and select the new Password policies.

K.4.5 Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.

After a new password policy is assigned to a Samba or DSfW user, rerun the YaST–based configuration and select the new Password policies.

K.4.6 Enabling File Access for DSfW Servers Across Domains

DSfW requires that users be LUM-enabled to access NSS file services through Samba. For a user to access a DSfW server in a different domain, the user needs to be a LUM-enabled user on the other server. DSfW provisioning establishes shortcut trust between domains. Users from other domains in the forest can access non-NSS volumes as long as they have rights on the resources.

To achieve this, the context of the partition root for the user object should be added as a search context for LUM. This needs to be done in addition to the trustee rights provided to the user (or the user's group) as part of file system rights.

L Documentation Updates

This section summarizes the changes made to this manual since the initial release of Novell Open Enterprise Server 2.

June 5, 2013

Chapter or Section Changed	Summary of Changes
"Using the Identity Manager 3.6.1 Bundle Edition" on page 163	Fixed broken links.
Various	The iFolder team no longer publishes the iFolder 3.8.4 documentation in HTML format. All broken link coding has been removed. Text has been retained for manually accessing the PDF documentation.

May 3, 2013

Chapter or Section Changed	Summary of Changes
"New or Changed with the April 2013 Patch Release" on page 15	New section.

January 12, 2013

Chapter or Section Changed	Summary of Changes
"New or Changed with the January 2013 Patch Release" on page 15	New section.

December 5, 2012

Chapter or Section Changed	Summary of Changes
"Novell FTP (Pure-FTPd) and OES 2" on page 202	Updated statement regarding gateway functionality.

August 7, 2012

Chapter or Section Changed	Summary of Changes
"Changing Proxy Passwords Automatically" on page 288	Updated explanation to reflect change coming in next patch. Cronjob execution will then occur on the 15th of every month.

April 20, 2012

Chapter or Section Changed	Summary of Changes
Section 22.4.15, "Port/Service: smb (139/tcp)," on page 235	Section added.

April 19, 2012

Chapter or Section Changed	Summary of Changes
Table F-1 on page 261	Removed the reference to Tomcat Manager, which is a NetWare-only tool.

April 13, 2012

Chapter or Section Changed	Summary of Changes
Step 2 on page 279	Changed examples to use LDAP syntax.

January 16, 2012

Chapter or Section Changed	Summary of Changes
Throughout	Formatted to comply with corporate standard.

December 13, 2011

Chapter or Section Changed	Summary of Changes
Section 22.4, "Resolving Nessus Security Scan Issues," on page 229	New section added.

September 6, 2011

Chapter or Section Changed	Summary of Changes
All	Guide content revised to reflect support for SLES 10 SP4 as the base platform for OES 2 SP3.

August 2, 2011

Chapter or Section Changed	Summary of Changes
Chapter 2, “What About SLES 10 SP4?,” on page 25	Added a link to instructions for preventing the upgrade in ZLM 11.

July 29, 2011

Chapter or Section Changed	Summary of Changes
“Planning Your OES 2 Implementation” on page 29	Removed outdated recommendation to reset the common proxy user password.

July 14, 2011

Chapter or Section Changed	Summary of Changes
“Assigning the Common Proxy to Existing Services” on page 279	Corrected example to use LDAP syntax, i.e. a comma (,) rather than a dot (.) (cn=admin,o=novell), clarified that this is for the administrator doing the installation, and also mentioned that running the script enables the automatic password change feature.

May 10, 2011

Chapter or Section Changed	Summary of Changes
Chapter 2, “What About SLES 10 SP4?,” on page 25	Included a notice that SLES 10 SP4 is not currently compatible with OES 2 SP3.

April 25, 2011

Chapter or Section Changed	Summary of Changes
Appendix B, “Changing an OES 2 SP3 Server’s IP Address,” on page 247	Updated the IP address change section for OES 2 SP3.

March 3, 2011

Chapter or Section Changed	Summary of Changes
Chapter 13, “Network Services,” on page 101	Updated the SLP information to better reflect and explain changes introduced in SP3.

February 3, 2011

Chapter or Section Changed	Summary of Changes
Chapter 1, “What’s New or Changed,” on page 15	Provided more direct access to what’s new information for SP3.

December 2010

Chapter or Section Changed	Summary of Changes
Entire guide	General updates for SP3.

July 15, 2010

Chapter or Section Changed	Summary of Changes
Section 1.7.1, “Dynamic Storage Technology,” on page 22 and Table 4-1 on page 29	These sections incorrectly stated that Dynamic Storage Technology (DST) is supported on NCP and POSIX volumes. Although that functionality was initially planned, and Novell hopes to add support for additional volume and file system types in a future release, DST is currently supported on only Novell Storage Services (NSS) volumes.

November 2009

Chapter or Section Changed	Summary of Changes
Various	The guide was updated to include OES 2 SP2.

July 31, 2009

Chapter or Section Changed	Summary of Changes
“System User and Group Management in OES 2 SP3” on page 269.	Completely reworked and expanded Section.
“Administrative Users in OES 2 SP3” on page 293.	New Section.

June 22, 2009

Chapter or Section Changed	Summary of Changes
"Avoid Uninstalling eDirectory" on page 67.	New Section.
"Novell-tomcat Is for OES Use Only" on page 72.	New Section.

May 6, 2009

Chapter or Section Changed	Summary of Changes
"SLP" on page 116.	Removed all information and instructions that refer to incompatibilities between Novell SLP and OpenSLP. This information was outdated. Although there are differences in the two SLP services (see Table 13-4 on page 118), they are completely compatible regarding the sharing of service information.

April 23, 2009

Chapter or Section Changed	Summary of Changes
"What's New or Changed" on page 15.	In response to a user comment, reorganized section for clarity.

April 7, 2009

Chapter or Section Changed	Summary of Changes
Throughout the guide.	General editing changes. Nothing substantive.