

## Domain Services for Windows Administration Guide

# Novell® Open Enterprise Server

**2.0 SP1**

December 2008

[www.novell.com](http://www.novell.com)



## Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to [www.novell.com/info/exports/](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.

Copyright © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the online documentation for this and other Novell products, and to get updates, see [www.novell.com/documentation](http://www.novell.com/documentation).

## **Novell Trademarks**

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

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>9</b>
<b>1 Overview</b>	<b>11</b>
1.1 Features and Benefits	11
1.2 Architectural Overview	12
1.3 Basic Directory Services Concepts	13
1.3.1 Domains, Trees, and Forests	13
1.3.2 Naming	14
1.3.3 Security Model	14
1.3.4 Groups	14
1.4 Deployment Scenarios	14
1.5 Differences between the DSfW LDAP Server and the eDirectory Server	15
<b>2 Installing and Configuring Domain Services for Windows</b>	<b>17</b>
2.1 General Prerequisites	17
2.2 DNS Settings in a DSfW Environment	18
2.3 Unsupported Service Combinations	19
2.4 Installing DSfW	19
2.4.1 Installing the First DSfW Server in a New eDirectory Tree	22
2.4.2 Installing the First DSfW Server in an Existing eDirectory Tree	29
2.4.3 Installing a Name-Mapped Child Domain in an Existing DSfW Forest	39
2.4.4 Configuring a Non-Name-Mapped Child Domain in an Existing DSfW Forest	51
2.4.5 Configuring an Additional Domain Controller in a Domain	60
2.4.6 Using a Container Admin to Install and Configure DSfW	67
2.4.7 Migrating NKDC Users to a DSfW Domain	68
2.5 Configuring DNS in a DSfW Environment	69
2.6 Configuring a Domain Controller as a Backup Domain Controller	70
2.7 Utilities Not Supported in DSfW	71
2.8 Post-Install Operations	71
2.8.1 Restarting DNS	71
2.8.2 Network Ports Used by DSfW	71
2.9 Restarting the DSfW Services	72
2.10 Verifying the Installation	72
2.11 Removing a DSfW Server	73
2.11.1 Transferring the ADPH Master Role to Other Domain Controllers	74
2.11.2 Transferring Role from an Primary Domain Controller to an Additional Domain Controller	75
2.11.3 Removing Unknown Objects After Removing an Additional Domain Controller	76
2.11.4 Child Domain Installation on a Non-name-mapped Setup	76
<b>3 Logging In from a Windows Workstation</b>	<b>77</b>
3.1 Joining a Windows Workstation to a DSfW Domain	77
3.2 Logging In to a DSfW Domain	80
3.3 Logging Out	80

<b>4</b>	<b>Creating and Provisioning Users</b>	<b>81</b>
4.1	Creating Users in iManager	81
4.2	Creating Users in MMC	83
4.3	Managing Users	84
4.3.1	Moving User Objects Across Containers	84
4.3.2	Primary Group Appears Twice in the memberOf Properties Page	84
4.3.3	Adding Newly Created Users to a Group gives Error Message	84
4.3.4	Dynamic Group Is Not Supported in DSfW	84
<b>5</b>	<b>Managing Group Policy Settings</b>	<b>85</b>
5.1	Using the Users and Computers Tool	85
5.2	Group Policy Objects	86
5.2.1	Account Policies and Gpo2nmas	87
5.2.2	Enforcing Computer Configuration and User Configuration	88
5.2.3	Known Issues	88
5.2.4	Troubleshooting	88
5.3	Group Policy Management	89
5.3.1	Blocking GPO Inheritance in DSfW	89
5.3.2	Ignore Warnings while Backing up Group Policies	89
5.3.3	WMI Filters Cannot be Applied for Processing GPOs	89
<b>6</b>	<b>Managing Trust Relationships in Domain Services for Windows</b>	<b>91</b>
6.1	What is a Trust?	91
6.2	Cross-Forest Trust Relationships	92
6.2.1	Creating a Cross-forest Trust between Active Directory and Domain Services for Windows Forests	92
6.2.2	Shortcut Trusts	123
<b>7</b>	<b>Schema</b>	<b>125</b>
7.1	Schema Objects	125
7.1.1	Syntaxes	128
7.1.2	Attribute Mappings	129
7.1.3	Special Attributes	130
7.1.4	Class Mappings	132
7.2	Extending the Third-Party Schema	132
7.3	Changing the PAS Status of an Attribute	133
<b>8</b>	<b>Printing in the Domain Services for Windows Environment</b>	<b>135</b>
8.1	Deploying iPrint in a DSfW Partition	135
8.2	Setting Up iPrint	135
8.3	Special Handling for iPrint on DSfW	135
8.3.1	Secure and Non-Secure Printing	136
8.3.2	Using a Common Driver Store in a DSfW partition	136
8.4	iPrint Clustering in a DSfW Environment	136
8.4.1	iPrint Clustering on NSS Clusters	136
<b>9</b>	<b>Upgrade and Migration Issues</b>	<b>137</b>
9.1	Upgrading from OES 1.0 Linux	137
9.2	Migrating Data to a Domain Services for Windows Server	137

<b>10 Providing Access to Server Data</b>	<b>139</b>
10.1 Accessing Files by Using Native Windows Methods	139
10.1.1 Samba: A Key Component of DSfW	139
10.1.2 Samba in the DSfW Environment	140
10.1.3 Creating Samba Shares in iManager	141
10.1.4 Creating Samba Shares in the smb.conf File	143
10.1.5 Assigning Rights to Samba Shares	143
10.1.6 Adding a Network Place	145
10.1.7 Adding a Web Folder	146
10.1.8 Mapping Drives to Shares	146
10.2 Accessing Files by Using the Novell Client for Windows	147
10.3 Accessing Files in Another Domain	147
<b>11 Configuring Domain Services for Windows for Novell Cluster Services</b>	<b>149</b>
11.1 Services that Can Be Clustered	149
<b>12 Troubleshooting</b>	<b>151</b>
12.1 Supported Patterns	151
12.2 Troubleshooting DSfW	151
12.2.1 If administrator and default group objects are accidentally deleted	152
12.2.2 Tree admin is not automatically granted rights for DSfW administration	153
12.2.3 DSfW services stop working if the concurrent LDAP bind limit is set to 1	153
12.2.4 The provision utility succeeds only with the <i>--locate-dc</i> option	153
12.2.5 Users are not samified when the RID master role is seized	154
12.2.6 Shared volumes are not accessible	154
12.2.7 Users cannot join a workstation to a domain	154
12.2.8 Making the DSfW server working when the IP address is changed	154
12.2.9 Requirements for Samba/CIFS aAccess to NSS volumes via DSfW	156
12.2.10 Identifying novell-named hang	157
12.3 iPrint Issues	157
12.3.1 Driver store fails to create in a name-mapped FRD	157
<b>13 Miscellaneous</b>	<b>159</b>
13.1 Configuring DSfW with Windows DNS server	159
<b>Glossary</b>	<b>161</b>





# About This Guide

This documentation describes how to install, configure, and use Novell® Domain Services for Windows on a Novell Open Enterprise Server (OES) 2 server.

- ♦ Chapter 1, “Overview,” on page 11
- ♦ Chapter 2, “Installing and Configuring Domain Services for Windows,” on page 17
- ♦ Chapter 3, “Logging In from a Windows Workstation,” on page 77
- ♦ Chapter 4, “Creating and Provisioning Users,” on page 81
- ♦ Chapter 5, “Managing Group Policy Settings,” on page 85
- ♦ Chapter 6, “Managing Trust Relationships in Domain Services for Windows,” on page 91
- ♦ Chapter 7, “Schema,” on page 125
- ♦ Chapter 8, “Printing in the Domain Services for Windows Environment,” on page 135
- ♦ Chapter 9, “Upgrade and Migration Issues,” on page 137
- ♦ Chapter 11, “Configuring Domain Services for Windows for Novell Cluster Services,” on page 149
- ♦ Chapter 10, “Providing Access to Server Data,” on page 139
- ♦ Chapter 12, “Troubleshooting,” on page 151

## Audience

This guide is intended for network installers and administrators.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to [www.novell.com/documentation/oes2/index.html](http://www.novell.com/documentation/oes2/index.html) and enter your comments there.

## Documentation Updates

For the most recent version of the *OES 2: Domain Services for Windows Administration Guide*, see the latest [Novell Open Enterprise Server 2 documentation \(http://www.novell.com/documentation/oes2/index.html\)](http://www.novell.com/documentation/oes2/index.html).

## Documentation Conventions

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

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

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

Novell Domain Services for Windows (DSfW), a component of Open Enterprise Server (OES) 2 SP1, creates seamless cross-authentication capabilities between Windows/Active Directory\* and Novell OES 2 Linux/eDirectory™ servers. This suite of technologies allows Novell customers with Windows networking environments to set up one or more “virtual” Active Directory domains in an eDirectory tree. Users can then log in and authenticate to both eDirectory and Active Directory from a Windows workstation without requiring multiple logins or having the Novell Client™ for Windows installed.

With Domain Services for Windows, eDirectory users can use familiar Windows desktop operations to access file services regardless of the platform/operating system where the service resides. Users can access Novell Storage Services™ (NSS) volumes on Linux servers by using Samba shares or NTFS files on Windows servers that use CIFS shares. eDirectory users can also access shares in trusted Active Directory forests.

- ♦ [Section 1.1, “Features and Benefits,” on page 11](#)
- ♦ [Section 1.2, “Architectural Overview,” on page 12](#)
- ♦ [Section 1.3, “Basic Directory Services Concepts,” on page 13](#)
- ♦ [Section 1.4, “Deployment Scenarios,” on page 14](#)
- ♦ [Section 1.5, “Differences between the DSfW LDAP Server and the eDirectory Server,” on page 15](#)

## 1.1 Features and Benefits

DSfW is designed to simplify the network infrastructure in mixed Windows/OES 2 SP1 Linux environments, thereby reducing costs and streamlining IT operations. Minimal changes are required to the default authentication, authorization, and replication mechanisms in existing eDirectory and Active Directory environments. DSfW enforces the Active Directory security model in eDirectory and applies it to all users and groups within the DSfW domain, regardless of the tool used to create the users and groups. Both Microsoft\* and Novell applications can be used unmodified. Resources in either the Active Directory or eDirectory environment remain securely accessible by eDirectory users.

Specific benefits of DSfW include the following:

- ♦ **Clientless login and cross-platform file access for Windows users:** From a standard Windows workstation, users can authenticate to an OES 2 SP1 Linux server running eDirectory without the need for the Novell Client software or multiple logins. After the Windows workstations have joined the DSfW domain, authorized users can log in and access the file and print services they are authorized to use, whether the services are provided by OES 2 SP1 Linux servers in the DSfW domain or Windows servers in a trusted Active Directory domain.
- ♦ **Unified repository of user account information:** DSfW is not a directory synchronization solution. Each user is represented by a single user account, and that account can reside in either eDirectory or Active Directory. A single password is used to authenticate each user to resources in either environment.

- ♦ **Support for cross-domain and cross-forest trust relationships:** DSfW allows administrators to create cross-domain and cross-forest trusts between a Windows 2003 Active Directory domain/forest and a DSfW domain/forest. This allows authenticated and authorized DSfW users to access data on servers in an Active Directory domain/forest.
- ♦ **Support for existing management tools:** Administrators can use familiar tools for their environment, such as iManager for OES 2 SP1 and Microsoft Management Console (MMC) for Windows, thus eliminating the need for re-training. For example, Windows server/workstation policy settings in the domain Group Policies can be changed by using MMC.

---

**NOTE:** MMC is currently the only tool other than iManager that is supported for use with DSfW.

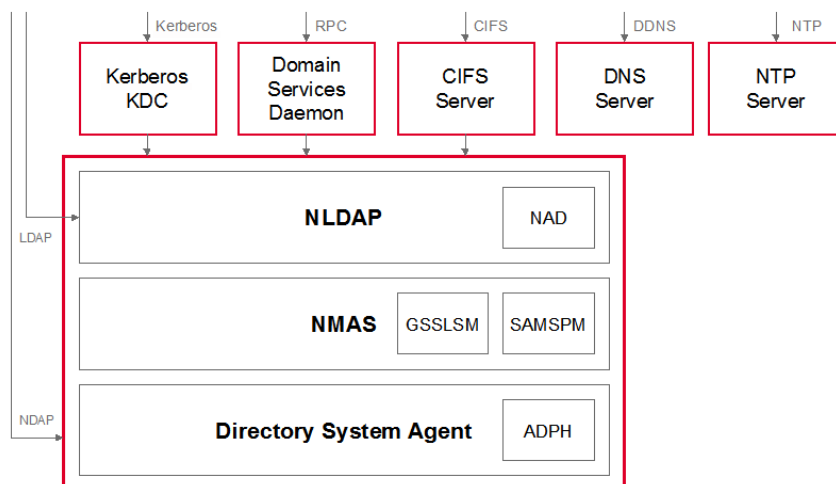
---

- ♦ **Support for common authentication protocols and open standards:** DSfW supports common authentication protocols used in the Windows environment, including Kerberos\*, NTLM, and SSL/TLS.

## 1.2 Architectural Overview

Figure 1-1 illustrates the components included in DSfW and how they interact.

**Figure 1-1** DSfW Components



DSfW is made up of the following technologies:

- ♦ **eDirectory:** eDirectory 8.8 SP4 contains the modifications required for DSfW.
- ♦ **Kerberos Key Distribution Center (KDC):** Provides Active Directory-style authentication.

---

**NOTE:** This is a specialized KDC specifically developed for DSfW. It is different from the [Novell Kerberos KDC \(http://www.novell.com/documentation/kdc15/index.html\)](http://www.novell.com/documentation/kdc15/index.html).

---

- ♦ **NMAS Extensions:** Provide support for GSS-API authentication mechanisms, and for SAMSPM, to generate Active Directory-style credentials when a user's Universal Password is changed.

- ♦ **Active Directory Provisioning Handler (ADPH /Directory System Agent):** Provides agent-side support for the Active Directory information model, regardless of access protocol. It enforces Active Directory security and information models, allocates Security Identifier (SIDs) to users and groups, validates entries, and enables existing eDirectory users and groups to use Active Directory and RFC 2307 authorization.
- ♦ **Domain Services Daemon:** Provides support for Windows RPCs, including Local Security Authority, Security Accounts Manager, and Net Logon.
- ♦ **NAD Virtualization Layer:** Virtualizes the Active Directory information model within eDirectory so that LDAP requests are handled appropriately.
- ♦ **CIFS:** Provides file services and transport for DCE RPC over SMB. The services are provided by the Samba 3.x software included with SUSE® Linux Enterprise Server 10 SP2 and OES 2 SP1.
- ♦ **DNS:** The DNS server has been modified to support GSS-TSIG (Kerberos secured dynamic updates).
- ♦ **NTP:** The NTP server has been modified to support the secure signing of NTP responses.

## 1.3 Basic Directory Services Concepts

To effectively set up and work with DSfW, a basic understanding of both eDirectory and Active Directory is required. This section briefly outlines helpful concepts and terminology.

- ♦ [Section 1.3.1, “Domains, Trees, and Forests,” on page 13](#)
- ♦ [Section 1.3.2, “Naming,” on page 14](#)
- ♦ [Section 1.3.3, “Security Model,” on page 14](#)
- ♦ [Section 1.3.4, “Groups,” on page 14](#)

### 1.3.1 Domains, Trees, and Forests

**Domain:** In Active Directory, a domain is a security boundary. A domain is analogous to a partition in eDirectory.

**Forest:** A forest is a collection of Active Directory domains. A forest is analogous to a tree in eDirectory. You can set up trust relationships to share authentication secrets between domains.

Each Active Directory server has a domain, a configuration, and a schema partition.

**Global Catalog:** Global catalogs are special Active Directory domain controllers that store a complete copy of all the Active Directory objects belonging to the host domain and a partial copy of all other objects in the forest.

Federation can be accomplished through establishing cross-domain and cross-forest trusts.

---

**IMPORTANT:** DSfW requires the Windows 2003 Server functional level for cross-forest trusts. It does not support Windows 2000, Windows NT\*, or mixed mode functional levels.

---

## 1.3.2 Naming

Active Directory uses DC (domain class) naming at the root of a partition, while eDirectory supports other naming attributes like Organization (O) and Organizational Unit (OU). For example, in eDirectory a partition might be specified as:

```
ou=sales.o=company
```

In Active Directory, the partition is specified as:

```
dc=sales,dc=company
```

Every Active Directory domain maps to a DNS domain. The DNS domain name can be derived from the Active Directory domain name. DSfW also follows this rule and supports mapping of eDirectory partitions to DSfW domains.

For example, the `ou=sales.o=company` partition can be mapped to the DSfW domain `dc=sales,dc=company,dc=com`.

## 1.3.3 Security Model

The Active Directory security model is based on shared secrets. The authentication mechanism is based on Kerberos. The domain controller contains all users' Kerberos keys. The KDC, Remote Procedure Call (RPC) server, and Directory System Agent (DSA) operate inside a "trusted computing base" and have full access to all user information.

Active Directory users and groups are identified by unique Security Identifiers. The SID consists of domain-specific prefix, followed by an integer suffix or "relative ID" that is unique within the domain.

For more information about Active Directory, see the [Microsoft Active Directory Technical Library \(http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx\)](http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx).

## 1.3.4 Groups

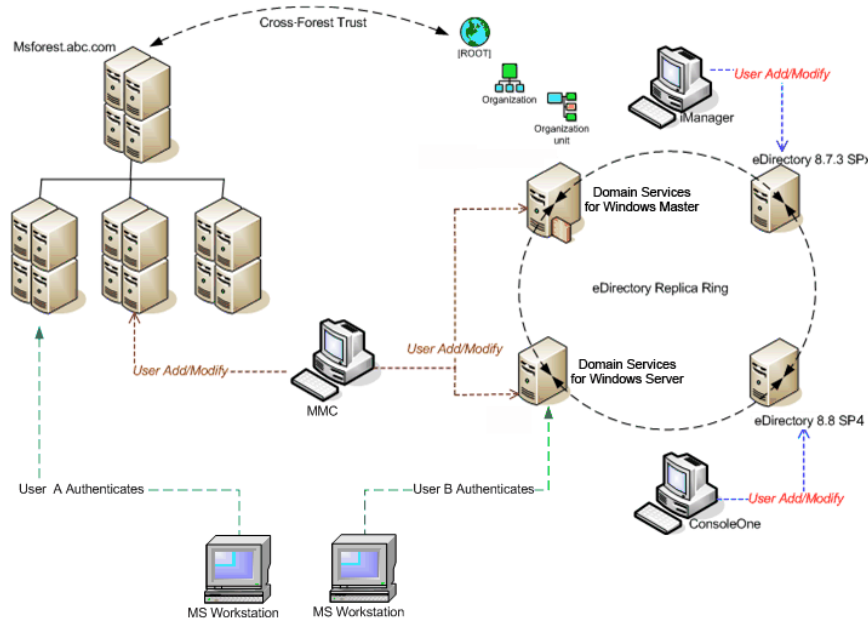
Active Directory supports universal, global, and local groups. DSfW supports the semantics of these groups with different scopes when the group management is performed through MMC. However, there are exceptions. For example validation of group type transitions is not supported. Groups can also contain other groups, which is known as nesting. Other limitations largely result from the way eDirectory supports nested groups. You cannot add a group from other domains as a member of a group. In addition eDirectory supports dynamic groups, because Active Directory does not support them, dynamic groups are not supported in DSfW. All groups created by using iManager or MMC can be used as security principals in an Access Control List in eDirectory. Token groups can only have groups that are enabled as security groups through MMC.

## 1.4 Deployment Scenarios

DSfW supports installing into a new eDirectory tree, an existing eDirectory tree, or an existing forest, creating multiple DSfW domains, and setting up multiple DSfW domain controllers within the same domain.

**Figure 1-2** illustrates a typical deployment scenario in a mixed Novell/Microsoft environment.

**Figure 1-2** Cross-Forest Trust between Active Directory and DSfW



The diagram shows an Active Directory forest and a DSfW forest. Within the DSfW forest are two DSfW servers, an eDirectory 8.8 SP1 server, and an eDirectory 8.7.3 server, configured in the same replica ring. Novell administrators can manage the domain by using iManager connected to any of these servers, and a Microsoft administrator can use MMC connected to one of the DSfW servers. The same set of users can access resources from the Active Directory forest through the establishment of a cross-forest trust, which is a two-way, Kerberos-based, transitive trust between the two forests.

Within the authentication/authorization boundary (realm) established by DSfW, eDirectory replication can be used to expand the scope of users and groups that can access resources in a cross-domain and cross-forest scenario. In the example scenario shown above, users created in eDirectory 8.8 SP4 and 8.7.3 are replicated into the DSfW domain and can therefore access servers in the Active Directory forest as well.

## 1.5 Differences between the DSfW LDAP Server and the eDirectory Server

- LDAP requests, such as Search and Modify, to a DSfW server on port 389 or 636 must use domain name format instead of eDirectory X.500 format. LDAP ports 1389 and 1636 are enabled to support LDAP requests using the traditional X.500 format and to behave as eDirectory ports. This feature is applicable only when DSfW is configured. LDAP requests along with LDAP schematic controls (2.16.840.1.113719.1.513.4.5) allow LDAP requests to select X.500 or the domain format.
- LDAP requests, such as Search and Modify, to a DSfW server on port 389 or 636 return only those objects that exist in the partition and do not search beyond the partition boundary. An LDAP referral is returned, but if the calling LDAP application does not support referrals, it fails to search beyond the partition boundary. A search request on global catalog ports (3268, 3269) spans partition boundaries and searches the entire forest. The result set contains only the attributes marked as Partial Attribute Set (PAS).

- ♦ Attribute and class mappings are changed for some object classes. For example, User and Group object classes are mapped to user and group; server is mapped to ndsServer User and Group object classes are extended to hold additional Active Directory attributes.
- ♦ Every DSfW server has a unique domain partition (required by the Active Directory security model).
- ♦ The eDirectory Multiple Instances feature is not supported on a DSfW server.
- ♦ DSfW does not support NT ACLs. Directory objects are protected by proven eDirectory ACLs. Login authorization and auditing is performed by using NMASTM. Data on the wire is encrypted as mandated by the workstations. All keys, including Kerberos and NTLM, are encrypted by using a per attribute NCI key.



# Installing and Configuring Domain Services for Windows

# 2

This section describes how to install and configure DSfW using the YaST administrative tool. It covers the following topics:

- ♦ [Section 2.1, “General Prerequisites,” on page 17](#)
- ♦ [Section 2.2, “DNS Settings in a DSfW Environment,” on page 18](#)
- ♦ [Section 2.3, “Unsupported Service Combinations,” on page 19](#)
- ♦ [Section 2.4, “Installing DSfW,” on page 19](#)
- ♦ [Section 2.5, “Configuring DNS in a DSfW Environment,” on page 69](#)
- ♦ [Section 2.6, “Configuring a Domain Controller as a Backup Domain Controller,” on page 70](#)
- ♦ [Section 2.7, “Utilities Not Supported in DSfW,” on page 71](#)
- ♦ [Section 2.8, “Post-Install Operations,” on page 71](#)
- ♦ [Section 2.9, “Restarting the DSfW Services,” on page 72](#)
- ♦ [Section 2.10, “Verifying the Installation,” on page 72](#)
- ♦ [Section 2.11, “Removing a DSfW Server,” on page 73](#)

## 2.1 General Prerequisites

This section lists general prerequisites for all DSfW installations. Prerequisites for specific installation scenarios are given in the each installation section.

- ❑ To install DSfW, you need a server that meets the system requirements for SUSE® Linux Enterprise Server (SLES) 10 SP2 and Open Enterprise Server 2 SP1. For more information, see [“Meeting All Server Software and Hardware Requirements”](#) in the *OES2 SP1: Linux Installation Guide*.
- ❑ If you configure DSfW in an existing eDirectory partition, the existing Universal Password policies are overwritten. Administrators must enable *Allow admin to retrieve passwords* option in the new password policies enabling the users to access samba shares from non-DSfW servers in the tree.

---

**NOTE:** It is not required for non name-mapped scenarios.

---

- ❑ Ensure that only root account is created during the SLES installation because administrator or other AD account names can conflict with the DSfW users.
- ❑ During the child domain controller installation, DNS search is expected in the order that has child domain first, followed by forest root domain and then the name server address. To configure DNS in both the child domain and the forest root domain, the order must be changed to have the forest root domain first, followed by the child domain and then the name server.
- ❑ YaST doesn't allow mapping contexts with the Organization (O) container if this container is under Domain Component (DC) or Organizational Unit (OU) containers.

- ❑ You should have access to the installation media for SLES 10 SP2 and OES 2, either on physical CD/DVD media or on a networked installation source server. For more information about installing OES 2 SP1 from an installation source, see “[Setting Up an Installation Source](#)” in the *OES2 SP1: Linux Installation Guide*
- ❑ The Windows clients must be running a supported version of Windows. See [Chapter 3, “Logging In from a Windows Workstation,”](#) on page 77 for more information.
- ❑ DSfW configuration fails on certain NetBIOS names. Do not use the following NetBIOS names:
  - ♦ security
  - ♦ schema
  - ♦ linkengine
  - ♦ administrator
  - ♦ ndsschema
  - ♦ ndscontainer

## 2.2 DNS Settings in a DSfW Environment

Before installing DSfW, review the following notes:

- ♦ By default, DNS is configured on all the forest root domain controllers. For both name-mapped and non-name-mapped installations, the *Configure this server as a Primary DNS server* option is selected by default on a forest root domain controller. Because DSfW installation configures a DNS server on the forest root domain, DSfW services must use the DNS server from one of the DSfW servers for secure updates to work.
- ♦ A YaST page takes additional parameters for DNS configuration. DNS configuration requires three object locations: the contexts of the Locator object, RootServerInfo object, and DNS-DHCP group object. Only one instance of these objects can exist in an eDirectory tree. You must provide the location of existing DNS objects if you are installing into an existing tree with DNS already configured.
- ♦ The default location of the contexts of the Locator object, RootServerInfo object, DNS-DHCP group object, and the DNS server object is the NCP™ server location (`ou=novell,$DOMAIN`). The DNS Server object exists in this location, and the contexts of the Locator object, RootServerInfo object, and DNS-DHCP group object can exist anywhere in the tree in a name-mapped installation. In a non-name-mapped installation, because this is the first server in the tree, these objects are placed in the NCP Server location, such as `ou=novell,$DOMAIN`.
- ♦ A DNS administrator object must be created for DNS server configuration. Provide the name and the location of the DNS administrator object. A new object is created if the DNS Install utility fails to locate the object in the tree. This information is required only if you configure this server as a primary DNS server. Because you are configuring DNS by default, this information is required for forest root domain configurations. For information on installing and configuring Novell® DNS service, refer to “[Planning Your DNS/DHCP Implementation](#)” in the *OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux*.
- ♦ The location of the contexts of the Locator object, RootServerInfo object, and DNS-DHCP group object is automatically populated as the NCP server object location in the YaST page. Edit it if the location is different, such as, when you are configuring an additional domain controller or a child domain controller (when the DNS service is not being configured and you are using an existing DNS server configured in the forest root domain).

- ♦ In order to reduce the complexity of installing an additional domain controller, the additional domain controller design does not allow you to configure DNS services. This is also useful for administrators who might not want to configure many DNS services in a network. Administrators can configure DNS services on any servers later, using the Java\* console or iManager.
- ♦ Because the default refresh interval of the DNS server is more than 10 minutes, any changes made to the DNS settings take effect in the subsequent refresh cycle. For the changes to be applied immediately, the DNS server (novell-named) must be restarted so that the DNS server reads the newer data from the server again.

For information on installing and configuring Novell® DNS service, refer to “**Installing and Configuring DNS**” in the *OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux*

## 2.3 Unsupported Service Combinations

---

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

---

- ♦ File Server (SLES 10 - Samba)
- ♦ Novell AFP
- ♦ Novell Archive and Version Services
- ♦ Novell CIFS
- ♦ Novell Cluster Services™ (NCS)
- ♦ Novell FTP
- ♦ Novell iFolder®
- ♦ Novell NetStorage
- ♦ Novell Pre-Migration Server
- ♦ Novell QuickFinder™
- ♦ Novell Samba

DSfW installation is not supported through Red Carpet®.

## 2.4 Installing DSfW

As part of Open Enterprise Server 2, DSfW is available as a selectable pattern during the SLES 10 SP2 installation via YaST. You must install SLES 10 SP2 with Open Enterprise Server 2 as an add-on product, as instructed in “**Installing Open Enterprise Server 2 SP1 Linux**” in the *OES2 SP1: Linux Installation Guide*. Most of the settings are common for all the installation scenarios, except a few where examples are provided to differentiate these scenarios.

**Table 2-1** *Specific Settings for Installing DSfW*

YaST Section	Heading, Field, or Option	Instructions	Setting for the Example Configuration
Installation Summary: Installation Settings	Click the <i>Software</i> heading.	Select <i>Novell DSfW</i> from the <i>OES Services</i> category.	
Configuration: Hostname	Hostname and Domain Name  Change Hostname via DHCP  <i>Write Hostname to /etc/hosts</i>	Specify the DNS hostname and domain name that you plan to use for this server.  Deselect this option.  Leave this option selected.	Refer to the individual installation scenarios for the hostname and domain name.
Configuration: Network	<i>Network Interfaces</i>	Select <i>Static Address Setup</i> and assign a static IP address for the server's network interface. Change the subnet mask, if necessary.	IP Address: 192.168.1.1
	<i>Detailed Settings &gt; Hostname and Name Server</i>	Specify the IP address of the DNS server in the <i>Name Server 1</i> field and the domain name of the forest root domain in the <i>Domain Search</i> field.	Name Server 1: 192.168.1.1
		<b>IMPORTANT:</b> If you want to configure the child domain controller to act as a primary DNS server, make sure that the DNS servers of the forest root domain and the child domain controller act as passive primary DNS servers of each other's zones, otherwise you cannot configure an additional domain controller as a child domain controller.	

YaST Section	Heading, Field, or Option	Instructions	Setting for the Example Configuration
	<i>Detailed Settings &gt; Routing</i>	<p>If you are accessing the SLES 10 SP2/OES 2 installation source from other servers on the network, specify the IP address of a DNS server that can find the installation source servers as Name Server 2 and type its domain name in the <i>Domain Search</i> field.</p> <p>Specify the IP address of the default gateway for your network.</p>	Domain Search: example.com
Configuration: Service	CA Management and OpenLDAP Server	Accept the defaults.	
Configuration: OES Configuration		Continue with the individual installation scenarios given below.	

Settings in the [Table 2-1](#) are useful when you install both SLES10 SP2 and OES2 SP1 together, with the latter as an add-on product. If SLES10 SP2 is already installed and OES 2 SP1 is subsequently configured as an add-on product, the Network Settings page does not display. You must change the DNS domain name to the DSfW domain name that you want to configure. For changing the DNS domain name, go to the *Yast2 > Network Devices > Network Card* and change the domain name to the DSfW domain name.

After configuring DSfW domain, certain operations such as search and modify might not work as intended if you rename the domain controllers of that domain. For a proper functioning of these operations, you should not rename them.

**NOTE:** For more information on making appropriate settings for installing and configuring DSfW server, refer to the “[Installing Open Enterprise Server 2 SP1 Linux](#)” in the *OES2 SP1: Linux Installation Guide*.

DSfW installation is covered in the following sections:

- ♦ [Section 2.4.1, “Installing the First DSfW Server in a New eDirectory Tree,”](#) on page 22
- ♦ [Section 2.4.2, “Installing the First DSfW Server in an Existing eDirectory Tree,”](#) on page 29
- ♦ [Section 2.4.3, “Installing a Name-Mapped Child Domain in an Existing DSfW Forest,”](#) on page 39
- ♦ [Section 2.4.4, “Configuring a Non-Name-Mapped Child Domain in an Existing DSfW Forest,”](#) on page 51
- ♦ [Section 2.4.5, “Configuring an Additional Domain Controller in a Domain,”](#) on page 60
- ♦ [Section 2.4.6, “Using a Container Admin to Install and Configure DSfW,”](#) on page 67
- ♦ [Section 2.4.7, “Migrating NKDC Users to a DSfW Domain,”](#) on page 68

## 2.4.1 Installing the First DSfW Server in a New eDirectory Tree

This section explains how to install and configure the first DSfW server in a new eDirectory™ tree. At the same time, you are creating a new domain in a new forest. The DSfW server is automatically configured to be a domain controller and acts as a primary DNS server.

- ♦ “Prerequisites” on page 22
- ♦ “Installation Procedure” on page 22

### Prerequisites

Make sure you have performed the prerequisite tasks listed in [Section 2.1, “General Prerequisites,” on page 17](#). No other prerequisites apply to this installation scenario.

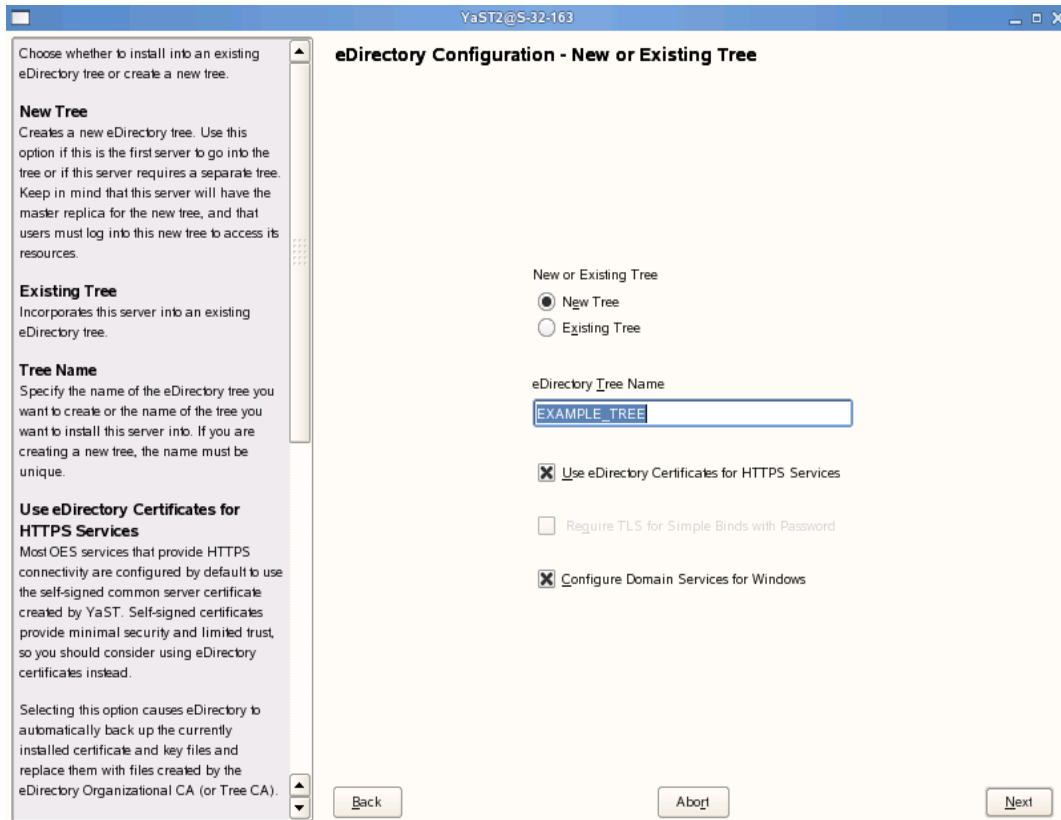
### Installation Procedure

The example configuration shown in this section assumes that you are setting up an eDirectory tree and DSfW server with the following parameters:

- ♦ **Tree Name:** EXAMPLE\_TREE
- ♦ **Primary IP Address of the Server:** 192.168.1.1
- ♦ **Hostname (also used for server name):** oesdc
- ♦ **Domain Name:** example.com
- ♦ **Domain NetBIOS Name:** EXAMPLE

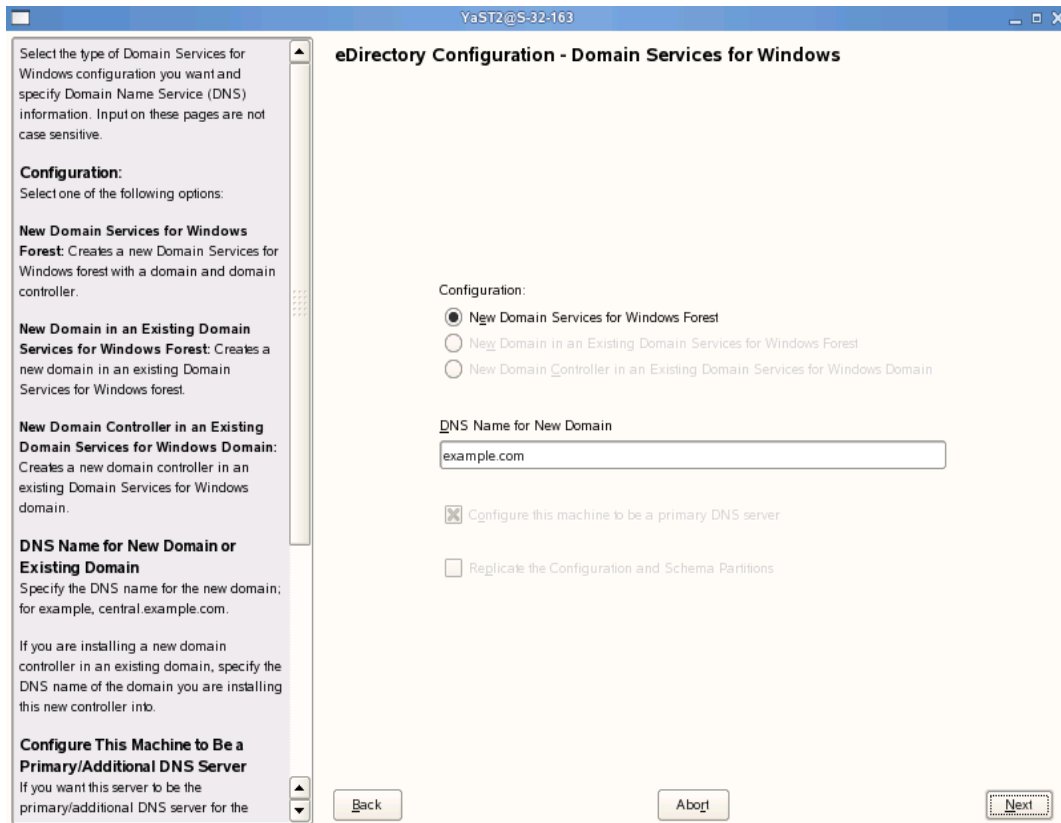
As you follow the procedure below, substitute your own names and IP addresses for the ones used in the example configuration.

- 1 On the first eDirectory configuration page in YaST, specify that you are installing the server into a new eDirectory tree:



- 1a Select *New Tree* and specify a name for the tree (EXAMPLE\_TREE in the example configuration).
- 1b Select *Use eDirectory certificates for HTTPS Services* if you want your OES services that provide HTTPS connectivity to use the more secure eDirectory certificates instead of the self-signed certificates created by YaST.
- 1c Make sure *Configure Domain Services for Windows* is selected. It is not possible to configure DSfW later, as you can with other OES services. It must be configured now, along with eDirectory.
- 1d Click *Next* to continue.

## 2 Select settings for the DSfW configuration and DNS:



**2a** YaST displays a DNS name for the new domain, based on the domain name you configured earlier (example.com in the example configuration). Leave this setting as it is.

---

**TIP:** A container named example can be mapped to any of the following:

- ♦ example.company.com
- ♦ exmaple.division.company.com
- ♦ example.company.countrycode

---

For the first server, the *Configure this machine to be a primary DNS server* option is disabled because this server is automatically configured as a primary DNS server.

**2b** Click *Next* to continue.



- 3 Leave the NetBIOS name setting at the default (EXAMPLE in the example configuration), then click *Next* to continue.

Specify the information required to create a context for this server in the new domain or as a new domain controller in a Domain Services for Windows forest.

**Domain NetBIOS Name**

Specify a NetBIOS name for the Domain Services for Windows domain, or specify the NetBIOS name for the Domain Services for Windows domain you are installing this domain or controller into.

By default, this is the domain context name without the parent context. For example, in the domain `cn=central,dc=example,dc=com`, the default NetBIOS name is `central`.

Domain NetBIOS Name

EXAMPLE

Back Abort Next

The domain NetBIOS name defaults to the domain context name without the parent context. This is the name that is displayed in the Windows login dialog box when you log in to the domain.

- 4 Specify the DSfW Administrator password in both fields to verify that you are typing it correctly, then click *Next*.

YaST2@melanin

**eDirectory Configuration - Domain Services for Windows**

When creating a new domain, specify a password for the Domain Services for Windows Administrator account.

If creating a new domain controller, specify the existing password for an existing the Domain Services for Windows Administrator account to allow this controller access to the domain information.

**New or Existing Domain Administrator Name**

Note the name and context of the Administrator account. This is the Administrator you are entering the password for. You will use this account to log in to the Domain Services for Windows domain.

**Specify Administrator Password**

Specify a password for

New Domain Administrator Name  
cn=Administrator.cn=Users.dc=example.dc=com

Specify Administrator Password  
\*\*\*\*\*

Verify Administrator Password  
\*\*\*\*\*

Back Abort Next

**5** Select the settings for the local server configuration:

YaST2@melanin

Specify the configuration for the local server in the eDirectory tree.

**Server Context**  
The parent context for the Domain Services for Windows domain is shown.

**Enter Directory Information Base (DIB) Location**  
Specify a location for the eDirectory database. The default path is /var/opt/novell/eDirectory/data/dib but you can use this option to change the location if you expect the number of objects in your tree to be large and if the current file system does not have sufficient space.

**LDAP and Secure LDAP Ports**  
The LDAP and secure LDAP port numbers this server will use to service LDAP requests are shown.

**eDirectory Configuration - Local Server Configuration**

Server Context  
ou=novell.dc=example.dc=com

Directory Information Base (DIB) Location  
/var/opt/novell/eDirectory/data/dib

Enter LDAP Port  
389

Enter Secure LDAP Port  
636

Enter iMonitor Port  
8028

Enter Secure iMonitor Port  
8030

Back Abort Next

- 5a** Leave the location of the Directory Information Base (DIB) at the default setting. This should suffice for most eDirectory servers.
- 5b** Leave the iMonitor port settings at the defaults unless you need to change them to avoid port conflicts with other services.
- 5c** Click *Next* to continue.

## 6 Specify the Novell DNS server information:

**Novell DNS Services Configuration**

Use this dialog to specify options for configuring a DNS server that is integrated with eDirectory on this server.

**Get Context and Proxy User Information from Existing DNS Server**

If you are configuring DNS in an existing tree where DNS is already configured and you want to use the existing Locator, Root Server Info, Group and Proxy User contexts, you can select the 'Get context information from existing DNS server' check box and provide the IP of an NCP server hosting the existing DNS server and click 'Retrieve'. This will fetch the contexts of the Locator, Root Server Info, Group and Proxy User contexts. Make sure the NCP server hosting the existing DNS server is running before hitting 'Retrieve'.

If you do not wish to use existing contexts, you can provide those manually.

**Novell DNS Services Locator Object Context**

Specify the context for the DNS Locator object.  
For example: o=novell

The Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree.

**Novell DNS Services Root Server Info Context**

Specify the context for the DNS Services root

**Common DNS Configuration Object Contexts**

☐ Get context and proxy user information from existing DNS server

Existing Novell DNS server address:  
164.99.91.163  
Retrieve

Novell DNS Services Locator Object Context (e.g. o=novell):  
ou=novell,dc=example,dc=com

Novell DNS Services Root Server Info Context (e.g. o=novell):  
ou=novell,dc=example,dc=com

Novell DNS Services Group Object Context (e.g. o=novell):  
ou=novell,dc=example,dc=com

Proxy User for DNS Management (e.g. cn=myuser,o=novell):  
cn=dnsadmin,dc=example,dc=com

Specify Password for Proxy User  
\*\*\*\*\*

Verify Password for Proxy User  
\*\*\*\*\*

☒ Use Secure LDAP Port

Back Abort Next

- 6a** The *Existing Novell DNS server address* field is pre-populated with the first name server entry from the `/etc/resolv.conf` file.
- 6b** If you are using an existing Novell DNS server for the DSfW domain being configured, select the *Get context and proxy user information from existing DNS server* check box, then click *Retrieve*. Ensure that the IP address being used to retrieve the contexts points to the desired Novell DNS server. This action populates the *DNS Service Locator*, *DNS Group*, and *DNS Root ServerInfo* context fields.
- 6c** If you are configuring Novell DNS server along with the DSfW domain being configured,
- ◆ Specify the context of the DNS service locator object (for example, `ou=novell,dc=example,dc=com`).
  - ◆ Specify the context of the DNS group object (for example, `ou=novell,dc=example,dc=com`).
  - ◆ Specify the context of the DNS Root ServerInfo object (for example, `ou=novell,dc=example,dc=com`).
- 6d** Specify the fully distinguished, typeful name of an eDirectory user. For example: `cn=dnsadmin,dc=example,dc=com` to authenticate to eDirectory during runtime for accessing information for DNS. The user must have eDirectory read, write, and browse rights under the specified context.
- 6e** Specify the password of the eDirectory user that you specified for accessing DNS.

**6f** Use *Secure LDAP Port* option is selected by default to ensure that the data transferred by this service is secure and private. If you deselect this option, the data transferred is in clear text format.

**6g** Click *Next* to continue.

---

**IMPORTANT:** Leave all the inputs as the default. Specify only the proxy user name and password. Specify the inputs in DNS format. The first set of inputs is separated by periods (.) and the proxy user name is separated by commas (,).

---

**7** Complete the remainder of the OES configuration and SLES 10 SP2 installation as instructed in “[Installing Open Enterprise Server 2 SP1 Linux](#)” in the *OES2 SP1: Linux Installation Guide*, taking note of the following guidelines:

- ♦ Be sure to specify a reliable Network Time Protocol (NTP) provider. Novell eDirectory requires that all servers in a tree be time-synchronized. In a single-server scenario, you can specify the local machine as the NTP provider.
- ♦ On the NMAS Methods selection page, you do not need to select *SASL GSSAPI*. The GSSAPI authentication mechanism that DSfW uses is installed automatically.
- ♦ Review the OES configuration summary to ensure that the settings are correct according to your installation plan.

If necessary, click a heading in the summary page to modify an OES service’s configuration.

- ♦ The configuration of eDirectory and DSfW takes some time to complete. Please be patient.
- ♦ For the User Authentication Method, accept the default of *Local*.

**8** When the installation is complete, click *Finish* and wait for the server to reboot.

After the server is installed, see [Section 2.10, “Verifying the Installation,” on page 72](#) to verify that eDirectory and DSfW have been installed and configured correctly.

## 2.4.2 Installing the First DSfW Server in an Existing eDirectory Tree

This section explains how to install and configure the first DSfW server in an existing eDirectory tree. In this scenario, you select an eDirectory container to become the root of a new DSfW forest. You also have the option to enable LDAP name mapping for the container. A new DSfW domain is created in the forest, and the server is automatically configured to be a domain controller. You should make it a primary DNS server as well.

DSfW installation identifies the container and the objects within a partition that are associated with the password policies and modifies them to be associated with the Domain Password Policy. An administrator can review the password policy changes from the `/var/opt/novell/xad/log/dsfw-changes.log` file. Administrators must modify the Domain Password policy to match his domain requirements.

- ♦ “[Prerequisites](#)” on page 30
- ♦ “[Installation Procedure](#)” on page 31

## Prerequisites

In addition to the prerequisites listed in [Section 2.1, “General Prerequisites,”](#) on page 17, the following prerequisites apply to this installation scenario:

- ❑ You must have at least one eDirectory 8.8 SP2 or above server in the tree that holds a writable replica of the [Root] partition. While installing the DSfW server, provide the IP address of this server as the server holding the replica of the [Root] partition.
- ❑ The container you want to become the forest root must already exist in the eDirectory tree. The RDN of domain name being installed and the container name that is mapped from the existing tree must be the same.

For example, if the eDirectory container you are creating the DSfW domain in is `ou=example.o=novell`, the domain name you specify must be `example.com`.

You cannot insert a DSfW domain at the [Root] partition of an existing eDirectory tree. Also, because a `cn=users` container is created in the new domain, there shouldn't be an existing `ou=users` container in the container where the domain is being inserted.

A DSfW domain can only be created in Organization (O), Organizational Unit (OU) and Domain Component (DC) containers. Installing a name-mapped domain to map Country and Locality containers is not supported. However, you can map O and OU under these containers.

---

**NOTE:** If you have extended the schema to define custom container types that you want to use with DSfW, the container object must be derived from LoginProperties and must be able to contain the NCP Server object and various other objects created for the domain.

---

Refer to [Managing Objects \(http://www.novell.com/documentation/edir88/edir88/data/a2iikq.html\)](http://www.novell.com/documentation/edir88/edir88/data/a2iikq.html) in the *Novell eDirectory 8.8 Administration Guide* for instructions on creating and modifying eDirectory container objects.

- ❑ The eDirectory container must be partitioned before you can install the DSfW domain. The partition is the new domain partition for the domain being created.

Refer to [Managing Partitions and Replicas \(http://www.novell.com/documentation/edir88/edir88/data/a2iik.html\)](http://www.novell.com/documentation/edir88/edir88/data/a2iik.html) in the *Novell eDirectory 8.8 Administration Guide* for instructions on partitioning a container.

Also see [Section 2.4.6, “Using a Container Admin to Install and Configure DSfW,”](#) on page 67 for configuring Novell DSfW with container admin credentials.

- ❑ After configuring an eDirectory partition as a DSfW domain, you can log in from a Windows workstation in the domain only if you had Universal Password enabled prior to configuring DSfW.

---

**NOTE:** Universal Password is required for creating DSfW credentials. For users who did not have Universal Password enabled, the DSfW credentials are created when they log in to eDirectory again.

---

- ❑ The first component of the DNS Server name and the container name must be same. For example, a container `example.novell` can be mapped to any of the following domain names:
  - ♦ `example.company.com`
  - ♦ `example.division.company.com`
  - ♦ `example.company.countrycode`

---

**NOTE:** DSfW name-mapped installations can fail if there are time synchronization problems among the servers in the [root] replica ring. To ensure it does not encounter this problem during installation, you must have all the servers in the [root] replica synced correctly before installing DSfW.

---

WMI filters are not supported.

## Installation Procedure

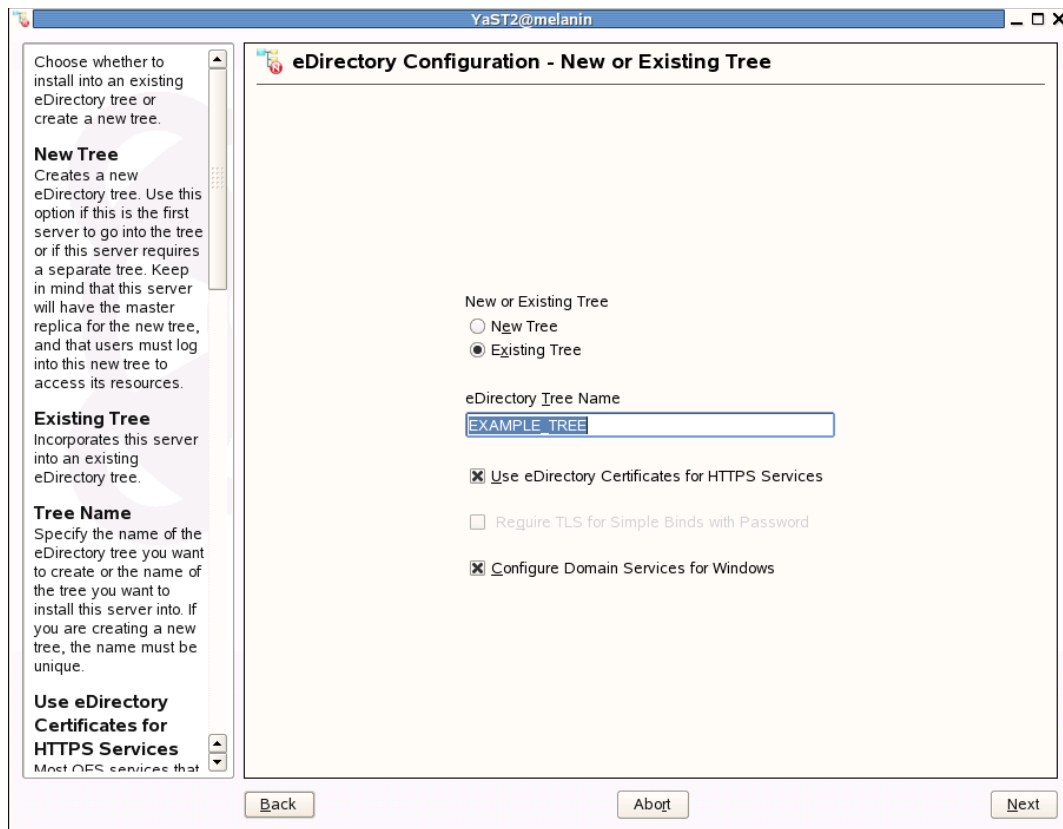
The example configuration shown in this section assumes that you are installing a DSfW server with the following parameters:

- ♦ **Existing eDirectory Tree Name:** EXAMPLE\_TREE
- ♦ **eDirectory Container to Become Forest Root:** ou=example.o=novell
- ♦ **Hostname:** dsfw1
- ♦ **Domain Name:** example.com
- ♦ **Domain NetBIOS Name:** EXAMPLE
- ♦ **Primary IP Address of the DSfW Server:** 192.168.1.1
- ♦ **IP Address of eDirectory 8.8 SP2 Server with Writable Replica of [Root]:** 192.168.1.100
- ♦ **Existing eDirectory Tree Admin Account:** cn=admin.o=novell

As you follow the procedure below, substitute your own names and IP addresses for the ones used in the example configuration.

- 1** If you are installing from an installation source on the network, assign a static IP address to the server instead of getting it from your DHCP server. OES configuration can sometimes fail when the address changes during the network configuration when DHCP address is assigned.
- 2** On the service configuration page, accept the default settings for *CA Management* and *OpenLDAP Server*.

**3** On the first eDirectory configuration page, select the following settings:



**3a** Select *Existing Tree*.

**3b** Specify the eDirectory tree name (EXAMPLE\_TREE in the example configuration).

**3c** Select *Use eDirectory Certificates for HTTPS Services* if you want your OES services that provide HTTPS connectivity to use the more secure eDirectory certificates instead of the self-signed certificates created by YaST.

Do not select this option if you have already installed certificates from a third-party certificate authority.

**3d** Select *Configure Domain Services for Windows*.

**3e** Click *Next* to continue.



**4** Provide information about the existing eDirectory tree:

**IP Address of an Existing eDirectory Server with a Replica**  
Specify the IP address of an existing eDirectory server that is part of the eDirectory tree you are installing this server into.

**Enter NCP Port on the Existing Server**  
Specify the NCP port number of the existing server. The default NCP port for most eDirectory servers is 524.

**Enter LDAP Port on the Existing Server**  
Specify the LDAP port number of the existing eDirectory server specified in the prior field. The default LDAP port for most eDirectory servers is 389.

**Enter Secure LDAP Port on the Existing Server**  
Specify the secure LDAP port number of the existing eDirectory

**eDirectory Configuration - Existing Tree Information**

IP Address of an existing eDirectory server with a replica  
192.168.1.100

Enter NCP Port on the existing server  
524

Enter LDAP Port on the existing server  
389

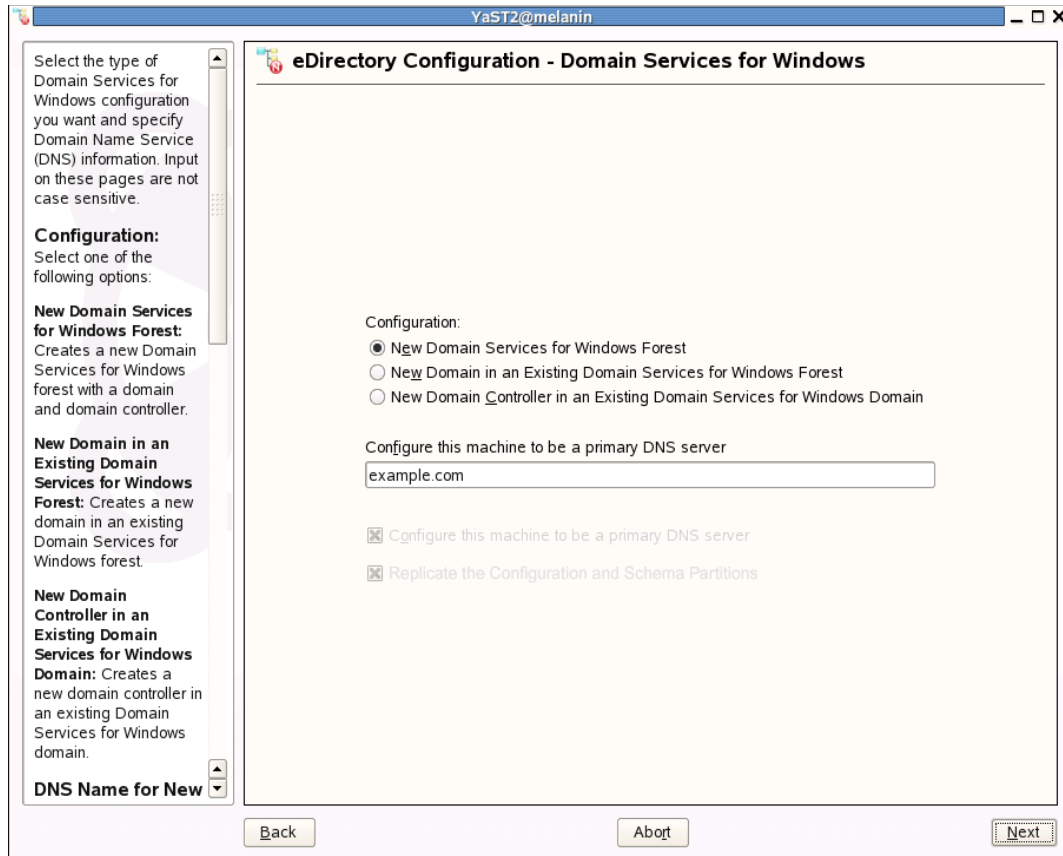
Enter Secure LDAP Port on the existing server  
636

EDN Existing admin name with context (e.g. cn=admin,o=novell)  
cn=admin,o=novell

Admin Password  
\*\*\*\*\*

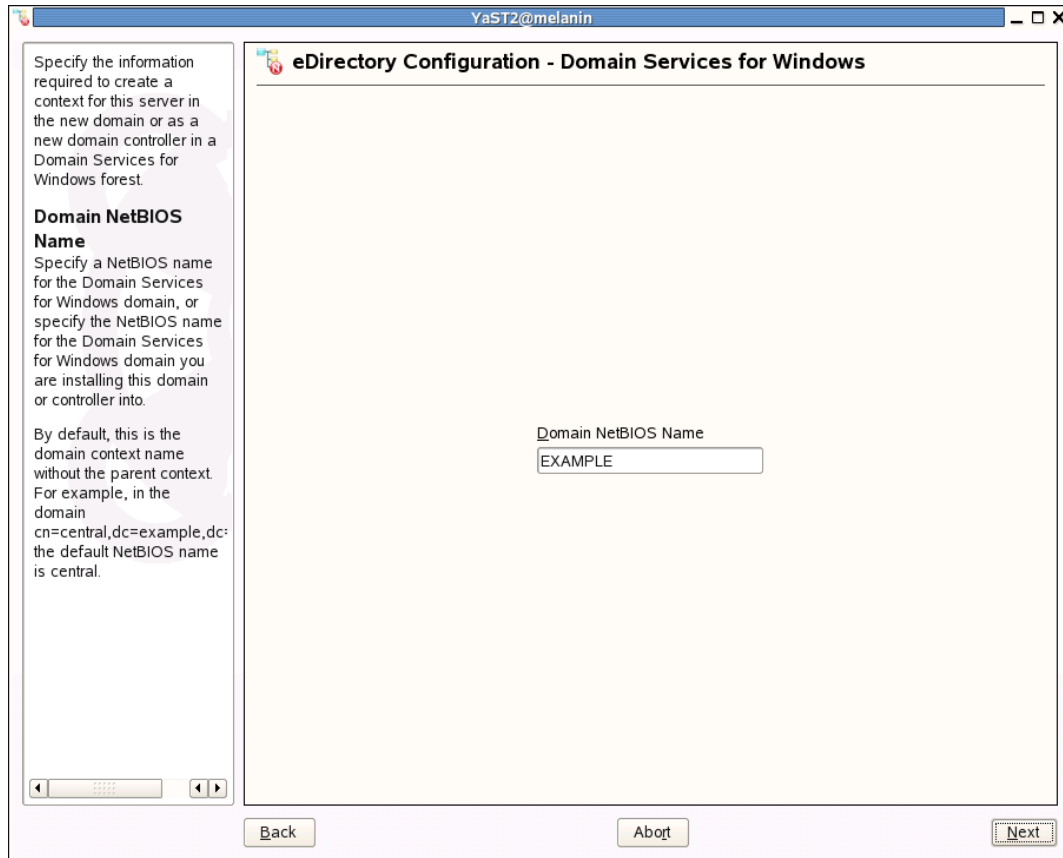
Back Abort Next

- 4a** Specify the IP address of an existing eDirectory server that holds a replica in the tree you are installing this server into. In the example configuration, this is 192.168.1.100.
  - 4b** Leave the NCP and LDAP port parameters at the default settings unless you selected alternative ports when you installed the eDirectory tree. YaST displays the location of the eDirectory administrator.
  - 4c** Specify the password for the eDirectory tree admin account, then click *Next* to continue.
- 5** Select settings for the DSfW configuration and DNS:



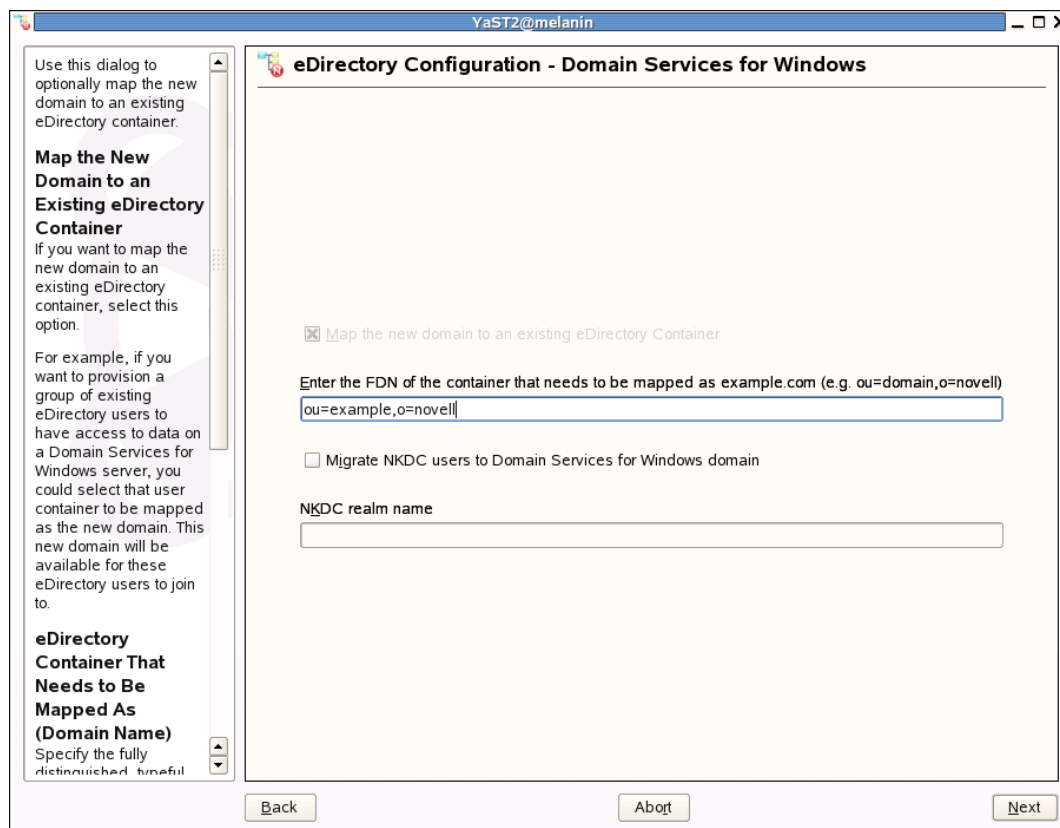
- 5a** Select *New Domain Services for Windows Forest* as the type of configuration.
- 5b** YaST displays a DNS name for the new domain, based on the domain name you configured earlier (example.com in the example configuration). Leave this setting as it is.

- 6 Leave the NetBIOS name setting at the default (EXAMPLE in the example configuration), then click *Next* to continue.



By default, the domain NetBIOS name is the domain name without the parent context. This is the name that is displayed in the Windows logon dialog box when you log in to the domain.

- 7 Specify the name of the eDirectory container that you are mapping the new domain to (ou=example,o=novell in the example configuration).



- 7a If you select *Migrate NKDC users to Domain Services for Windows domain*, users will be migrated from an already existing Novell Kerberos KDC (NKDC) realm to the overlapping DSfW domain. After the migration, the NKDC users become DSfW users. It is possible to migrate only one realm to one DSfW domain. The supported Novell Kerberos KDC release is V1.5.
- 7b Click *Next* to continue.

**8** Select the settings for the local server configuration:

YaST2@melanin

**eDirectory Configuration - Local Server Configuration**

Specify the configuration for the local server in the eDirectory tree.

**Server Context**  
The parent context for the Domain Services for Windows domain is shown.

**Enter Directory Information Base (DIB) Location**  
Specify a location for the eDirectory database. The default path is /var/opt/novell/eDirectory/data/dib but you can use this option to change the location if you expect the number of objects in your tree to be large and if the current file system does not have sufficient space.

**LDAP and Secure LDAP Ports**  
The LDAP and secure LDAP port numbers this server will use to service LDAP requests are shown.

Server Context  
ou=novell,ou=example,o=novell

Directory Information Base (DIB) Location  
/var/opt/novell/eDirectory/data/dib

Enter LDAP Port  
389

Enter Secure LDAP Port  
636

Enter iMonitor Port  
8028

Enter Secure iMonitor Port  
8030

Back About Next

- 8a** Leave the location of the Directory Information Base (DIB) at the default setting. This should suffice for most eDirectory servers.
- 8b** Leave the iMonitor port settings at the defaults unless you need to change them to avoid port conflicts with other services.
- 8c** Click *Next* to continue.

## 9 Enter the Novell DNS server information:

**Novell DNS Services Configuration**

Use this dialog to specify options for configuring a DNS server that is integrated with eDirectory on this server.

**Get Context and Proxy User Information from Existing DNS Server**

If you are configuring DNS in an existing tree where DNS is already configured and you want to use the existing Locator, Root Server Info, Group and Proxy User contexts, you can select the 'Get context information from existing DNS server' check box and provide the IP of an NCP server hosting the existing DNS server and click 'Retrieve'. This will fetch the contexts of the Locator, Root Server Info, Group and Proxy User contexts. Make sure the NCP server hosting the existing DNS server is running before hitting 'Retrieve'.

If you do not wish to use existing contexts, you can provide those manually.

**Novell DNS Services Locator Object Context**

Specify the context for the DNS Locator object.  
For example: o=novell

The Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree.

**Novell DNS Services Root Server Info Context**

Specify the context for the DNS Services root

**Common DNS Configuration Object Contexts**

☐ Get context and proxy user information from existing DNS server

Existing Novell DNS server address:  
192.168.1.1

Retrieve

Novell DNS Services Locator Object Context (e.g. o=novell):

Novell DNS Services Root Server Info Context (e.g. o=novell):

Novell DNS Services Group Object Context (e.g. o=novell):

Proxy User for DNS Management (e.g. cn=myuser,o=novell)

Specify Password for Proxy User

Verify Password for Proxy User

☒ Use Secure LDAP Port

Back Abort Next

- 9a** The *Existing Novell DNS server address* field is pre-populated with the first name server entry from the `/etc/resolv.conf` file.
- 9b** If you are using an existing Novell DNS server for the DSfW domain being configured, select the *Get context and proxy user information from existing DNS server* check box, then click *Retrieve*. Ensure that the IP address being used to retrieve the contexts points to the desired Novell DNS server. This action populates the *DNS Service Locator*, *DNS Group*, and *DNS Root ServerInfo* context fields.
- 9c** If you are configuring Novell DNS server along with the DSfW domain being configured,
- ◆ Specify the context of the DNS service locator object (for example, `ou=novell.dc=example.dc=com`).
  - ◆ Specify the context of the DNS group object (for example, `ou=novell.dc=example.dc=com`).
  - ◆ Specify the context of the DNS Root ServerInfo object (for example, `ou=novell.dc=example.dc=com`).
- 9d** Specify the fully distinguished, typeful name of an eDirectory user. For example: `cn=dnsadmin,dc=example,dc=com` to authenticate to eDirectory during runtime for accessing information for DNS. The user must have eDirectory read, write, and browse rights under the specified context.
- 9e** Specify the password of the eDirectory user that you specified for accessing DNS.

**9f** *Use Secure LDAP Port* option is selected by default to ensure that the data transferred by this service is secure and private. If you deselect this option, the data transferred is in clear text format.

**9g** Click *Next* to continue.

---

**IMPORTANT:** Leave all the inputs as the default. Specify only the proxy user name and password. Specify the inputs in DNS format. The first set of inputs is separated by periods (.) and the proxy user name is separated by commas (,).

---

**10** Complete the remainder of the OES configuration and SLES 10 SP2 installation as instructed in “[Installing Open Enterprise Server 2 SP1 Linux](#)” in the *OES2 SP1: Linux Installation Guide*, taking note of the following guidelines:

- ♦ Be sure to specify a reliable Network Time Protocol (NTP) provider. Novell eDirectory requires that all servers in a tree be time synchronized.
- ♦ On the NMAS Methods selection page, you do not need to select *SASL GSSAPI*. The GSSAPI authentication mechanism that DSfW uses is installed automatically.
- ♦ Review the OES configuration summary to ensure that the settings have been made correctly according to your installation plan.

If necessary, click a heading in the summary page to modify an OES service’s configuration.

- ♦ The configuration of eDirectory and DSfW takes some time to complete. Please be patient.
- ♦ For the User Authentication Method, accept the default of `Local`.

**11** When the installation is complete, click *Finish*.

After the server is installed, see [Section 2.10, “Verifying the Installation,” on page 72](#) to verify that eDirectory and DSfW have been installed and configured correctly.

### 2.4.3 Installing a Name-Mapped Child Domain in an Existing DSfW Forest

This section explains how to install and configure a DSfW server to create a child domain in an eDirectory tree. In this scenario, you have already installed the first DSfW server/domain and you now want to install another server and create a child domain to the domain you previously created. The new server is automatically configured as a domain controller for the child domain.

- ♦ “[Prerequisites](#)” on page 40
- ♦ “[Installation Procedure](#)” on page 41

## Prerequisites

In addition to the prerequisites listed in [Section 2.1, “General Prerequisites,” on page 17](#), the following prerequisites apply to this installation scenario:

- ❑ The container you want to become the child domain must already exist in the eDirectory tree. The RDN of domain name being installed and the container name that is mapped from the existing tree must be same, or the installation cannot proceed.

For example, if the eDirectory container you are creating the DSfW domain in is `ou=eng.ou=example.o=novell`, the domain name you specify must be `eng.example.com`.

Because a `cn=users` container is created in the new domain, there can't be an existing `ou=users` container in the container where the domain is being inserted.

A DSfW domain can only be created in Organization (O), Organizational Unit (OU) and Domain Component (DC) containers. Installing a name-mapped domain to map Country and Locality containers is not supported. However, you can map O and OU under these containers.

---

**NOTE:** If you have extended the schema to define custom container types that you want to use with DSfW, the container object must be derived from `LoginProperties` and be able to contain the NCP Server object and various other objects created for the domain.

---

Refer to [Managing Objects \(http://www.novell.com/documentation/edir88/edir88/data/a2iikq.html\)](http://www.novell.com/documentation/edir88/edir88/data/a2iikq.html) in the *Novell eDirectory 8.8 Administration Guide* for instructions on how to create and modify eDirectory container objects.

- ❑ The eDirectory container must be partitioned before you can install the DSfW domain.  
Refer to [Managing Partitions and Replicas \(http://www.novell.com/documentation/edir88/edir88/data/a2iikq.html\)](http://www.novell.com/documentation/edir88/edir88/data/a2iikq.html) in the *Novell eDirectory 8.8 Administration Guide* for instructions on how to partition a container.
- ❑ After configuring an eDirectory partition as a DSfW domain, you can log in from a Windows desktop in the domain only if you had Universal Password enabled prior to configuring DSfW. Universal Password is required for creating DSfW credentials. For users who did not have Universal Password enabled, the DSfW credentials are created when they log in to eDirectory again.

---

**IMPORTANT:** Ensure that the nameserver listed in `/etc/resolv.conf` points to the DNS server already configured for the parent domain. The domain name of the local server must be the name of child domain you are configuring.

---

- ❑ The first component of the DNS Server name and the container name must be same. For example, a container `example.novell` can be mapped to any of the following domain names:
  - ♦ `example.company.com`
  - ♦ `example.division.company.com`
  - ♦ `example.company.countrycode`



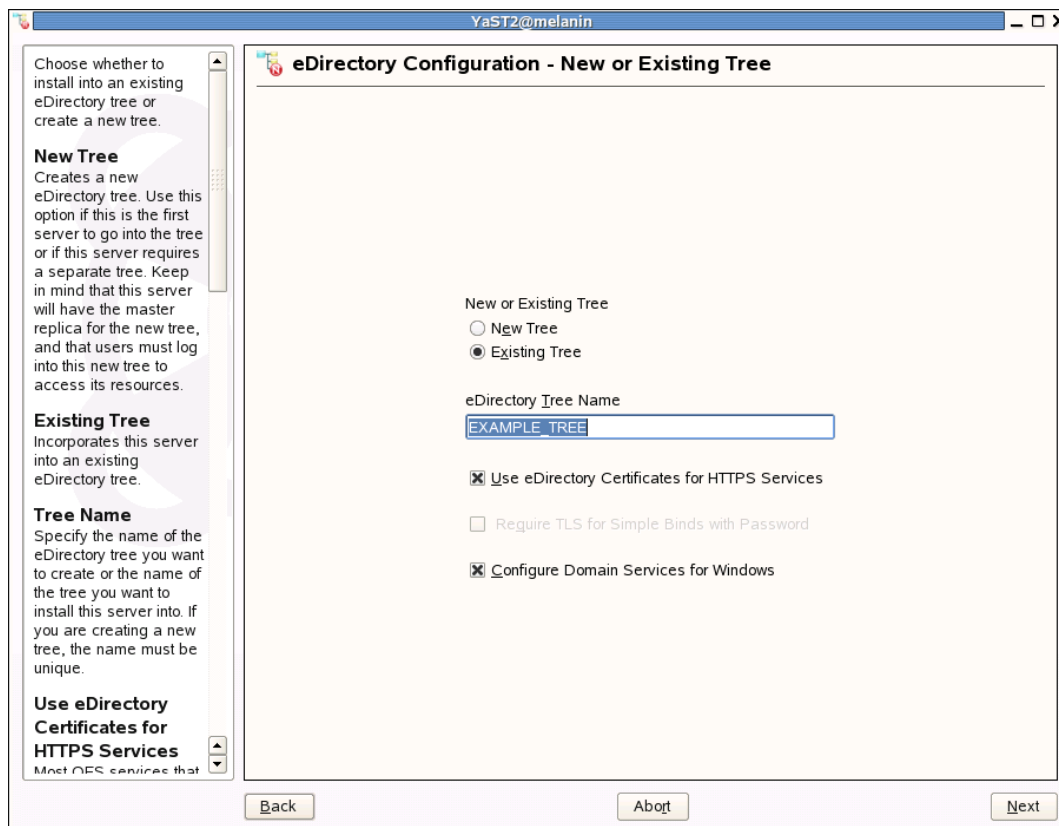
## Installation Procedure

The example configuration shown in this section builds upon the scenario described in [Section 2.4.2, “Installing the First DSfW Server in an Existing eDirectory Tree,” on page 29](#). It assumes that you are installing a second DSfW server into the same eDirectory tree with the following parameters:

- ♦ **Existing eDirectory Tree Name:** EXAMPLE\_TREE
- ♦ **eDirectory Container for New Domain:** ou=eng.ou=example.o=novell
- ♦ **Forest Root Domain:** example.com
- ♦ **Parent Domain:** example.com
- ♦ **Hostname (also used for server name):** dsfw2
- ♦ **Child Domain Name:** eng.example.com
- ♦ **Domain NetBIOS Name:** ENG
- ♦ **Primary IP Address of the DSfW Server:** 192.168.1.2
- ♦ **IP Address of the Parent Domain Server:** 192.168.1.1
- ♦ **Existing eDirectory Tree Admin Account:** cn=admin.o=novell
- ♦ **Existing DSfW Administrator Account:**  
cn=Administrator.cn=Users.dc=example.dc=com

As you follow the procedure below, substitute your own names and IP addresses for the ones used in the example configuration.

- 1 On the first eDirectory configuration page, specify that you are installing the server into an existing eDirectory tree:



- 1a Select *Existing Tree*.
- 1b Specify the name of the eDirectory tree (EXAMPLE\_TREE in the example configuration).
- 1c Select *Use eDirectory Certificates for HTTPS Services* if you want your OES services that provide HTTPS connectivity to use the more secure eDirectory certificates instead of the self-signed certificates created by YaST.  
Do not select this option if you have already installed certificates from a third-party certificate authority.
- 1d Select *Configure Domain Services for Windows*.
- 1e Click *Next* to continue.

## 2 Provide information about the existing eDirectory tree:

**IP Address of an Existing eDirectory Server with a Replica**  
Specify the IP address of an existing eDirectory server that is part of the eDirectory tree you are installing this server into.

**Enter NCP Port on the Existing Server**  
Specify the NCP port number of the existing server. The default NCP port for most eDirectory servers is 524.

**Enter LDAP Port on the Existing Server**  
Specify the LDAP port number of the existing eDirectory server specified in the prior field. The default LDAP port for most eDirectory servers is 389.

**Enter Secure LDAP Port on the Existing Server**  
Specify the secure LDAP port number of the existing eDirectory

**eDirectory Configuration - Existing Tree Information**

IP Address of an existing eDirectory server with a replica  
192.168.1.100

Enter NCP Port on the existing server  
524

Enter LDAP Port on the existing server  
389

Enter Secure LDAP Port on the existing server  
636

EDN Existing admin name with context (e.g. cn=admin,o=novell)  
cn=admin,o=novell

Admin Password  
\*\*\*\*\*

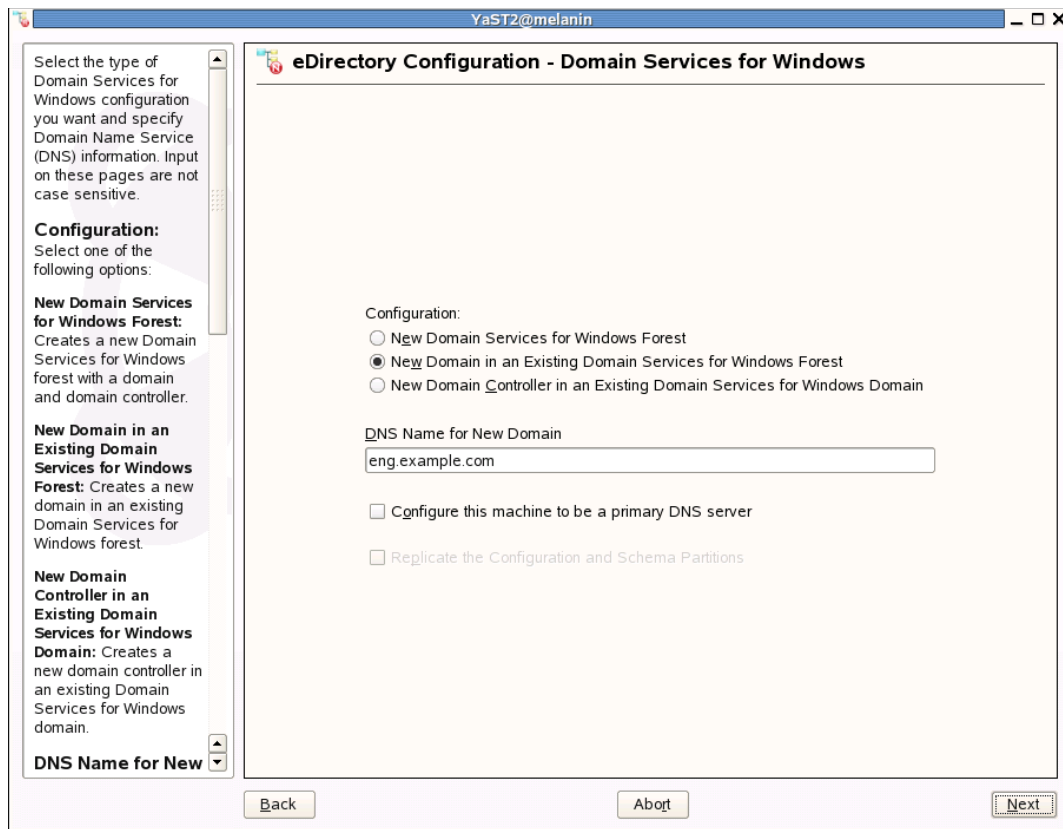
Back Abort Next

**2a** Leave the NCP™ and LDAP port parameters at the default settings unless you selected alternative ports when you installed the eDirectory tree. YaST specifies the location of the eDirectory administrator.

**2b** Enter the DSfW Administrator password.

**2c** Click *Next*.

### 3 Select settings for the DSfW configuration and DNS:



**3a** Select *New Domain in an Existing Domain Services for Windows Forest* as the type of configuration.

**3b** Specify the new domain name (eng.example.com in the example configuration).

To configure the DNS server, either use the existing DSfW DNS server or configure it by selecting the *Configure this machine to be a primary DNS server* check box. You cannot configure DNS after the server is installed. After installing DSfW, refer to [Section 2.8.1, “Restarting DNS,” on page 71](#) for more information on updating the new DNS records.

If you want to configure the child domain controller to act as a primary DNS server, ensure DNS servers of the forest root domain and the child domain controller act as passive primary DNS servers of each other's zones, else installation of an additional domain controller to the child domain fails.

---

**NOTE:** For an existing DNS server in your DSfW forest to act as a primary DNS server for the domain being installed, refer to section [Section 2.5, “Configuring DNS in a DSfW Environment,” on page 69](#).

---

**3c** Click *Next* to continue.

**4** Select the domain NetBIOS name setting and other DSfW settings unique to this scenario:

Specify the information required to create a context for this server in the new domain or as a new domain controller in a Domain Services for Windows forest.

**Domain NetBIOS Name**  
Specify a NetBIOS name for the Domain Services for Windows domain, or specify the NetBIOS name for the Domain Services for Windows domain you are installing this domain or controller into.

By default, this is the domain context name without the parent context. For example, in the domain cn=central,dc=example, the default NetBIOS name is central.

**Forest Root Domain**  
Specify the name of the forest root domain that you want to create this domain or domain controller in.

Domain NetBIOS Name  
eng

Forest Root Domain  
example.com

Parent Domain  
example.com

Trust Posix Offset (a value between 1 and 4294967294)  
122335671

Back Abort Next

**4a** Leave *Domain NetBIOS Name* at the default (ENG for the example configuration).

By default, the domain NetBIOS name is the domain context name without the parent context. This is the name that is displayed in the Windows login dialog box when you log in to the domain.

**4b** Specify the forest root domain and the parent domain.

**IMPORTANT:** The forest root domain is the first domain created in the forest when the first DSfW server was installed in the eDirectory tree. The parent domain is the immediate parent of the domain that you are configuring.

In this configuration example, the forest root domain and the parent domain are the same because you are creating a child domain to the first domain created in the eDirectory tree.

**4c** Set the Trust Posix Offset value.

**NOTE:** You can leave the field blank because the value is not considered.

**4d** Click *Next* to continue.

- 5 The Administrator's name is populated by default. Specify the Administrator password in both fields to verify that you are typing it correctly, then click *Next*.

YaST2@melanin

**eDirectory Configuration - Domain Services for Windows**

When creating a new domain, specify a password for the Domain Services for Windows Administrator account.

If creating a new domain controller, specify the existing password for an existing the Domain Services for Windows Administrator account to allow this controller access to the domain information.

**New or Existing Domain Administrator Name**

Note the name and context of the Administrator account. This is the Administrator you are entering the password for. You will use this account to log in to the Domain Services for Windows domain.

**Specify Administrator Password**

Specify a password for

New Domain Administrator Name  
cn=Administrator.cn=Users.dc=eng.dc=example.dc=com

Specify Administrator Password  
\*\*\*\*\*

Verify Administrator Password  
\*\*\*\*\*

Back Abort Next

**6** Provide information about the parent domain:

Specify the information needed to identify the parent domain for the new domain you are creating.

**IP Address of Parent Domain**  
Specify the IP address of the domain that will be the parent of the new domain you are creating.

**LDAP Secure Port for the Parent Domain Server**  
Note the secure port for accessing LDAP services on the parent domain.

**Parent Domain Administrator Name**  
Note the name and context for the parent domain administrator that you are creating this domain in.

**Admin Password**  
Specify the password for the Administrator account of the parent domain.

IP Address of the Parent Domain  
192.168.1.1

LDAP Secure Port for the Parent Domain Server  
536

Parent Domain Administrator Name  
cn=Administrator,cn=Users,dc=example,dc=com

Enter Administrator Password  
\*\*\*\*\*

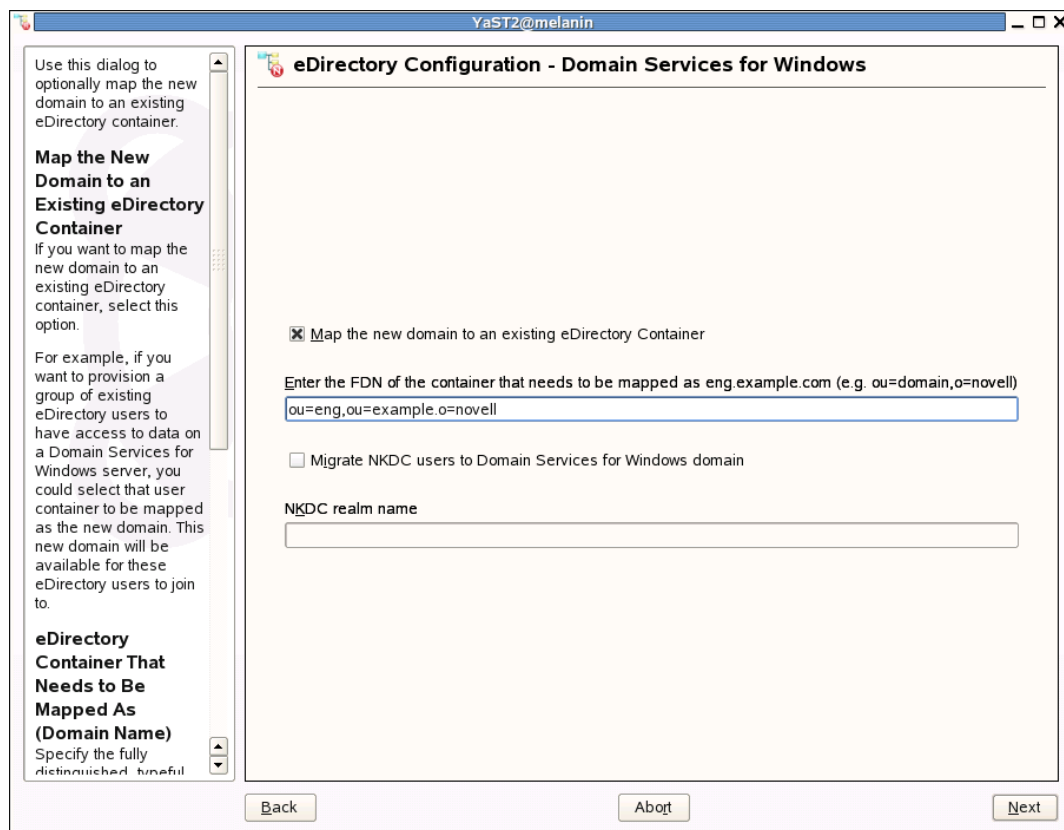
Back Abort Next

**6a** Specify the IP address of the DSfW server in the parent domain. In the example configuration, this is 192.168.1.1.

**6b** Specify the password for the parent domain's Administrator account.

**6c** Click *Next* to continue.

- 7** Select *Map the new domain to an existing eDirectory Container* to allow name-mapping to the new domain.



**NOTE:** Name mapping allows existing eDirectory users in the partition to access NSS file systems and other Novell resources without the need for the Novell Client software. You should enable this option if you plan to remove the Novell Client from the Windows workstations in the domain to simplify your user and desktop management.

- 7a** Specify the name of the eDirectory container that you are mapping the new domain to (ou=eng,ou=example,o=novell in the example configuration).
- 7b** Click *Next* to continue.



## 8 Specify settings for the local server configuration:

Specify the configuration for the local server in the eDirectory tree.

**Server Context**  
The parent context for the Domain Services for Windows domain is shown.

**Enter Directory Information Base (DIB) Location**  
Specify a location for the eDirectory database. The default path is /var/opt/novell/eDirectory/data/dib but you can use this option to change the location if you expect the number of objects in your tree to be large and if the current file system does not have sufficient space.

**LDAP and Secure LDAP Ports**  
The LDAP and secure LDAP port numbers this server will use to service LDAP requests are shown.

**Server Context**  
ou=novell,ou=eng,ou=example,o=novell

**Directory Information Base (DIB) Location**  
/var/opt/novell/eDirectory/data/dib

**Enter LDAP Port**  
389

**Enter Secure LDAP Port**  
636

**Enter iMonitor Port**  
8028

**Enter Secure iMonitor Port**  
8030

Back Abort Next

The *Server Context* field displays the context of the NCP Server object being added as a part of the DSfW installation. It cannot be modified.

- 8a** Leave the location of the Directory Information Base (DIB) at the default setting. This should suffice for most eDirectory servers.
- 8b** Leave the iMonitor port settings at the defaults unless you need to change them to avoid port conflicts with other services.
- 8c** Click *Next* to continue.

## 9 Specify the Novell DNS server information:

**Get Context Information from Existing DNS Server**  
If you are configuring DNS in an existing tree where DNS is already configured and you want to use the existing Locator and Group object contexts, you can select the 'Get context information from existing DNS server' check box and provide the IP of an NCP server hosting the existing DNS server and click 'Retrieve'. This will fetch the contexts of the Locator and Group contexts. Make sure the NCP server hosting the existing DNS server is running before hitting 'Retrieve'.

If you do not wish to use existing contexts, you can provide those manually.

**Novell DNS Services Locator Object Context**  
Specify the context for the DNS Locator object.  
For example: o=novell

The Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree.

**Novell DNS Services Group Object Context**  
Specify the context for the DNS Group object.  
For example: o=novell

This object is used to grant DNS servers the necessary rights to other data within the eDirectory tree.

**Novell DNS Services Configuration**

Common DNS Configuration Objects Context

☒ Get context information from existing DNS server

Existing Novell DNS server address:  
192.168.1.100

Retrieve

Novell DNS Services Locator Object Context (e.g. o=novell):

Novell DNS Services Group Object Context (e.g. o=novell):

Back Abort Next

- 9a** The *Existing Novell DNS server address* field is pre-populated with the first name server entry from the `/etc/resolv.conf` file.
- 9b** The option of using this IP address and fetching the context of Novell DNS specific objects is disabled by default. To enable it, select the *Get context and proxy user information from existing DNS server* check box, then click *Retrieve*. Ensure that a Novell-DNS server that you want to use for DSfW domain being installed belongs to the IP address specified in the *Existing Novell DNS server address* field.
- 9c** Specify the context of the existing DNS service locator object. (for example, `ou=novell.dc=example.dc=com`). This is the context where the DNS service locator object is located.
- 9d** Specify the context of the DNS group object where the DNS group object is located.
- 9e** Click *Next* to continue.

---

**IMPORTANT:** Leave all the inputs as the default. Specify the inputs in DNS format. The first set of inputs is separated by periods (.).

---

- 10** Complete the remainder of the OES configuration and SLES 10 SP2 installation as instructed in “**Installing Open Enterprise Server 2 SP1 Linux**” in the *OES2 SP1: Linux Installation Guide*, taking note of the following guidelines:
  - ♦ Be sure to specify a reliable Network Time Protocol (NTP) provider. Novell eDirectory requires that all servers in a tree be time synchronized.

- ♦ It is not necessary to set up Service Location Protocol (SLP) if you have fewer than three servers on your network.

If you need to set up SLP, see [Configuring OpenSLP for eDirectory](http://www.novell.com/documentation/edir88/edir88/data/aksbdp5.html) (<http://www.novell.com/documentation/edir88/edir88/data/aksbdp5.html>) in the *Novell eDirectory 8.8 Administration Guide* for more information.

- ♦ On the NMASS Methods selection page, you do not need to select *SASL GSSAPI*. The GSSAPI authentication mechanism that DSfW uses is installed automatically.
- ♦ Review the OES configuration summary to ensure that the settings have been made correctly according to your installation plan.

If necessary, click a heading in the summary page to modify an OES service's configuration.

- ♦ The configuration of eDirectory and DSfW takes some time to complete. Please be patient.
- ♦ For the User Authentication Method, accept the default of *Local*.

**11** When the installation is complete, click *Finish*.

**12** Continue with [Section 2.8, "Post-Install Operations," on page 71](#) to restart the DNS after you have installed the child domain.

## 2.4.4 Configuring a Non-Name-Mapped Child Domain in an Existing DSfW Forest

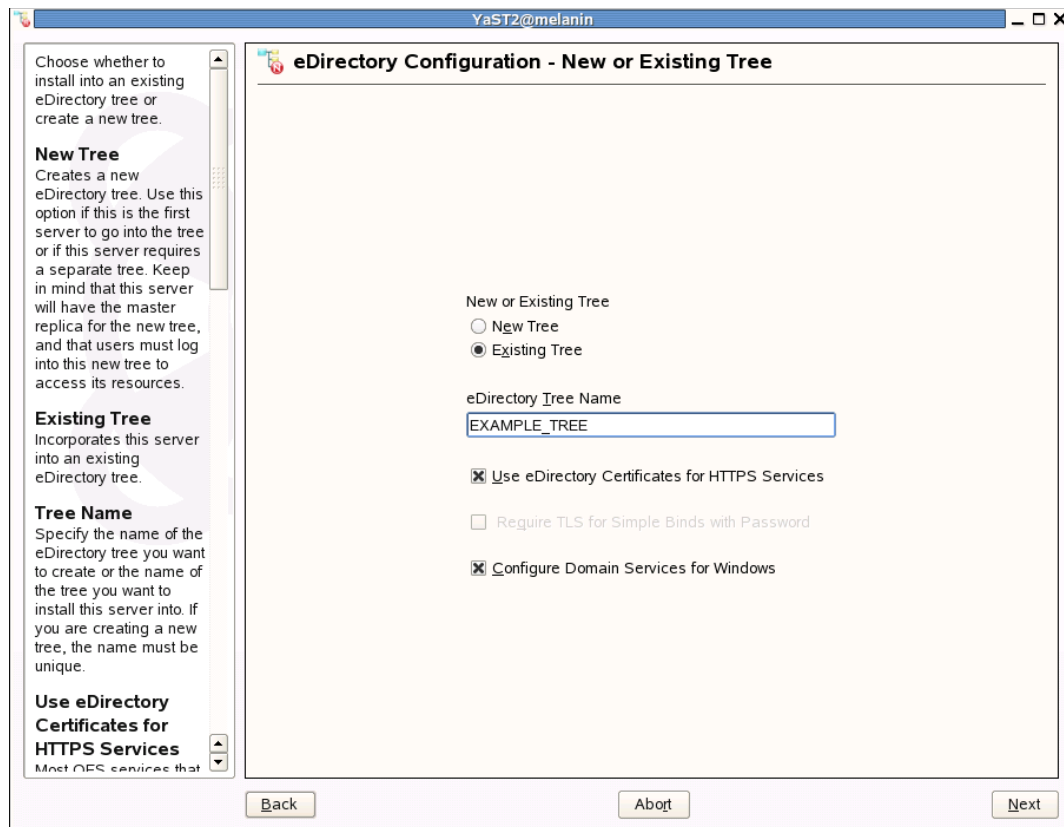
This section explains how to configure a DSfW server as a non-name-mapped child domain in an existing tree.

---

**IMPORTANT:** Ensure that your nameserver in `/etc/resolv.conf` points to the DNS server already configured. The domain name of the local server must be the name of child domain you are configuring.

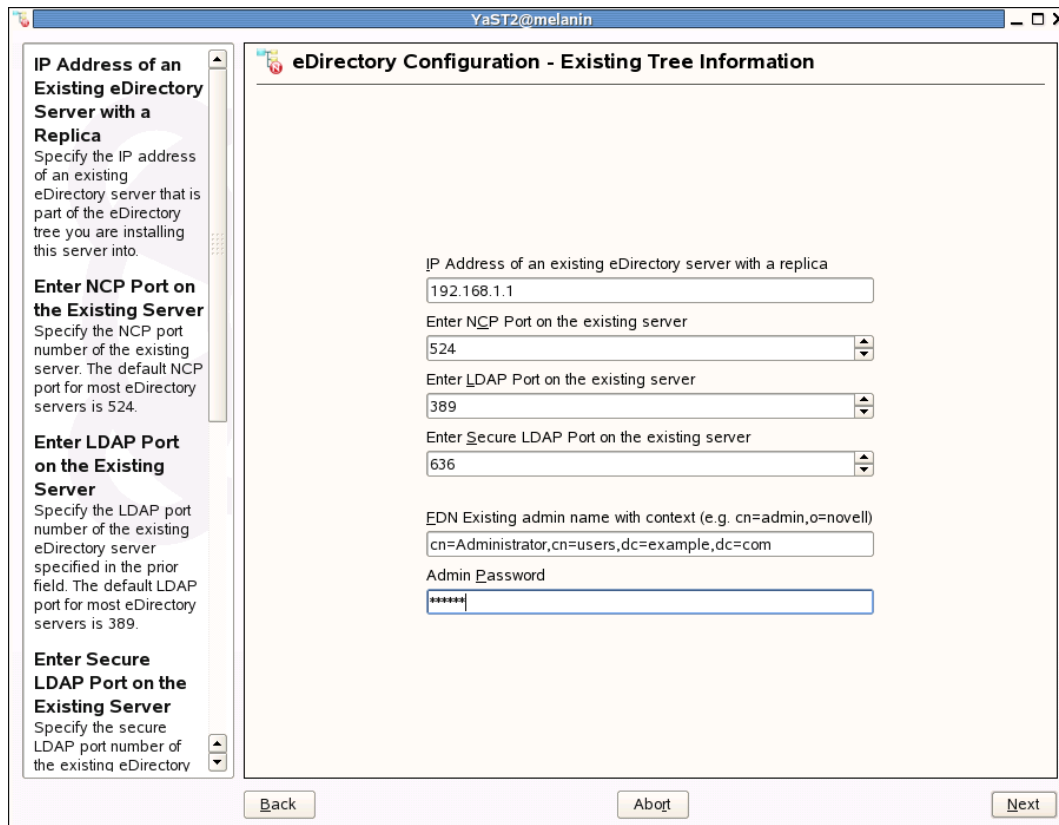
---

- 1 Select the existing tree option and ensure that the check box for *Configuring Domain Services for Windows* is selected.



- 2 Specify the IP address of an existing eDirectory server with a replica, then specify the IP address of the primary domain controller of the domain.
- 3 For the existing admin name and password, specify the fully distinguished name and password of a tree administrator who has rights to [Root].

- 4 Leave the other settings at the defaults unless you used different settings when you installed the existing tree. Click *Next* to continue.



The image shows a Windows-style window titled "eDirectory Configuration - Existing Tree Information". On the left is a sidebar with four sections: "IP Address of an Existing eDirectory Server with a Replica", "Enter NCP Port on the Existing Server", "Enter LDAP Port on the Existing Server", and "Enter Secure LDAP Port on the Existing Server". Each section contains a brief instruction. The main area of the window contains several input fields: "IP Address of an existing eDirectory server with a replica" (text box with "192.168.1.1"), "Enter NCP Port on the existing server" (spin box with "524"), "Enter LDAP Port on the existing server" (spin box with "389"), "Enter Secure LDAP Port on the existing server" (spin box with "636"), "EDN Existing admin name with context (e.g. cn=admin,o=novell)" (text box with "cn=Administrator,cn=users,dc=example,dc=com"), and "Admin Password" (password box with "\*\*\*\*\*"). At the bottom are "Back", "Abort", and "Next" buttons.

**IP Address of an Existing eDirectory Server with a Replica**  
Specify the IP address of an existing eDirectory server that is part of the eDirectory tree you are installing this server into.

**Enter NCP Port on the Existing Server**  
Specify the NCP port number of the existing server. The default NCP port for most eDirectory servers is 524.

**Enter LDAP Port on the Existing Server**  
Specify the LDAP port number of the existing eDirectory server specified in the prior field. The default LDAP port for most eDirectory servers is 389.

**Enter Secure LDAP Port on the Existing Server**  
Specify the secure LDAP port number of the existing eDirectory

IP Address of an existing eDirectory server with a replica  
192.168.1.1

Enter NCP Port on the existing server  
524

Enter LDAP Port on the existing server  
389

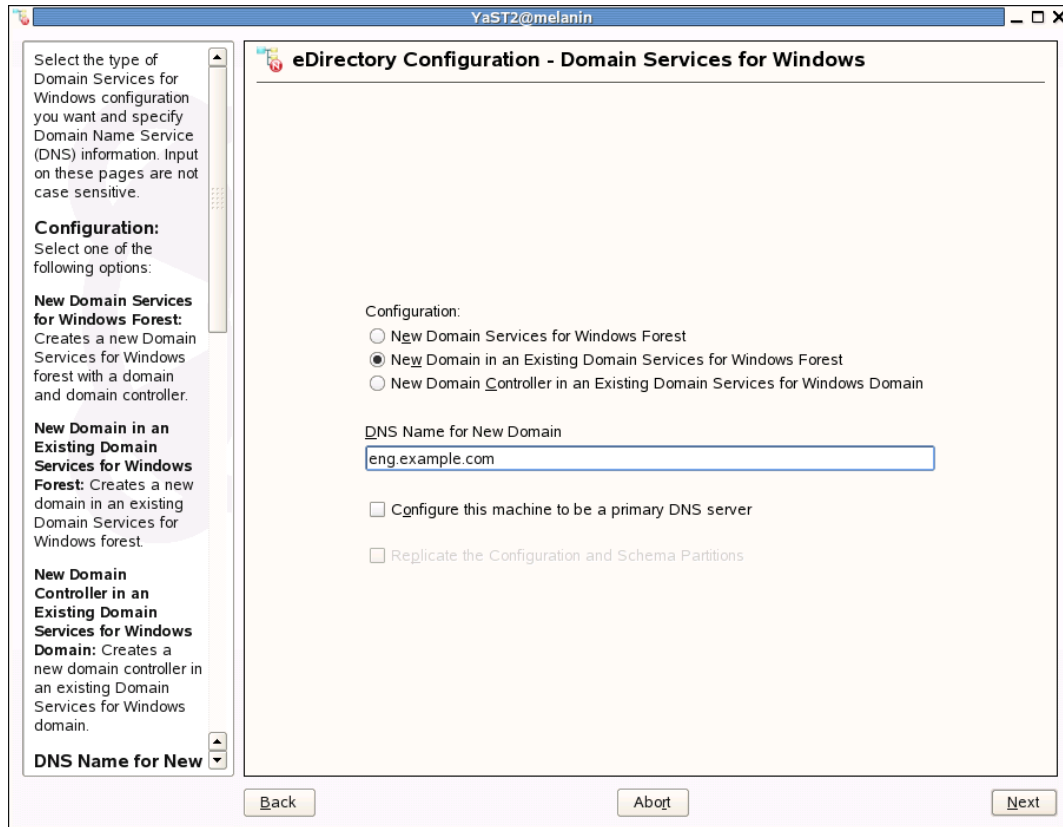
Enter Secure LDAP Port on the existing server  
636

EDN Existing admin name with context (e.g. cn=admin,o=novell)  
cn=Administrator,cn=users,dc=example,dc=com

Admin Password  
\*\*\*\*\*

Back Abort Next

- 5 Select *New Domain in an Existing Domain Services for Windows Forest* and type the new domain name.



- 5a If you want to configure DNS, select the *Configure this machine to be a primary DNS server* option. This option is deselected by default.

If you want to configure the child domain controller to act as a primary DNS server, ensure DNS servers of the forest root domain and the child domain controller act as passive primary DNS servers of each other's zones, else installation of an additional domain controller to the child domain controller fails.

**IMPORTANT:** The forest root domain should be the first domain server in the forest. The parent domain is the immediate parent of the domain that you are configuring.

- 5b Click *Next* to continue.

6 Specify the NetBIOS name for the new DSfW domain, forest root domain and parent domain.

Specify the information required to create a context for this server in the new domain or as a new domain controller in a Domain Services for Windows forest.

**Domain NetBIOS Name**  
Specify a NetBIOS name for the Domain Services for Windows domain, or specify the NetBIOS name for the Domain Services for Windows domain you are installing this domain or controller into.

By default, this is the domain context name without the parent context. For example, in the domain cn=central,dc=example, the default NetBIOS name is central.

**Forest Root Domain**  
Specify the name of the forest root domain that you want to create this domain or domain controller in.

Domain NetBIOS Name  
eng

Forest Root Domain  
example.com

Parent Domain  
example.com

Trust Posix Offset (a value between 1 and 4294967294)  
122335671

Back Abort Next

6a You can enter any value in the Trust Posix Offset field because the value is not considered.

6b Click *Next* to continue.

7 Specify the Administrator password twice, then click *Next*.

YaST2@melanin

**eDirectory Configuration - Domain Services for Windows**

When creating a new domain, specify a password for the Domain Services for Windows Administrator account.

If creating a new domain controller, specify the existing password for an existing the Domain Services for Windows Administrator account to allow this controller access to the domain information.

**New or Existing Domain Administrator Name**

Note the name and context of the Administrator account. This is the Administrator you are entering the password for. You will use this account to log in to the Domain Services for Windows domain.

**Specify Administrator Password**

Specify a password for

New Domain Administrator Name  
cn=Administrator.cn=Users.dc=eng.dc=example.dc=com

Specify Administrator Password  
\*\*\*\*\*

Verify Administrator Password  
\*\*\*\*\*

Back Abort Next



8 Specify the parent domain administrator name and password, then click *Next*.

Specify the information needed to identify the parent domain for the new domain you are creating.

**IP Address of Parent Domain**  
Specify the IP address of the domain that will be the parent of the new domain you are creating.

**LDAP Secure Port for the Parent Domain Server**  
Note the secure port for accessing LDAP services on the parent domain.

**Parent Domain Administrator Name**  
Note the name and context for the parent domain administrator that you are creating this domain in.

**Admin Password**  
Specify the password for the Administrator account of the parent domain.

eDirectory Configuration - Domain Services for Windows

IP Address of the Parent Domain  
192.168.1.1

LDAP Secure Port for the Parent Domain Server  
636

Parent Domain Administrator Name  
cn=Administrator, cn=Users, dc=example, dc=com

Enter Administrator Password  
\*\*\*\*\*

Back Abort Next

## 9 Specify settings for the local server configuration:

Specify the configuration for the local server in the eDirectory tree.

**Server Context**  
The parent context for the Domain Services for Windows domain is shown.

**Enter Directory Information Base (DIB) Location**  
Specify a location for the eDirectory database. The default path is /var/opt/novell/eDirectory/data/dib but you can use this option to change the location if you expect the number of objects in your tree to be large and if the current file system does not have sufficient space.

**LDAP and Secure LDAP Ports**  
The LDAP and secure LDAP port numbers this server will use to service LDAP requests are shown.

**Enter iMonitor Port**

**eDirectory Configuration - Local Server Configuration**

Server Context  
cn=users,dc=eng,dc=example,dc=com

Directory Information Base (DIB) Location  
/var/opt/novell/eDirectory/data/dib

Enter LDAP Port  
389

Enter Secure LDAP Port  
636

Enter iMonitor Port  
8028

Enter Secure iMonitor Port  
8030

Back About Next

The *Server Context* field displays the context of the NCP Server object being added as a part of DSfW installation. It cannot be modified.

- 9a** Leave the location of the Directory Information Base (DIB) at the default setting. This should suffice for most eDirectory servers.
- 9b** Leave the iMonitor port settings at the defaults unless you need to change them to avoid port conflicts with other services.
- 9c** Click *Next* to continue.

## 10 Specify the Novell DNS server information:

**Get Context Information from Existing DNS Server**  
If you are configuring DNS in an existing tree where DNS is already configured and you want to use the existing Locator and Group object contexts, you can select the 'Get context information from existing DNS server' check box and provide the IP of an NCP server hosting the existing DNS server and click 'Retrieve'. This will fetch the contexts of the Locator and Group contexts. Make sure the NCP server hosting the existing DNS server is running before hitting 'Retrieve'.

If you do not wish to use existing contexts, you can provide those manually.

**Novell DNS Services Locator Object Context**  
Specify the context for the DNS Locator object. For example: o=novell

The Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree.

**Novell DNS Services Group Object Context**  
Specify the context for the DNS Group object. For example: o=novell

This object is used to grant DNS servers the necessary rights to other data within the eDirectory tree.

**Novell DNS Services Configuration**

Common DNS Configuration Objects Context

☒ Get context information from existing DNS server

Existing Novell DNS server address:  
192.168.1.100

Retrieve

Novell DNS Services Locator Object Context (e.g. o=novell):

Novell DNS Services Group Object Context (e.g. o=novell):

Back Abort Next

**10a** The *Existing Novell DNS server address* field is pre-populated with the first name server entry from the `/etc/resolv.conf` file.

**10b** The option of using this IP address and fetching the context of Novell DNS specific objects is disabled by default. To enable it, select the *Get context and proxy user information from existing DNS server* check box, then click *Retrieve*. Ensure that a Novell-DNS server that you want to use for DSfW domain being installed belongs to the IP address specified in the *Existing Novell DNS server address* field.

**10c** Specify the context of the existing DNS service locator object. (for example, `ou=novell.dc=example.dc=com`). This is the context where the DNS service locator object is located.

**10d** Specify the context of the DNS group object where the DNS group object is located.

**10e** Click *Next* to continue.

---

**IMPORTANT:** Leave all the inputs as the default. Specify only the proxy user name and password. Specify the inputs in DNS format. The first set of inputs is separated by periods (.).

---

**11** Complete the remainder of the OES configuration and SLES 10 installation as instructed in the *OES 2: Linux Installation Guide*, taking note of the following guidelines:

- ♦ Accept the defaults on the CA Management page.

- ♦ Be sure to specify a reliable Network Time Protocol (NTP) provider. Novell eDirectory requires that all servers in a tree be time synchronized. In a single-server scenario, you can specify the local machine as the NTP provider.
- ♦ It is not necessary to set up Service Location Protocol (SLP) if you have fewer than three servers on your network.
- ♦ In the NMAS Methods selection page, you do not need to select SASL GSSAPI. The GSSAPI authentication mechanism that DSfW uses is installed automatically.
- ♦ For the User Authentication Method, accept the default of Local.

**12** When the installation is complete, click *Finish* and wait for the server to reboot.

Continue with [Section 2.8, “Post-Install Operations,” on page 71](#) to configure DNS after you have installed the additional domain.

## 2.4.5 Configuring an Additional Domain Controller in a Domain

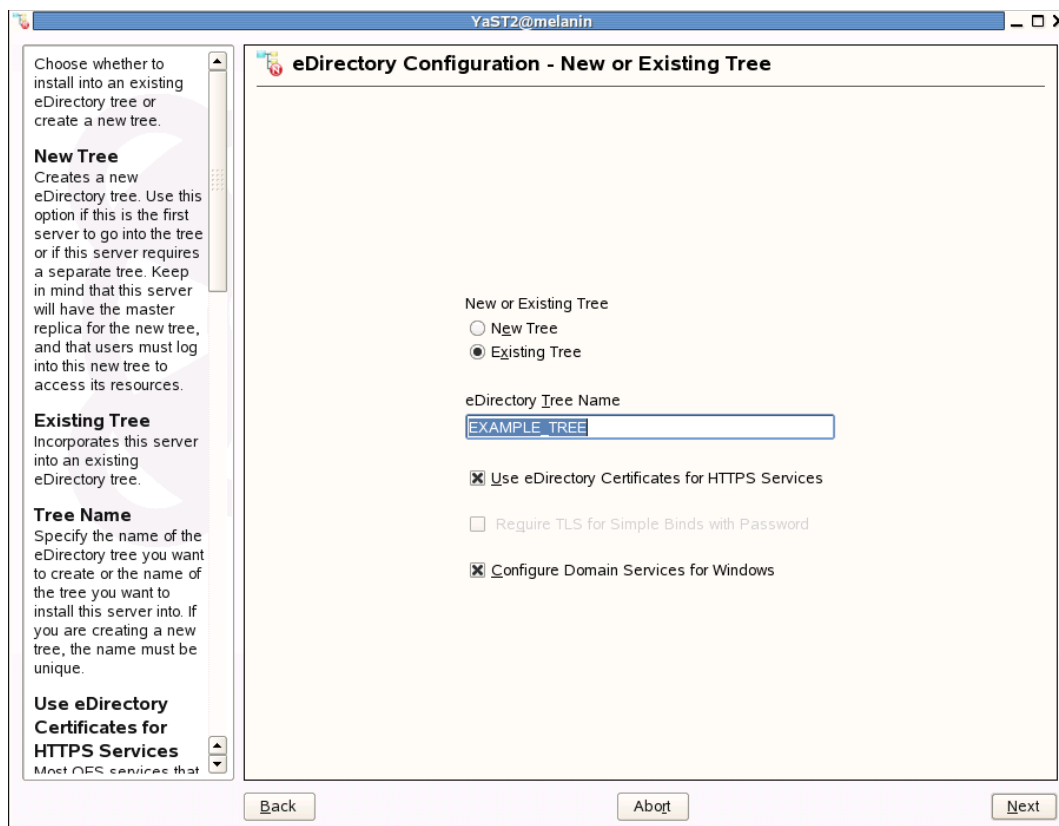
This section explains how to install and configure a DSfW server as an additional domain controller (ADC) in an existing domain. In this scenario you are installing an additional domain controller in a forest root domain that was configured in the [Section 2.4.1, “Installing the First DSfW Server in a New eDirectory Tree,” on page 22](#). The steps are similar for creating a child domain.

The example configuration shown in this section builds upon the scenario described in [Section 2.4.1, “Installing the First DSfW Server in a New eDirectory Tree,” on page 22](#). It assumes that you are installing an additional domain controller into the same eDirectory tree with the following parameters:

- ♦ **Existing eDirectory Tree Name:** EXAMPLE\_TREE
- ♦ **DNS name for the new Domain:** example.com
- ♦ **Forest Root Domain:** example.com
- ♦ **Existing Domain Administrator Name:**  
`cn=Administrator.cn=Users.dc=example.dc=com`
- ♦ **Hostname (also used for server name):** oesadc
- ♦ **Domain NetBIOS Name:** EXAMPLE-ADC
- ♦ **Primary IP Address of the DSfW Server:** 192.168.1.2
- ♦ **IP Address of the Parent Domain Server:** 192.168.1.1

As you follow the procedure below, substitute your own names and IP addresses for the ones used in the example configuration.

- 1 On the first eDirectory configuration page, select *Existing Tree* and specify a name for the tree (EXAMPLE\_TREE in the example configuration). Ensure that the check box for configuring DSfW is selected.



- 1a Select *Use eDirectory certificates for HTTPS services* if you want your OES services that provide HTTPS connectivity to use the more secure eDirectory certificates instead of the self-signed certificates created by YaST.
  - 1b Make sure *Configure Domain Services for Windows* is selected. It is not possible to configure DSfW later, as you can with other OES services. It must be configured now, along with eDirectory.
  - 1c Click *Next* to continue.
- 2 Specify the IP address of the primary domain controller of the domain.

While installing an additional domain controller in a domain, YaST prompts you to specify the IP address of the eDirectory server holding the replica. If you specify the IP address of a plain eDirectory server valid in name-mapped installation scenarios, YaST tries to authenticate to the existing eDirectory server with the forest root domain admin credentials. Because the admin fully distinguished name is specified in the DC format, a plain eDirectory server cannot map it

with the actual object. However, you can configure it after specifying the IP address of a DSfW server in the forest (preferably the first domain controller of the domain to which you are adding an additional domain controller) as the IP address of the existing eDirectory server.

**IP Address of an Existing eDirectory Server with a Replica**  
Specify the IP address of an existing eDirectory server that is part of the eDirectory tree you are installing this server into.

**Enter NCP Port on the Existing Server**  
Specify the NCP port number of the existing server. The default NCP port for most eDirectory servers is 524.

**Enter LDAP Port on the Existing Server**  
Specify the LDAP port number of the existing eDirectory server specified in the prior field. The default LDAP port for most eDirectory servers is 389.

**Enter Secure LDAP Port on the Existing Server**  
Specify the secure LDAP port number of the existing eDirectory

**eDirectory Configuration - Existing Tree Information**

IP Address of an existing eDirectory server with a replica  
192.168.1.1

Enter NCP Port on the existing server  
524

Enter LDAP Port on the existing server  
389

Enter Secure LDAP Port on the existing server  
636

EDN Existing admin name with context (e.g. cn=admin,o=novell)  
cn=Administrator,cn=users,dc=example,dc=com

Admin Password  
\*\*\*\*\*

Back Abort Next

- 2a** For the existing admin name and password, specify the fully distinguished name and password of a tree administrator who has rights to [Root].

---

**NOTE:** Enter the tree administrator or container administrator if the install is based on container admin rights. Refer to the [Section 2.4.6, “Using a Container Admin to Install and Configure DSfW,” on page 67](#) for more information on container admin rights.

---

- 2b** Leave the other settings at the defaults unless you used different settings when you installed the existing tree.

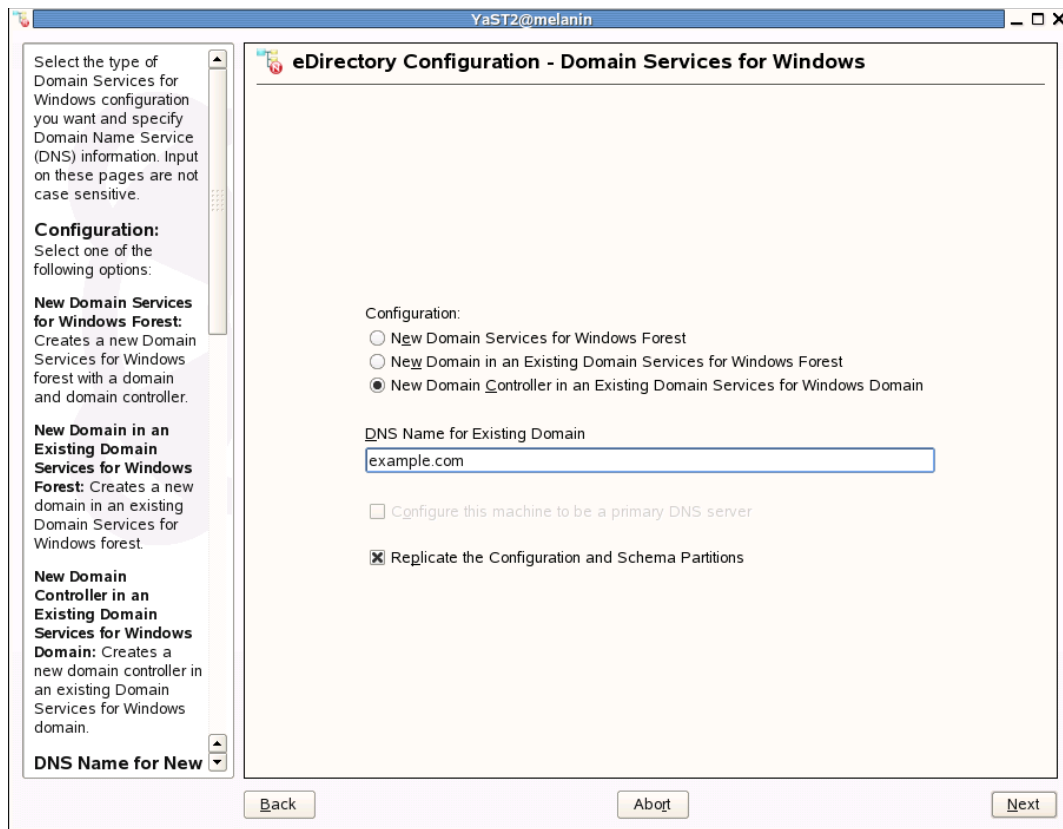
- 2c** Click *Next* to continue.

---

**NOTE:** When a child domain controller is configured as an primary DNS server and if you are adding an additional domain controller to it, make sure that the DNS server of the forest root domain and the child domain controller act as passive primary DNS servers of each other's zones.

---

### 3 Select settings for the DSfW configuration and DNS.



- 3a** Ensure that the *New Domain Controller in an Existing Domain Services for Windows Domain* option is selected.
- 3b** YaST displays a DNS name for the new domain, based on the domain name you configured earlier (example.com in the example configuration). Leave this setting as it is.
- 3c** Ensure that the *Replicate the Configuration and Schema Partitions* option is selected to improve the response time and performance of the server.
- 3d** Click *Next* to continue.

- 4 Specify the forest root domain. The forest root domain is the domain name if the server is being added as an additional domain controller in the forest root. If this domain controller is added in a child domain, *Forest Root Domain* should reflect the name of the first domain in the forest. Click *Next* to continue.

Specify the information required to create a context for this server in the new domain or as a new domain controller in a Domain Services for Windows forest.

**Forest Root Domain**  
Specify the name of the forest root domain that you want to create this domain or domain controller in.

The forest root domain is the first domain in the first tree of the Domain Services for Windows forest. The forest root has no parent, and it provides the LDAP entry point to Domain Services for Windows.

Forest Root Domain

Back Abort Next



- 5 Specify the password for the domain administrator. The default administrator for the example domain is `cn=Administrator,cn=Users,dc=example,dc=com`. Click *Next* to continue.

YaST2@melanin

**eDirectory Configuration - Domain Services for Windows**

When creating a new domain, specify a password for the Domain Services for Windows Administrator account.

If creating a new domain controller, specify the existing password for an existing the Domain Services for Windows Administrator account to allow this controller access to the domain information.

**New or Existing Domain Administrator Name**

Note the name and context of the Administrator account. This is the Administrator you are entering the password for. You will use this account to log in to the Domain Services for Windows domain.

**Specify Administrator Password**

Specify a password for

Existing domain administrator name

Specify Administrator Password

Back Abort Next

- 6 Specify the Novell DNS server information. The *Existing Novell DNS server address* field is pre-populated with the first name server entry from the `/etc/resolv.conf` file.

**Get Context Information from Existing DNS Server**  
If you are configuring DNS in an existing tree where DNS is already configured and you want to use the existing Locator and Group object contexts, you can select the 'Get context information from existing DNS server' check box and provide the IP of an NCP server hosting the existing DNS server and click 'Retrieve'. This will fetch the contexts of the Locator and Group contexts. Make sure the NCP server hosting the existing DNS server is running before hitting 'Retrieve'.  
  
If you do not wish to use existing contexts, you can provide those manually.

**Novell DNS Services Locator Object Context**  
Specify the context for the DNS Locator object.  
For example: o=novell  
  
The Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree.

**Novell DNS Services Group Object Context**  
Specify the context for the DNS Group object.  
For example: o=novell  
  
This object is used to grant DNS servers the necessary rights to other data within the eDirectory tree.

**Novell DNS Services Configuration**  
**Common DNS Configuration Objects Context**  
☒ Get context information from existing DNS server  
Existing Novell DNS server address:  
192.168.1.1  
Retrieve  
Novell DNS Services Locator Object Context (e.g. o=novell):  
Novell DNS Services Group Object Context (e.g. o=novell):  
Back Abort Next

- 6a** The option of using this IP address and fetching the context of Novell DNS specific objects is disabled by default. To enable it, select the *Get context and proxy user information from existing DNS server* check box, then click *Retrieve*. Ensure that a Novell-DNS server that you want to use for DSfW domain being installed belongs to the IP address specified in the *Existing Novell DNS server address* field.
- 6b** Specify the context of the existing DNS service locator object. (for example, `ou=novell.dc=example.dc=com`). This is the context where the DNS service locator object is located.
- 6c** Specify the context of the DNS group object where the DNS group object is located.
- 6d** Click *Next* to continue.
- 7** Complete the remainder of the OES configuration and SLES 10 installation as instructed in the *OES 2: Linux Installation Guide*, taking note of the following guidelines:
- ♦ Accept the defaults on the CA Management page.
  - ♦ Be sure to specify a reliable Network Time Protocol (NTP) provider. Novell eDirectory requires that all servers in a tree be time synchronized. In a single-server scenario, you can specify the local machine as the NTP provider.
  - ♦ It is not necessary to set up Service Location Protocol (SLP) if you have fewer than three servers on your network.

- ♦ On the NMASS Methods selection page, you do not need to select SASL GSSAPI. The GSSAPI authentication mechanism that DSfW uses is installed automatically.
- ♦ For the User Authentication Method, accept the default of Local.

8 When the installation is complete, click *Finish*.

Continue with [Section 2.8, “Post-Install Operations,” on page 71](#) to configure DNS after you have installed the additional domain.

---

**IMPORTANT:** After configuring a DSfW domain, certain operations such as search and modify might not work as intended if you rename the domain controllers of that domain. For a proper functioning of these operations, you should not rename them.

---

## 2.4.6 Using a Container Admin to Install and Configure DSfW

For this procedure, assume that you want to configure DSfW in an existing tree with `o=novell,ou=india.o=novell` and `ou=blr.ou=india.o=novell` as root partitions.

The replica looks like:

```
o=novell cn=srv1.o=novell (M) , cn=srv2,ou=india,o=novell (RW) ou=india.o=novell
cn=srv2,ou=india,o=novell (M) ou=blr.ou=india.o=novell
cn=srv3.ou=blr.ou=india.o=novell (M)
```

To install DSfW in partition `ou=india,o=novell`, it must be mapped to `dc=india,dc=novell,dc=com`. You must have at least one eDirectory 8.8 SP4 server in the tree that holds a writable replica of the root partition. The root partition should be present on the server which is holding the name-mapped container. This is required for creating partitions and moving replicas around during DSfW configuration.

To configure a container admin:

- 1 Create a container in an already existing tree.  
eg: `ou=india.o=novell`
- 2 Install or configure a server under this container.  
eg: `cn=SRV2.ou=india.o=novell`
- 3 Create a user `cn=localadmin` under the container eg: `ou=india.o=novell`, and provide the following rights for the container admin:
  - ♦ The container must be partitioned (before or after installing the server) by using the admin for the tree.
  - ♦ A replica of the partition must exist on `cn=SRV2.ou=india.o=novell` only.  
The container admin does not have complete rights on the partition. If this replica exists on other servers, the admin can add a replica, but cannot remove it from other servers.
- 4 Assign the following rights to the container admin:
  - ♦ Supervisor rights on this partition.
  - ♦ Supervisor rights (inherited) for the entry rights to the security container.
  - ♦ Supervisor rights over the DNS locator and DNS group object.
  - ♦ Supervisor rights over the DNS server object if the DNS server is located in other domain.

- ♦ Supervisor rights (inheritable) on the `ou=novell` container holding the NCP Server object of the forest root domain, while installing an additional domain or an additional domain controller as a container admin.

For example, `ou=novell,dc=parent,dc=com` where `dc=parent,dc=com` is the forest root domain.

The container admin needs supervisor rights on the configuration partition to create an additional domain or an additional domain controller.

For more information on installing a secondary server into an existing tree as a nonadministrator user, refer to the *eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edir88/index.html?page=/documentation/edir88/edir88/data/a7ivcnh.html>).

## 5 Use the tree admin to extend the schema for DSfW:

**5a** On an existing OES 2 Linux server, run the Novell Schema tool found in *YaST > Open Enterprise Server > Novell Schema Tool* and enter the IP address of the eDirectory 8.8 SP4 server with a writable replica of the root.

**5b** Specify the tree admin's password and click *Next*.

**5c** Select Novell Linux User Management (lum), Novell DNS, Novell DSfW, and Novell NMAS.

It is not necessary to select any of the other items in the list. Wait for the schema changes to be synchronized across the tree before proceeding with the installation of the first DSfW server.

---

**NOTE:** You can use OES schema tool or iManager to extend the schema.

---

## 6 Configure Novell DSfW using YaST with the container admin credentials.

For information on installing and configuring Novell® DNS service, refer to “**Planning Your DNS/DHCP Implementation**” in the *OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux*

## 2.4.7 Migrating NKDC Users to a DSfW Domain

NKDC users are migrated to a DSfW domain by using the `migrate_nkdc_realm` migration tool. This migration offers them a DSfW domain identity, but they can continue using the NKDC identity.

**Migrating the NKDC Principals:** Standalone (Service) Principals are not migrated.

User Principals existing in the eDirectory user object or linked to an eDirectory user object (alias) are migrated. If an eDirectory user has multiple NKDC identities, the NKDC identity of that user object takes the precedence. If it is absent, but has single or multiple linked NKDC identities, the first entry from the alphabetically sorted list is considered.

**Migrating the NKDC Password and Ticket Policies:** Only the NKDC ticket policies are migrated to a DSfW domain. Only the NKDC realm object's ticket policies are migrated to the DSfW Default Domain Policy object. The migrated ticket policies apply to both the migrated users from the NKDC realm and the DSfW domain users.

**Migrating the NKDC Principal Kerberos Keys:** NKDC Principal Kerberos keys are not migrated.

If Universal Password is already enabled on the NKDC realm, it continues to be the password for NKDC identities because DSfW also uses it for generating the Kerberos keys.

If Universal Password is not enabled on the NKDC realm, the existing NKDCP Kerberos keys are not usable. Because NKDC Principals are implicitly associated with the Universal Password, they must use that password after the migration.

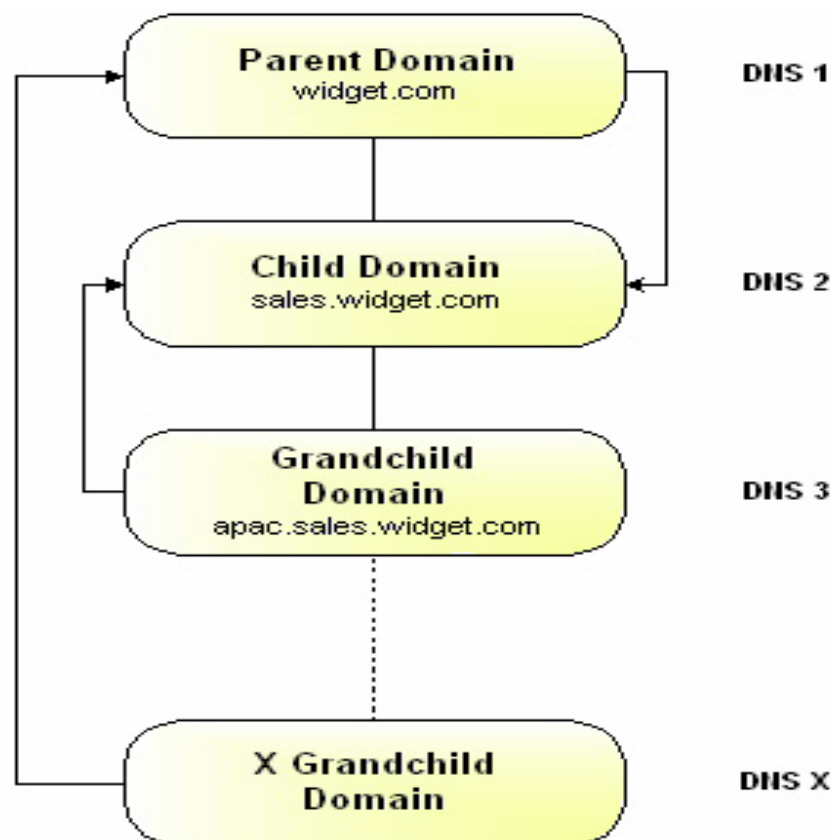
**Migrating the NKDC Specific Login Restrictions:** Login Restrictions specific to NKDC are not migrated.

## 2.5 Configuring DNS in a DSfW Enviroment

In your DSfW environment,

- ♦ **when only one DNS server exists:** Ensure that the nameserver entry in the `/etc/resolv.conf` file of the server being configured points to this DNS server.
- ♦ **when multiple DNS servers exist:** Ensure that the domain being configured can at least resolve the forest root domain and the immediate parent domain.

Assume that you are configuring `apac.sales.widget.com`, with `sales.widget.com` as its immediate parent domain and `widget.com` as the forest root domain.



In this DSfW environment, `sales.widget.com` and `widget.com` are configured as DNS servers for their respective domains. While configuring `apac.sales.widget.com`, for DNS2 to act as a primary DNS server for this domain, it should resolve `widget.com` as well, which requires you to configure DNS2 as a passive or secondary DNS server for `widget.com`.

DNS1 must also act as a secondary DNS for the sales.widget.com domain to handle the queries of this domain. For steps to configure a DNS server as the secondary/passive of a zone/domain hosted on other DNS server, refer to the “[Associating a Zone to Specific DNS Servers](#)” in the *OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux*

---

**NOTE:** The location of the child domain in a forest is not verified during the installation. Make sure that the DNS domain of the child domain is correct. Assume parent.com is the parent domain and child.parent.com is the child domain. Installation continues when the child domain is named as child.com, but DSfW will not function properly.

---

## 2.6 Configuring a Domain Controller as a Backup Domain Controller

For a domain controller to act as a backup controller:

- 1 Add the schema and the configuration partitions.
- 2 Using the `CASA-cli` client utility, set the CASA credentials on the backup domain controller with the following commands.

```
KEYVALUE=<dns-admin_dn> CASAcli -s -n dns-ldap -k CN
```

```
KEYVALUE=<password> CASAcli -s -n dns-ldap -k Password
```

---

**TIP:** The `CASA-cli` client utility is not installed by default. To execute these steps, install the `CASA-cli` package using YaST.

---

- 3 Using iManager, execute the following steps to configure DNS server in a passive mode:

- 3a Click *DNS>DNS Server Management>Create Server* option.

Specify the NCP server name of the backup domain controller, hostname and the domain name for the server object.

- 3b Click *DNS>DNS Server Management>View/Modify Zone* option.

- 3b1 Select the DNS zone from the list. Click *OK*.

- 3b2 Associate the zone with the DNS server. For details on associating zone with a DNS server, see “[Associating a Zone to Specific DNS Servers](#)” in the *OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux*.

---

**NOTE:** Passive DNS servers cannot accept dynamic updates, So we recommend that you do not join the workstations after the primary domain controller is down.

---

- 4 Restart novell-named on the backup domain controller using the following command:

```
rcnovell-named restart
```

- 5 Execute the instructions specified in [Transferring the ADPH Master Role to Other Domain Controllers](#) and [Transferring Role from an Primary Domain Controller to an Additional Domain Controller](#).

## 2.7 Utilities Not Supported in DSfW

The following utilities cannot be used on a DSfW server

- ♦ ldif2dib
- ♦ ndsmerge

## 2.8 Post-Install Operations

This section outlines tasks you need to do after the DSfW servers are installed.

- ♦ [Section 2.8.1, “Restarting DNS,” on page 71](#)
- ♦ [Section 2.8.2, “Network Ports Used by DSfW,” on page 71](#)

### 2.8.1 Restarting DNS

After you have installed a child domain or an additional domain controller, the DNS server running at forest root domain (or the DNS server you are pointing to in `/etc/resolv.conf` file) must be restarted. Execute the following command on the server hosting the Novell DNS service:

```
xadcntrl reload
```

For information on updating records, refer to “[Understanding DNS and DHCP Services](#)” in the *OES 2 SPI: Novell DNS/DHCP Administration Guide for Linux*.

### 2.8.2 Network Ports Used by DSfW

This section discusses the network ports that are used by DSfW services to listen on for incoming network traffic. These ports are configured automatically after the DSfW installation.

**Table 2-2** *Services and Network Ports used by DSfW*

Service	Port / Protocol
Microsoft-DS traffic	445/TCP, 445/UDP
LDAP	389/TCP (or 636/TCP if using SSL)
LDAP Ping	389/UDP
Kerberos	88/TCP, 88/UDP
DNS	53/TCP, 53/UDP
RPC Endpoint Manager	135/TCP, 135/UDP
RCP Dynamic Assignments	1024 - 65535/TCP
Global Catalog LDAP	3268/TCP
Global Catalog LDAP over SSL	3269/TCP
Network Time Protocol	123/UDP
NetBIOS Name Service	137/TCP, 137/UDP

Service	Port / Protocol
NetBIOS Datagram Service	138/UDP
NetBIOS Session Service	139/TCP

The RPC dynamic assignment rule allows inbound traffic on any port above 1023. If your firewall permits this, there is very little reason to enable a firewall. However, you can force `xadsd` to use a specific port by using the `-p` option. Otherwise, RPC ports are ephemeral.

After restarting the DNS server, refer to [Section 2.10, “Verifying the Installation,”](#) on page 72 to verify that eDirectory and DSfW have been installed and configured correctly.

---

**IMPORTANT:** After installing DSfW server into a partition in which you want to configure a domain, the DSfW server holds the master replica of that partition. This is required because the master replica holds the FSMO roles for the domain.

---

## 2.9 Restarting the DSfW Services

DSfW consists of several services that need to be restarted in sequence. Execute the following command to restart all DSfW services after installation.

```
xadcntrl reload
```

---

**NOTE:** You do not need to execute this command every time you install DSfW.

---

## 2.10 Verifying the Installation

Perform these tasks to verify that eDirectory and DSfW have been installed and configured correctly.

- ♦ Check the `/etc/hosts` file to ensure that it contains only one entry with this server’s primary IP address. For example:

```
192.168.1.1 oesdc.example.com oesdc
```

- ♦ Check the `/etc/resolv.conf` file to ensure that it contains a nameserver and domain search entry for this server. For example:

```
nameserver 192.168.1.1search example.com
```

- ♦ Verify that eDirectory has been properly configured by using the following command:

```
/opt/novell/eDirectory/bin/ndsstat -h localhost
```

This command should return information similar to the following:

```
Tree Name: EXAMPLE_TREE
Server Name:.CN=OESDC.OU=Novell.dc=example.dc=com,T=EXAMPLE_TREE
Binary Version: 20217.06
Root Most Entry Depth: 0
Product Version: eDirectory for Linux v8.8 SP4 [DS]
```

- ♦ Execute the following command to run the provisioning utility:



```
/opt/novell/xad/sbin/provision --locate-dc example.com
```

This command should return information similar to the following:

```
Domain Services for Windows Server Provisioning Tool
Copyright (c) 2001-2007 Novell, Inc. All rights reserved.
DC: \\oesdc.example.com
Address: \\192.168.1.1
Dom Guid: f3469fb6-4197-457b-4ba3-b69f46f39741
Dom Name: example.com
Forest Name: example.com
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV CLOSEST WRITABLE GTIMESERV DNS_DC
DNS_DOMAIN DNS_FOREST
```

---

**NOTE:** By default, the provision utility runs with the `--locate-dc` option only. To execute other options, export `SASL_PATH=/opt/novell/xad/lib64/sasl2` and run `kinit` with a valid domain username before using the provision utility.

---

- ♦ Verify that the KDC is working by using the following command to obtain a Kerberos ticket:

```
/opt/novell/xad/bin/kinit Administrator@EXAMPLE.COM
```

Enter the Administrator password when prompted. The command should complete without errors (nothing is displayed).

- ♦ Execute the following command:

```
rpcclient -k localhost -c dsroledomaininfo
```

If your server is configured correctly, you should see information similar to the following:

```
Machine Role = [5]
Directory Service is running.
Domain is in native mode.
```

You should now be able to add (join) a Windows machine to the new DSfW domain. This procedure is described in [Chapter 3, “Logging In from a Windows Workstation,”](#) on [page 77](#).

## 2.11 Removing a DSfW Server

Before deleting a domain controller from an OES 2 server, verify the following:

- ♦ It should not contain a child domain.
- ♦ It should not be an **ADPH** master. If this domain controller is an ADPH master, you must transfer the ADPH master role to another domain controller before deleting it. See [Section 2.11.1, “Transferring the ADPH Master Role to Other Domain Controllers,”](#) on [page 74](#) for more information on transferring the RID master role.
- ♦ If you delete an additional domain controller, at least one domain controller in this domain must have a copy of the config/schema partitions.

The example commands in this section assume that the following domains exist:

- ♦ Parent: example.com
- ♦ Child: child.example.com

To delete a DSfW server, run the `ndsdcrm` utility from `/opt/novell/xad/sbin/ndsdcrm`.

Examples:

For a non-name-mapped domain (such as example.com at IP address 1.2.3.4, with the admin password as 'n'), the command would be:

```
/opt/novell/xad/sbin/ndsdcrm -p 1.2.3.4 -w n
```

For a name-mapped domain (such as an eDirectory server at IP address 5.6.7.8, tree admin as cn=admin.o=novell, with the password as 'n'), the command would be:

```
/opt/novell/xad/sbin/ndsdcrm -p 5.6.7.8 -a cn=admin.o=novell -w n
```

The `ndsdcrm` utility can also remove a partial or failed installation. It can detect the presence of an additional domain controller or a domain controller in a domain and prompts accordingly. If a domain controller has the ADPH master role, it prompts and exits on removal. If a server or a domain controller is the ADPH master and contains only a replica of the configuration or schema partition, it must be moved to some other server in the domain by using management consoles.

The `ndsdcrm` utility removes only those objects that were created by DSfW installation and provisioning. Objects with mandatory reference attributes to any of the removed objects might become 'unknown' to it. These objects need to be manually deleted before you attempt to configure DSfW in the same partition.

---

**NOTE:** `ndsdcrm` does not restore the Samba Default Password Policy.

---

When DSfW is reconfigured, it is a good practice to reconfigure all the related services such as NAM, iFolder, and so on.

## 2.11.1 Transferring the ADPH Master Role to Other Domain Controllers

You can transfer the RID master role by using MMC or LDIF as follows:

### Using MMC

- 1 Open *Active Directory Users and Computers*.
- 2 Right click *Active Directory Users and Computers*, then click *Connect to Domain Controller*.
- 3 In the *Enter the name of another domain controller* text field, specify the name of the domain controller that you want to assign the RID master role.  
or  
Select the domain controller from the *Domain Controllers* drop down list.
- 4 Right click *Active Directory Users and Computers*, then click *Operations Masters*.
- 5 Click the *RID* tab, then select *Change*. This transfers the RID master role to other domain controllers.

## Using LDIF File

The FSMO roles are located on the RootDSE and the `becomeRidMaster` operational attribute is used to transfer them. The appropriate operational attribute is written on the new domain controller to receive the FSMO role operation, then the old domain controller is demoted and the new domain controller is automatically promoted.

The LDIF file looks like this,

```
dn:
changetype: Modify
becomeridmaster: 1
```

## 2.11.2 Transferring Role from an Primary Domain Controller to an Additonal Domain Controller

To transfer role from an active primary domain controller to an additional domain controller, execute the following steps:

---

**NOTE:** Before transferring the role of Primary Domain Controller to the Additional Domain Controller, ensure that you have transferred all the FSMO roles.

---

- 1 Copy all policies from the PDC to the additional DC. The policies are stored in `/var/opt/novell/xad/sysvol/sysvol/domain.com/Policies/{default domain policy GUID}` folder. If you have not modified or updated any policies, it is sufficient to copy the default domain policy.

If you have updated the policies, run `gpo2nmas` utility on the new PDC.

- 2 Add a crontab entry for `gpo2nmas` on the ADC.

For example: `*/30 * * * * /opt/novell/xad/sbin/gpo2nmas -q -g "{31B2F340-016D-11D2-945F-00C04FB984F9}"`

- 3 Traverse to the object `CN={31B2F340-016D-11D2-945F-00C04FB984F9}. CN=Policies. CN=System. dc=domain. dc=tld. T=oes2spl.`

Change the value of the `gpcfilesyspath` attribute to `//new-pdc.domain.tld/SYSVOL/domain.TLD/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}`.

Substitute the *new-pdc.domain* with the name of the PDC server.

- 4 Execute the following command to change the permissions for SYSVOL:

```
chown -R administrator uid : Domain admin gid/var/opt/novell/xad/sysvol
```

- 5 On the new PDC, add the following lines to the `smb.conf` file.

```
[sysvol]
comment = Group Policies
path = /var/opt/novell/xad/sysvol/sysvol
writable = Yes
share modes = No
nt acl support = No
```

- 6 In the `smb.conf` file of the ADC, traverse to the `msdfs` section. Here the `msdfs proxy` under `SYSVOL` section is referring the old PDC. Change the `msdfs proxy` to point to the new PDC. The changes take effect immediately.

### 2.11.3 Removing Unknown Objects After Removing an Additional Domain Controller

The `ndsrm` utility removes only those objects that were created by DSfW installation and provisioning. Objects with mandatory reference attributes to any of the removed objects might become 'unknown' to it. These objects need to be manually deleted before you attempt to configure DSfW in the same partition.

### 2.11.4 Child Domain Installation on a Non-name-mapped Setup

While installing a child domain, the command `kinit administrator@<parentdomain>` is executed because `kdc` is yet to be configured on the child domain. This command fails on the parent domain administrator because the `SamAccountName` of the administrator of the parent domain is garbled.

When a child domain is removed by using the `ndsrm` utility, its administrator object is flagged for deletion and bears the same `SamAccountName` as that of the parent domain's administrator. After merging the child and the parent partitions, but before the flagged administrator object is actually cleaned from the child domain, the Active Directory Provisioning Handler (ADPH) detects the two users with the same `SamAccountName` and changes it for one of them.

Typically, if the ADPH detects two user objects with the same `SamAccountName`, and when either of them is marked for deletion, it must not change the `SamAccountName`.

# Logging In from a Windows Workstation

# 3

With Domain Services for Windows (DSfW) properly set up, Windows workstations can be joined to the DSfW domain and users can log in to the domain.

Windows users can then use Windows Explorer (or other familiar Windows interfaces) to browse to the DSfW domain and see the CIFS shares to which they have access.

DSfW supports the following workstation operating systems:

- Windows XP Professional SP2 or greater
- Windows\* Vista\* Business SP1
- [Section 3.1, “Joining a Windows Workstation to a DSfW Domain,” on page 77](#)
- [Section 3.2, “Logging In to a DSfW Domain,” on page 80](#)
- [Section 3.3, “Logging Out,” on page 80](#)

## 3.1 Joining a Windows Workstation to a DSfW Domain

Kerberos authentication requires that the domain controller’s time and the Windows workstation’s time be synchronized. After the DSfW server is installed, verify that the Windows workstations in the domain are set to get their time from this server.

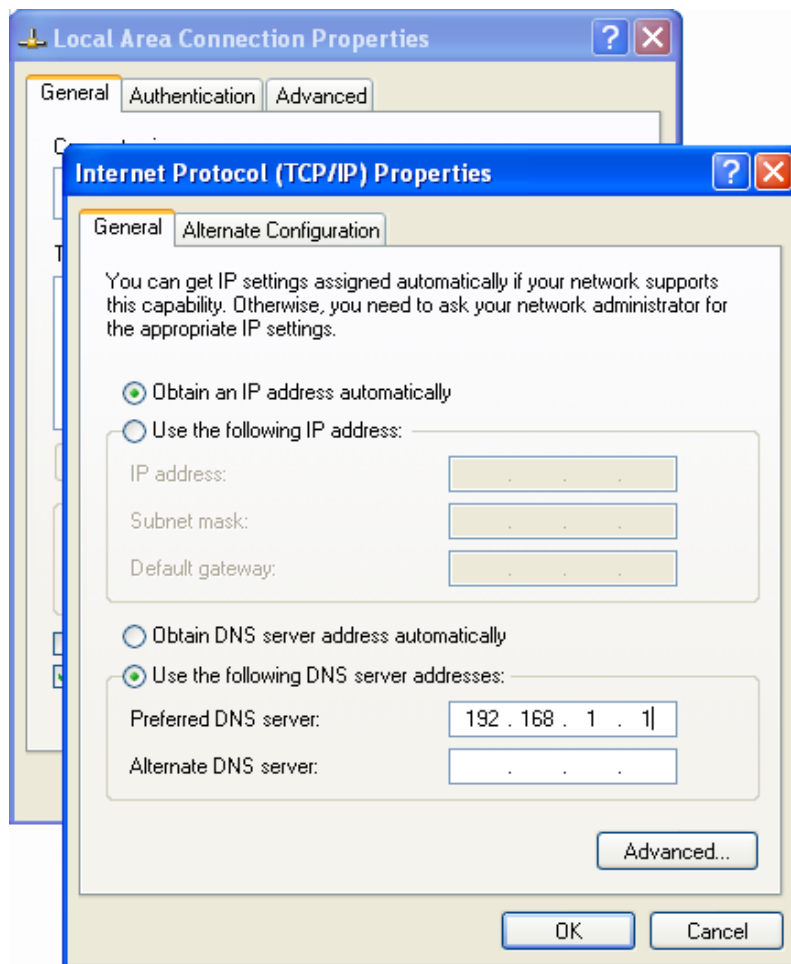
Follow these steps to join a Windows workstation to a DSfW domain.

---

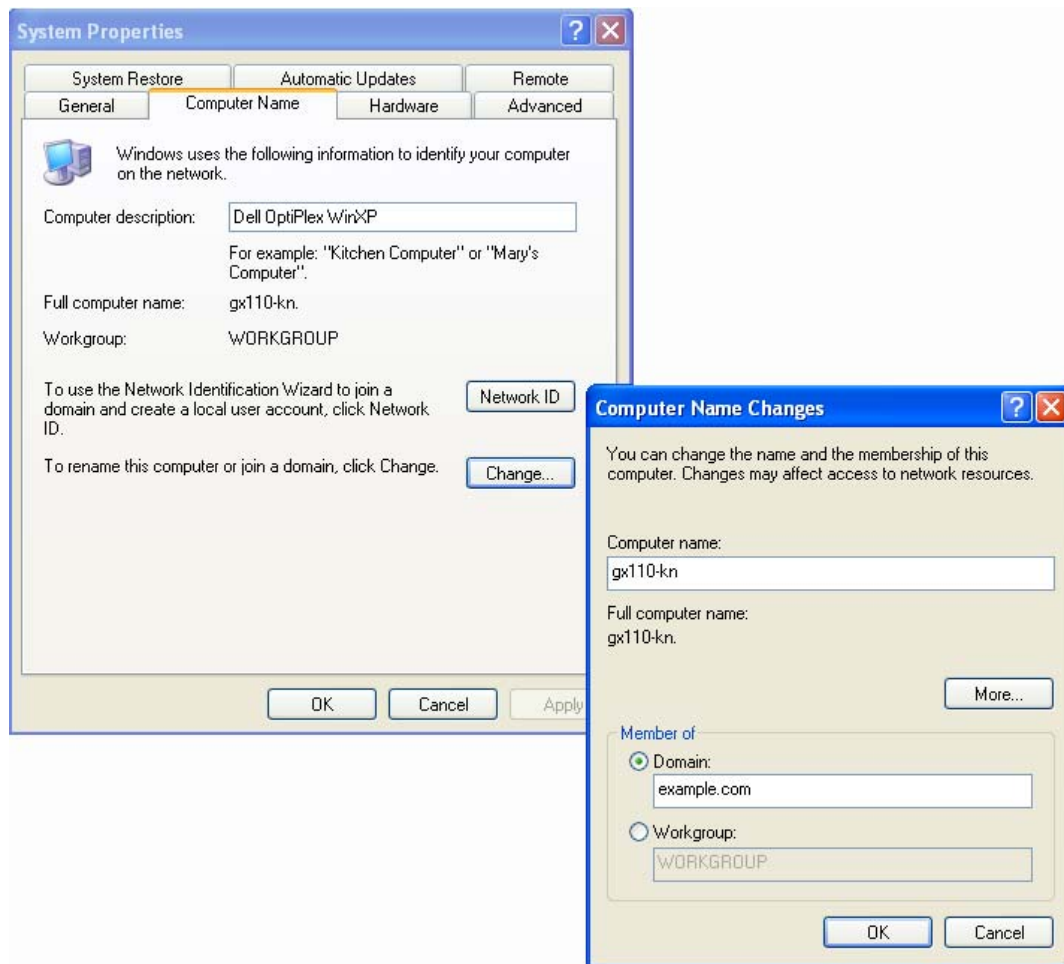
**NOTE:** The steps might vary depending on how you have Windows configured. The examples shown are for the Windows “classic” desktop.

---

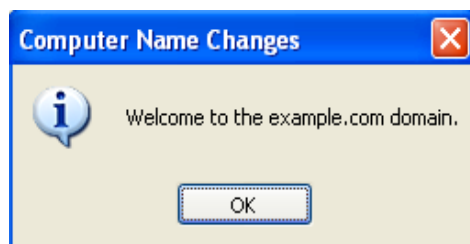
- 1** From a Windows computer on the same network as the DSfW server, go to Network Connections in the Control Panel, select Local Area Connection, and click *Properties*.
- 2** Select Internet Protocol (TCP/IP) and click *Properties*.
- 3** Select *Use the following DNS server addresses*. For the Preferred DNS Server, enter the IP address of the DNS server configured for DSfW, then click *OK*.



- 4 From the Start menu, right-click *My Computer* and select *Properties*.
- 5 On the *Computer Name* tab, click *Change*.
- 6 In the Computer Name Changes dialog box, select *Domain*, enter the DSfW domain name, then click *OK*.



- 7 When prompted, provide the name and password for an account with permission to join the domain. This is the Administrator and password configured when you installed DSfW.
- 8 A welcome message is displayed after the computer has successfully joined the domain. Click *OK* to continue.



- 9 As prompted, click *OK* to restart the computer for the changes to take effect.

The computer you just joined to the domain has an object created for it in the Computers container in the DSfW domain.

A user with administrative privileges for the container that is being name-mapped can join a workstation to the domain being created.

---

**NOTE:** When you install Windows XP, it prompts you to select whether it is part of the workgroup or the domain. If domain is selected, it reports that an invalid domain is specified. However, if there is an existing Windows XP machine installed, it is possible to join this workstation to the domain.

---

## 3.2 Logging In to a DSfW Domain

After the Windows workstation has joined the DSfW domain and the computer has been restarted (as explained in [Section 3.1, “Joining a Windows Workstation to a DSfW Domain,” on page 77](#)), DSfW user accounts can be used to log on to the Windows workstation.

- 1 Start the Windows workstation or press Ctrl+Alt+Del to bring up the Windows log on dialog box.
- 2 In the Log On to Windows dialog box, enter the user name and password of a user that has been provisioned for DSfW. Initially, the only provisioned user is the Administrator account created when you installed DSfW.
- 3 In the *Log on to* field, click the down-arrow to select the DSfW domain (identified by its NetBIOS name), then click *OK*.



## 3.3 Logging Out

To log out of the DSfW domain, select Log Off from the *Start* menu.



# Creating and Provisioning Users

# 4

After Domain Services for Windows (DSfW) is properly installed and configured, you can create users with either Novell iManager or a Microsoft Active Directory management tool such as Microsoft Management Console (MMC).

Although the users are created in eDirectory™, they appear in the domain when viewed from MMC. User account information that is common to both eDirectory and Active Directory can be managed with either tool.

Users created in the DSfW domain are automatically provisioned to use DSfW. In Active Directory, logon users are normally created in the Users container within the domain. In DSfW, users can be created anywhere within the domain (which corresponds to an eDirectory partition).

When a user is provisioned, the ADPH agent adds a number of Active Directory-specific operational attributes to the User object. These include SAM (Security Account Manager)-related attributes and RFC 2307 attributes.

- ♦ [Section 4.1, “Creating Users in iManager,” on page 81](#)
- ♦ [Section 4.2, “Creating Users in MMC,” on page 83](#)
- ♦ [Section 4.3, “Managing Users,” on page 84](#)

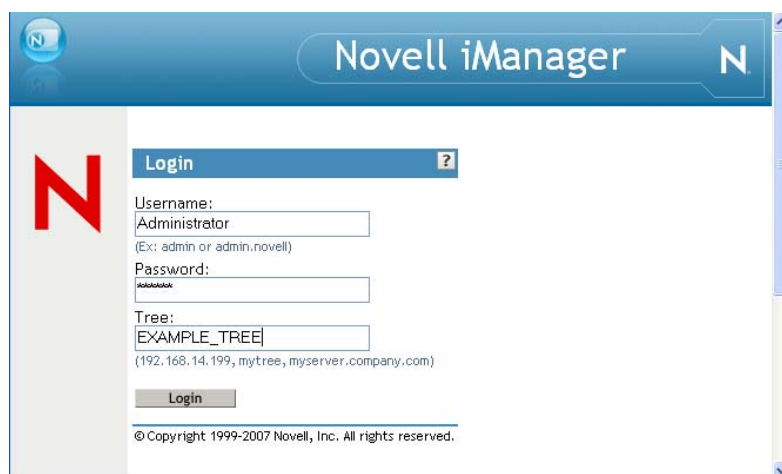
## 4.1 Creating Users in iManager

- 1 Start a browser and point to `http://ip_address_of_server/nps/iManager.html`.  
For example, `http://192.168.1.1/nps/iManager.html`.
- 2 Accept the certificate, enter the Administrator account/password and eDirectory tree, and click *Login*.

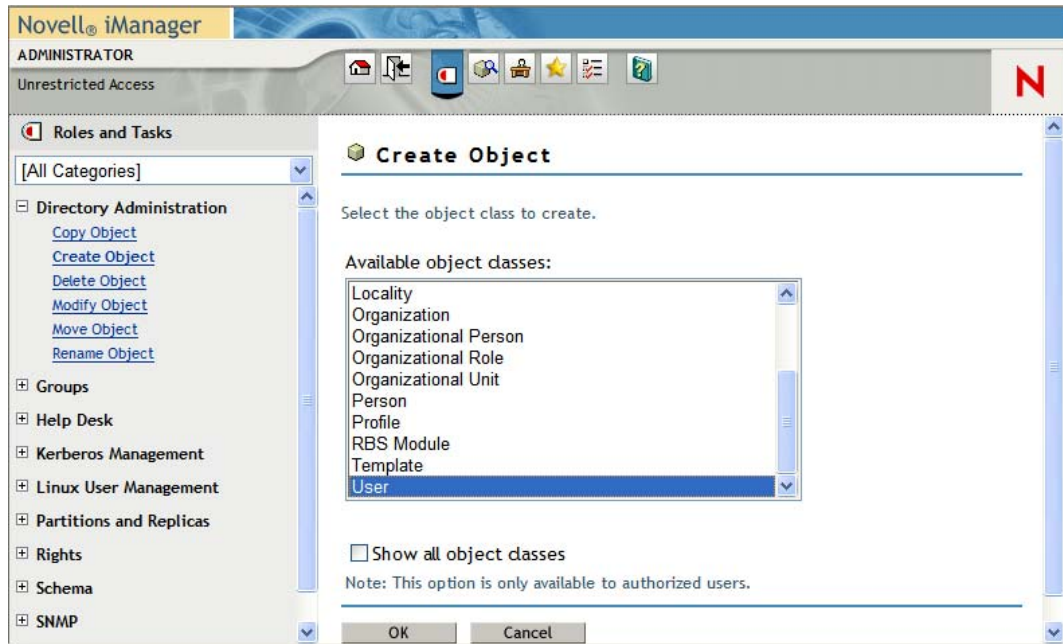
---

**IMPORTANT:** Contextless logins using iManager can lead to unexpected results if you try logging in as an administrator. An administrator object exists for every domain and you might accidentally attempt to log in as an administrator of a domain where you lack sufficient access.

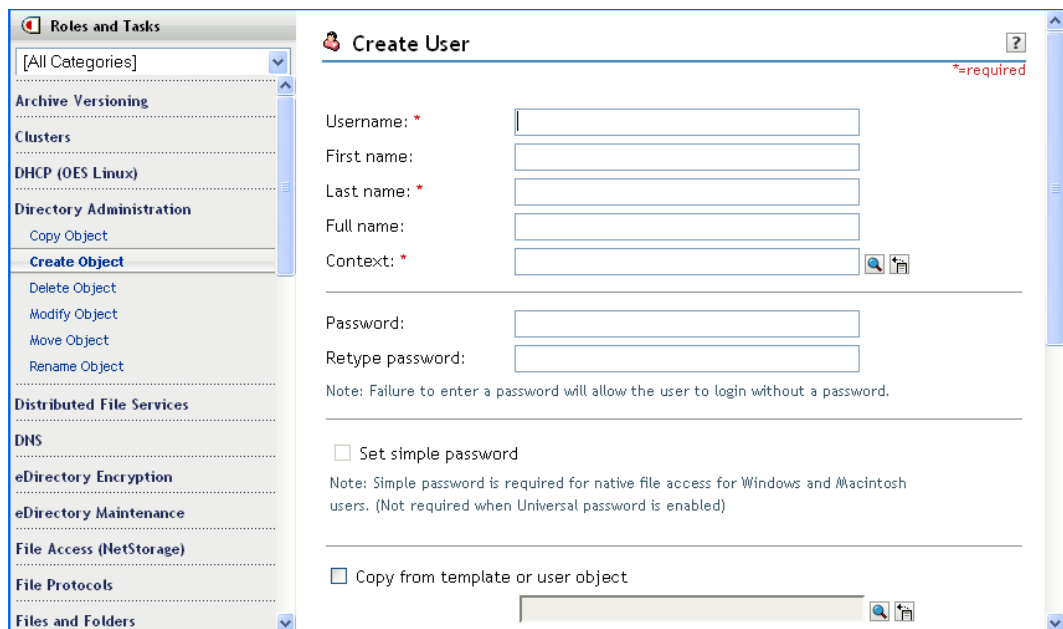
---



- 3 Under Roles and Tasks, select *Directory Administration > Create Object*.
- 4 Select the User object class and click *OK*.



- 5 Specify the user account information, specify the context, and click *OK*.



Users created anywhere in the domain (partition) are automatically provisioned for DSfW. Additional information you specify for each user, such as telephone numbers and e-mail addresses, can also be viewed and modified in MMC. However, attributes that are specific to eDirectory can not be managed in MMC.

---

**NOTE:** If an administrator changes the primary group of the user objects, the gidNumber and primaryGroupID attributes might not be synchronized. LUM refers to the gidNumber, and Samba depends on the primaryGroupId. File system access issues might occur if they are not synchronized.

---

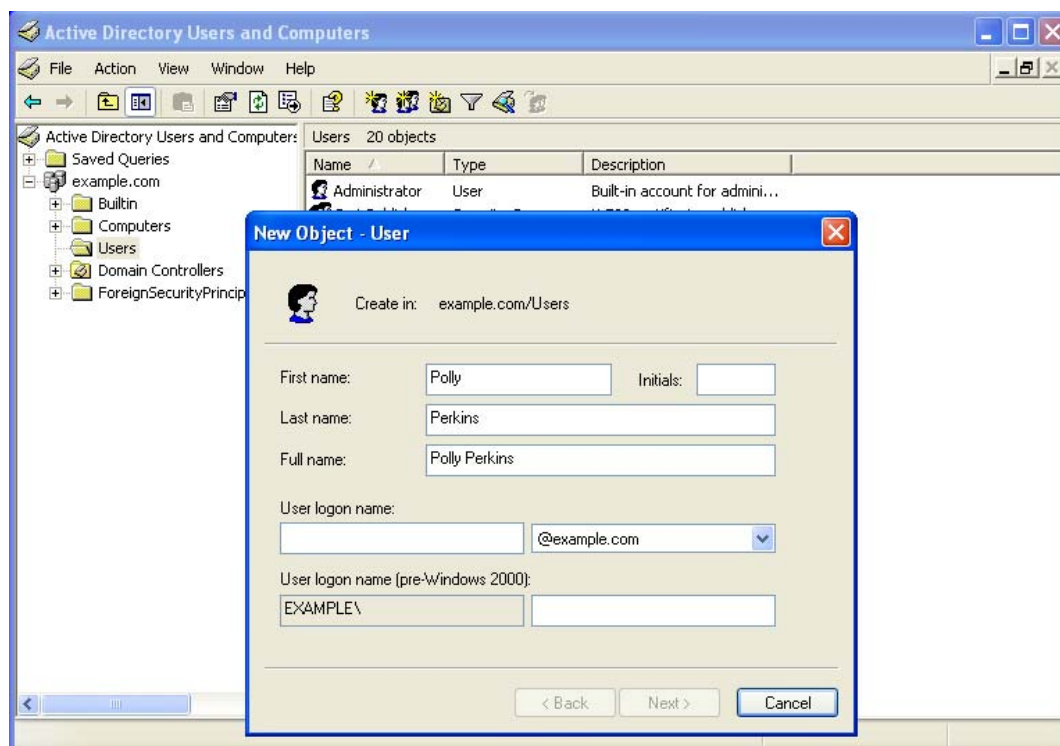
## 4.2 Creating Users in MMC

If you have a Windows Server 2003 network with Active Directory, you should have the Administrative Tools already installed. If not, they can be downloaded from [Microsoft's Web site](http://www.microsoft.com/downloads/details.aspx?FamilyID=C16AE515-C8F4-47EF-A1E4-A8DCBACFF8E3&displaylang=en) (<http://www.microsoft.com/downloads/details.aspx?FamilyID=C16AE515-C8F4-47EF-A1E4-A8DCBACFF8E3&displaylang=en>).

- 1 At a Windows workstation, click *Start > Run* and enter `mmc`.
- 2 When the Console opens, select *File > Add/Remove Snap-ins*.
- 3 Select *Active Directory Users and Computers* and click *Add*.
- 4 Click *OK*.

A new window opens with a list of objects in the left column, including the Domain Services for Windows domain name.

- 5 Open the Domain Services for Windows domain and click the Users container.
- 6 Select *Action > New > User*, or click on the user icon in the toolbar.



- 7 Follow the prompts to complete the user object creation.

Users created in the domain are automatically provisioned for DSfW. Additional information you specify for the user, such as telephone numbers and e-mail addresses, can also be viewed and modified in iManager. However, attributes that are specific to Active Directory cannot be managed in iManager.

## 4.3 Managing Users

- ♦ [Section 4.3.1, “Moving User Objects Across Containers,” on page 84](#)
- ♦ [Section 4.3.2, “Primary Group Appears Twice in the memberOf Properties Page,” on page 84](#)
- ♦ [Section 4.3.3, “Adding Newly Created Users to a Group gives Error Message,” on page 84](#)
- ♦ [Section 4.3.4, “Dynamic Group Is Not Supported in DSfW,” on page 84](#)

### 4.3.1 Moving User Objects Across Containers

When you move objects across containers through MMC, even though the move operation is successful, you might get an error message saying that Windows cannot move that object because there is no such object on the server. You can use MMC to connect to the domain controller that holds the master replica and retry the operation.

### 4.3.2 Primary Group Appears Twice in the memberOf Properties Page

DSfW explicitly adds users to the primary group. This causes MMC to display the group twice in the memberOf property page.

### 4.3.3 Adding Newly Created Users to a Group gives Error Message

You cannot add users by using MMC to Domain Local, Global and Universal Groups who do not have the Last Name property. Though an error message is displayed, the users are added to the groups. The error message can be avoided if the user is created with the Last Name property.

### 4.3.4 Dynamic Group Is Not Supported in DSfW

# Managing Group Policy Settings

# 5

In Active Directory, Group Policies ease the administrator's job of implementing security settings and enforcing IT policies for all users within an organizational unit, domain, or across an entire site. Group policy settings are made in a Group Policy Object (GPO). You can create GPOs for various departments in an organization to more easily manage the computers and users in each department. For example, you might create a GPO for the Engineering department and a different GPO for the Sales department.

DSfW supports all Group Policy settings that apply to Windows servers and workstations. Group Policy settings that apply to domain controllers (such as Password Policies) are not supported in the OES 2 environment. The Password Policies for DSfW users are controlled by eDirectory and the Universal Password settings.

When you install DSfW, a default Group Policy is created for the domain. It is recommended that you create a new Group Policy and make modifications to it, rather than change the default Group Policy.

You might get 'access denied' warnings while backing up Group Policies in XP and Vista clients connected to DSfW. It is safe to ignore them.

---

**NOTE:** You must be a member of the Domain Admins group to edit an Active Directory Group Policy for a domain.

---

- ♦ [Section 5.1, “Using the Users and Computers Tool,” on page 85](#)
- ♦ [Section 5.2, “Group Policy Objects,” on page 86](#)
- ♦ [Section 5.3, “Group Policy Management,” on page 89](#)

## 5.1 Using the Users and Computers Tool

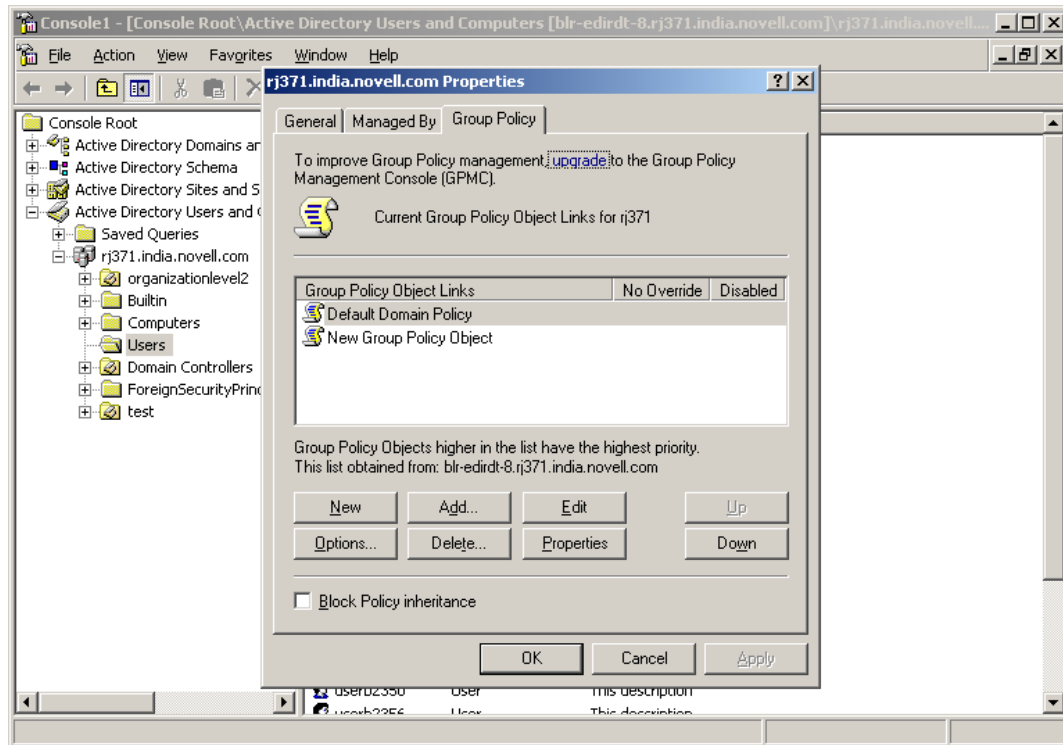
To create a new Group Policy, you can use the Active Directory Users and Computers tool.

---

**NOTE:** If you have installed the Group Policy Management Console from Microsoft, the *Group Policy* tab options described below are no longer accessible. Refer to the Microsoft Windows Server 2003 documentation for instructions on how to use the Group Policy Management Console to manage Group Policies.

---

- 1 Start Active Directory Users and Computers.
- 2 In the console tree, right-click the Domain Services for Windows domain, and then select *Properties*.
- 3 Click the *Group Policy* tab, then click *New* to create a new Group Policy.



- 4 Specify a name for the new Group Policy, then click Ok..

The policy settings you define are linked to the domain, which means the policy settings you define are applied to the domain according to the inheritance and preference options used by Active Directory.

For more information about Group Policy Object settings, refer to Microsoft's online [Group Policy documentation](http://technet2.microsoft.com/WindowsServer/en/library/abc2890d-f3f1-408c-bafc-ac9e4e5b0e831033.mspx?mfr=true) (<http://technet2.microsoft.com/WindowsServer/en/library/abc2890d-f3f1-408c-bafc-ac9e4e5b0e831033.mspx?mfr=true>). For more information about NMASTM and Universal Password settings, refer to the [Novell® eDirectory documentation](http://www.novell.com/documentation/edir88/) (<http://www.novell.com/documentation/edir88/>).

## 5.2 Group Policy Objects

Group Policy settings are stored in Group Policy Objects (GPO). A GPO consists of the following:

**Group Policy Container:** Stored in the directory.

**Group Policy Template:** Stored in the `sysvol` SMB volume.

The default configuration of `sysvol` resides in the `smb.conf` file.

```
[sysvol]
comment = Group Policies
path = /var/opt/novell/xad/sysvol/sysvol
writable = Yes
share modes = No
nt acl support = No
```

Group Policy Template is stored in the `sysvol` SMB volume. The `sysvol` volume of a domain is stored in the first domain controller of the domain. Other domain controllers in the domain have reference to this volume and do not physically store it. For Group Policies to work, ensure that the first domain controller is functional.

`sysvol` corresponds to the `/var/opt/novell/xad/sysvol/sysvol` directory on the domain controller. The Group Policy Template of the default domain policy GPO is stored in the `/var/opt/novell/xad/sysvol/sysvol/<domain name>/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}` directory.

A Group Policy Template contains the following information:

- ♦ Template-based administrative policies
- ♦ Security settings
- ♦ Script files
- ♦ Information for the applications that are available for Group Policy software installation.

## 5.2.1 Account Policies and Gpo2nmas

There is a group of security settings in the GPO called Account Policies that contains the following policies:

- ♦ Password Policy
- ♦ Account Lockout Policy
- ♦ Kerberos Policy

The `MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf` file inside `sysvol` contains the Account Policies of the GPO. They are managed by using the Samba server. The Password Policy and the Account Lockout Policy are enforced by eDirectory, and the Kerberos Policy is enforced by the Kerberos Key Distribution Center (KDC). The Account Policies settings are not read directly by eDirectory or KDC. The eDirectory server enforces only those policies that are stored in its Directory Information Base (DIB). Even the Kerberos KDC expects the Kerberos Policy to be stored in eDirectory.

The `gpo2nmas` tool synchronizes the policies stored in eDirectory with those in `sysvol`. This tool is programmed to run every 30 minutes by using the cron service. If the policies stored in eDirectory are newer than the Account Policies in `sysvol`, `gpo2nmas` updates the Account Policies. Similarly, it updates the policies in eDirectory if they do not match the Account Policies. When you modify the Account Policies in `sysvol` by using Group Policy Management Console (GPMC), `gpo2nmas` makes the relevant changes to the policies in eDirectory when it runs again.

Only those Account Policies settings that are on the Default Domain Policy GPO are synchronized with eDirectory and `gpo2nmas` tool works only on the Default Domain Policy GPO.

### Supported Account Policies Settings

Following Account Policies settings are supported:

- ♦ **Password Policies**
  - ♦ Enforce Password History
  - ♦ Maximum Password Age

- ♦ Minimum Password Age
- ♦ Minimum Password Length
- ♦ **Account Lockout Policy**
  - ♦ Account Lockout Duration
  - ♦ Account Lockout Threshold
  - ♦ Reset Account Lockout Counter After
- ♦ **Kerberos Policy**
  - ♦ Maximum Lifetime for User Ticket
  - ♦ Maximum Lifetime for User Ticket Renewal

---

**IMPORTANT:** Remember the following:

- ♦ DSfW follows the password history feature as mentioned in the [Password Policy for LDAP Directories \(http://tools.ietf.org/html/draft-behera-ldap-password-policy-08\)](http://tools.ietf.org/html/draft-behera-ldap-password-policy-08), where the current password is not part of the password history. Therefore, it takes one extra password change to reuse a password.

For example, if Enforce Password History Policy residing at *Default Domain Policy* > *Computer Configuration* > *Windows Setting* > *Security Settings* > *Password Policy* is set to 2, it takes 3 password changes in Domain Services for Windows to reuse a password.

- ♦ In a Domain Services for Windows domain, the password policies are stored in the container `cn=Domain Password Policy,cn=Password Policies,cn=System, <domain root>`.
- 

## 5.2.2 Enforcing Computer Configuration and User Configuration

DSfW supports computer configuration and user configuration settings in GPOs. You can change the computer configuration settings, such as customizing the start menu, desktop, and Internet Explorer\*, and the user configuration settings, such as roaming profiles and desktop customization.

## 5.2.3 Known Issues

Only the default domain GPO is honored by DSfW services. Because gpo2nmas synchronizes only the default domain GPO with the policies stored in eDirectory™, the other GPOs are ignored.

## 5.2.4 Troubleshooting

If you receive a message indicating that the computer configuration or user configuration is not applicable, do one of the following:

- ♦ Verify that winbindd is running and functional. The `getent passwd <username>` command should return the information for the local users and the domain users.
- ♦ Check the Samba log files in `/var/log/samba` for any errors.



## 5.3 Group Policy Management

- ♦ [Section 5.3.1, “Blocking GPO Inheritance in DSfW,” on page 89](#)
- ♦ [Section 5.3.2, “Ignore Warnings while Backing up Group Policies,” on page 89](#)
- ♦ [Section 5.3.3, “WMI Filters Cannot be Applied for Processing GPOs,” on page 89](#)

### 5.3.1 Blocking GPO Inheritance in DSfW

Blocking GPO inheritance is not working in DSfW. Blocking GPO inheritance prevents the GPOs linked to higher sites, domains, or organizational units from being automatically inherited by subsequent levels.

### 5.3.2 Ignore Warnings while Backing up Group Policies

You might get 'access denied' warnings while backing up Group Policies in XP and Vista clients connected to DSfW. It is safe to ignore them.

### 5.3.3 WMI Filters Cannot be Applied for Processing GPOs

WMI filters are not supported.



# Managing Trust Relationships in Domain Services for Windows

# 6

Trust relationships are a key to managing Domain Services for Windows (DSfW).

- ♦ [Section 6.1, “What is a Trust?,” on page 91](#)
- ♦ [Section 6.2, “Cross-Forest Trust Relationships,” on page 92](#)

## 6.1 What is a Trust?

A trust is used to allow users of one domain to access resources from another domain. Trusts are automatically created within an eDirectory™ tree when domains are created. For authentication and name lookups to work across domains, a trust relationship must be created between the domains. The trust relationship includes a shared secret that can be used for both Kerberos and NTLM authentication and information that is used to support name resolution.

DSfW supports the following trusts:

- ♦ **External Trusts:** These trusts are nontransitive trusts between two domains in different forests. They can be one-way or two-way. This type of trust is useful to allow resource sharing only between specific domains in different forests.
- ♦ **Forest Trusts:** These trusts are transitive trusts between two forests. These trusts include complete trust relationships between all domains in the relevant forests, so resource sharing among all domains in the forests is allowed. The trust relationship can be either one-way or bidirectional.

Both forests must be operating at the Windows Server 2003 forest functional level. By default, DSfW operates at this level. The use of forest trusts offers several benefits:

- ♦ They simplify resource management between forests by reducing the number of external trusts needed for resource sharing.
- ♦ They provide a wider scope of UPN authentications, which can be used across the trusting forests.
- ♦ They provide increased administrative flexibility by enabling administrators to split collaborative delegation efforts with administrators in other forests.
- ♦ They provide greater trustworthiness of authorization data. Administrators can use both the Kerberos and NTLM authentication protocols when authorization data is transferred between forests.

---

**NOTE:** External Trusts and Forest Trusts are cross-forest trusts.

---

- ♦ **Realm Trusts:** These are one-way and two-way transitive and nontransitive trusts that you can set up between an Active Directory domain and a Kerberos V5 realm, such as trusts found in UNIX and MIT implementations.

Refer to [Understanding Trusts \(http://technet.microsoft.com/en-us/library/cc736874.aspx\)](http://technet.microsoft.com/en-us/library/cc736874.aspx) and [New Trust Wizard Pages \(http://technet.microsoft.com/en-us/library/cc784531.aspx\)](http://technet.microsoft.com/en-us/library/cc784531.aspx) for more information on trusts.

## 6.2 Cross-Forest Trust Relationships

Administrators must configure trust relationships manually to access resources in a different forests. Every trust relationship between each domain in the different forests must be explicitly configured.

- ♦ [“Creating a Cross-forest Trust between Active Directory and Domain Services for Windows Forests” on page 92](#)
- ♦ [Section 6.2.2, “Shortcut Trusts,” on page 123](#)

### 6.2.1 Creating a Cross-forest Trust between Active Directory and Domain Services for Windows Forests

This section describes how to create a cross-forest trust between Active Directory and DSfW.

- ♦ [“Configuring the DNS Forwarders on the Domain Services for Windows Server” on page 93](#)
- ♦ [“Configuring the Reverse Lookup Zone Forwarder” on page 103](#)
- ♦ [“Configuring the DNS Forward Lookup Zone on the Active Directory Server” on page 113](#)
- ♦ [“Creating the Trust” on page 116](#)
- ♦ [“Verifying the Trust” on page 123](#)

In this example, win2003ad.com is the domain name of the Active Directory forest and dsfw.com is the domain name of the DSfW forest.

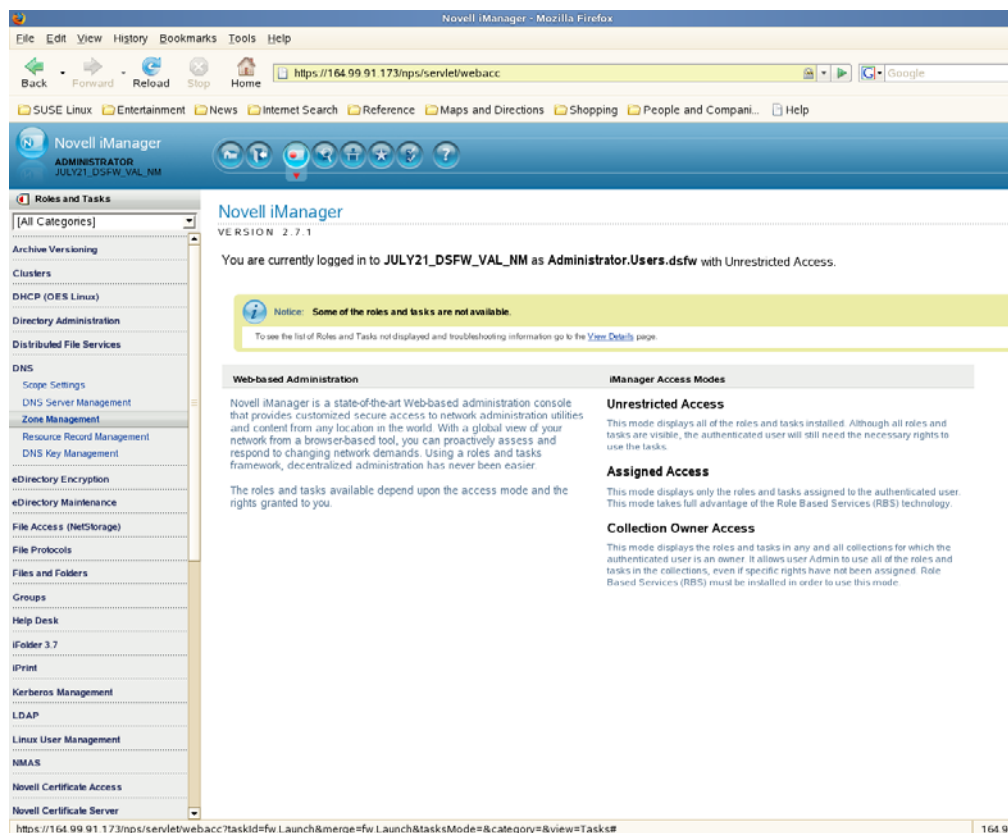
## Configuring the DNS Forwarders on the Domain Services for Windows Server

You need to configure a DNS forwarder on the DSfW DNS server to forward any DNS queries for the Active Directory domain to the Active Directory domain's DNS server.

- ♦ Active Directory domain name: win2003ad.com
- ♦ DSfW domain name: dsfw.com

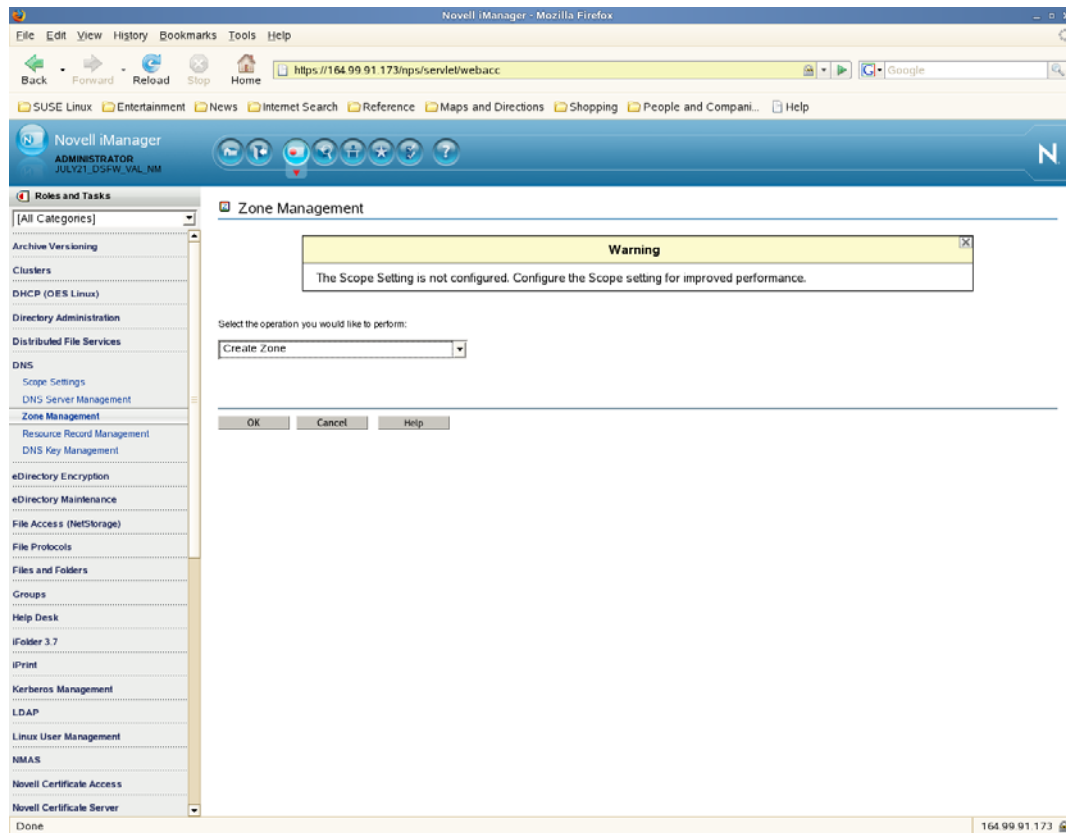
1 Open the Novell iManager DNS plug-in.

1a Click DNS > *Zone Management* to open the Zone Management window in the main panel..



1b Click DNS > *Zone Management* to open the Zone Management window in the main panel.

- 2 From the drop-down list select *Create Zone*, then click *OK* to open the Create DNS Zone window.



3 Select *Create New Zone* and specify the DNS configuration parameters as follows:

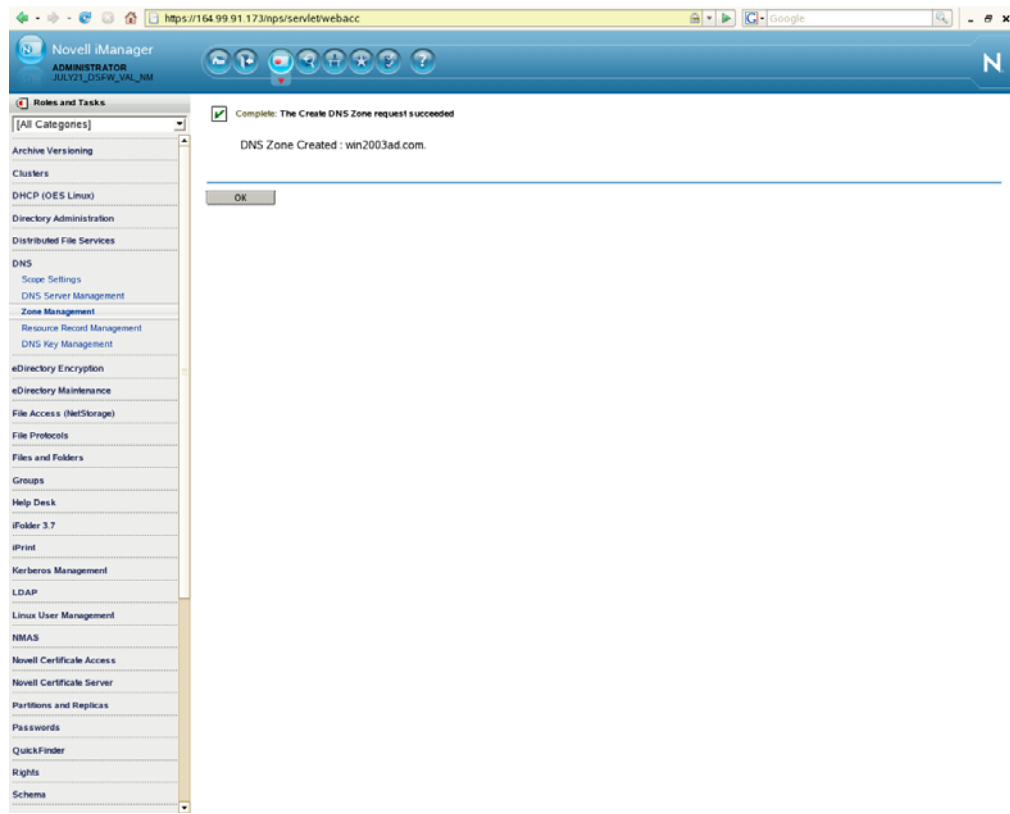
The screenshot shows the 'Create DNS Zone' web interface in Novell iManager. The left sidebar contains a 'Roles and Tasks' menu with categories like 'DNS', 'eDirectory Encryption', and 'eDirectory Maintenance'. The main content area is titled 'Create DNS Zone' and contains the following fields and options:

- Select Zone Type:** Radio buttons for 'Create New Zone' (selected) and 'Create IN-ADDR ARPA'.
- Specify eDirectory Context:** Text field containing 'novell.dsflw'.
- Enter the Zone Domain Name:** Text field containing 'win2003ad.com'.
- Select the Zone Type:** Radio buttons for 'Primary', 'Forward' (selected), and 'Secondary'.
- Enter Name Server IP Address:** A series of five input boxes for IP address entry, with an 'IPv6' checkbox to the right.
- Select Assigned Authoritative Zone Server:** A dropdown menu showing 'DNS\_oes-dc-1.novell.dsflw'.
- Name Server Information:** A section with 'Enter Host Name:' and an empty text field.
- Select Domain:** A text field with an 'Add' button next to it.

At the bottom of the form are three buttons: 'Create', 'Cancel', and 'Help'.

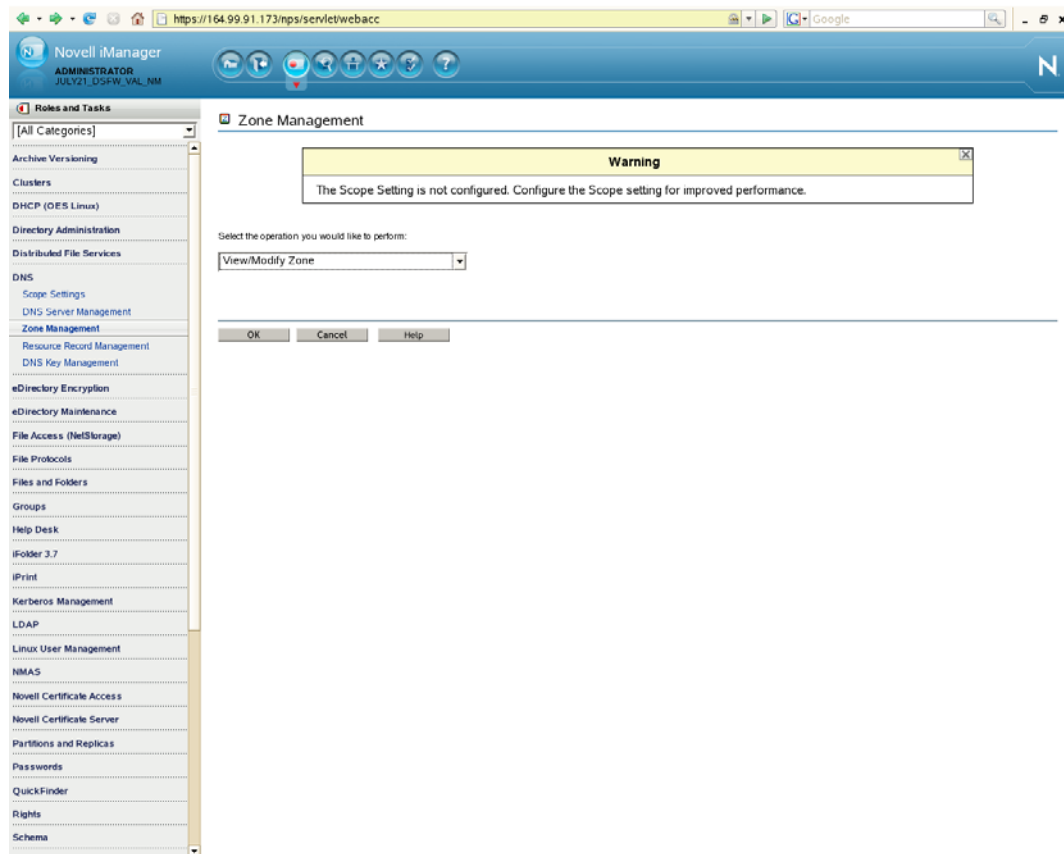
- 3a Specify a name for the zone; that is, the domain name of the Active Directory forest (in this example, it is win2003ad.com).
- 3b Specify the eDirectory context for the zone or browse to select it; that is, the container containing the DNS related objects (In this example, it is novell.dsflw).
- 3c Select the Zone Type as *Forward*.
- 3d Select a DNS server from the *Assigned Authoritative DNS Server* drop-down list. This is the name of the DNS server object. In this example, it is DNS\_oes-dc-1.novell.dsflw. This parameter is optional.

**3e** Click *Create*. A message indicates that the new forward zone has been created.

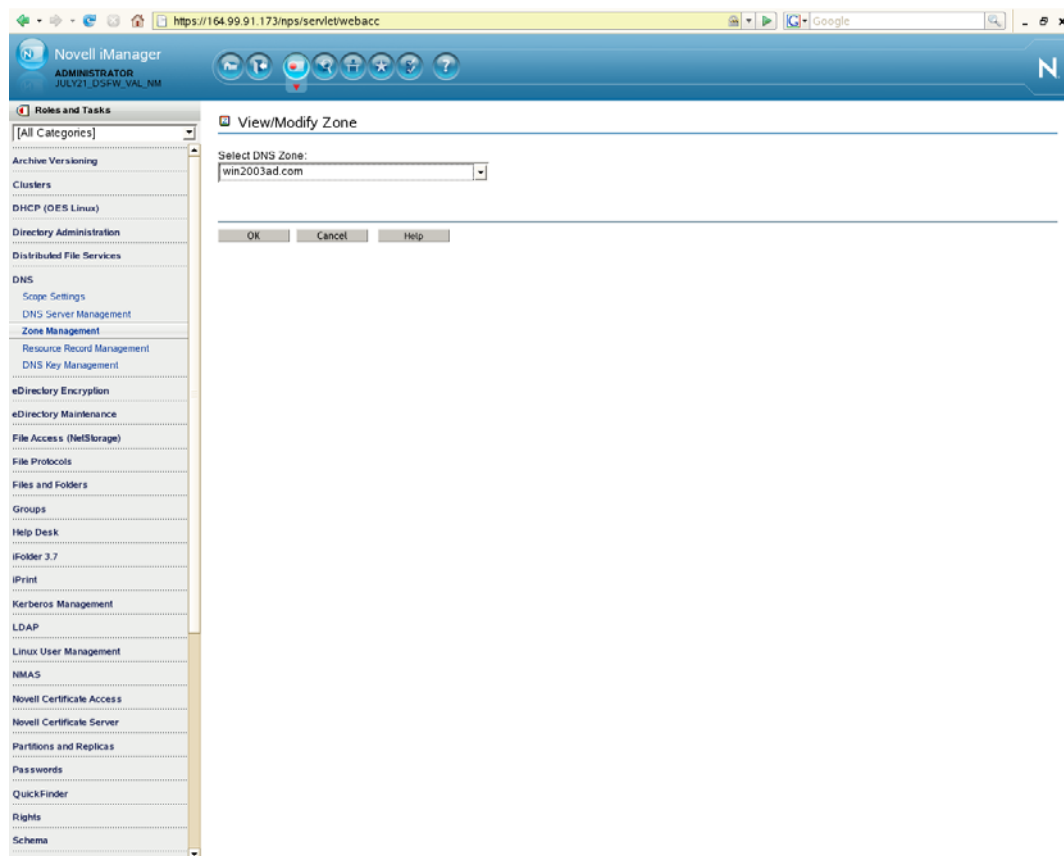




- 4 Select *Zone Management* from the iManager DNS plug-in, then select *View/Modify Zone* from the drop-down list and click *OK*.



- 5 Select Active Directory forest's domain zone from the drop-down list, then click *OK*.



## 6 Click *Next*.

The screenshot shows the Novell iManager web interface. The left sidebar contains a 'Roles and Tasks' menu with categories like 'Archive Versioning', 'Clusters', 'DHCP (OES Linux)', 'Directory Administration', 'Distributed File Services', 'DNS', 'eDirectory Encryption', 'eDirectory Maintenance', 'File Access (NetStorage)', 'File Protocols', 'Files and Folders', 'Groups', 'Help Desk', 'iFolder 3.7', 'iPrint', 'Kerberos Management', 'LDAP', 'Linux User Management', 'NMAAS', 'Novell Certificate Access', 'Novell Certificate Server', 'Partitions and Replicas', 'Passwords', 'QuickFinder', 'Rights', and 'Schema'. The 'DNS' category is expanded, showing sub-items: 'Scope Settings', 'DNS Server Management', 'Zone Management' (highlighted), 'Resource Record Management', and 'DNS Key Management'. The main content area is titled 'View/Modify Zone'. It shows the 'Selected DNS Zone' as 'win2003ad.com'. Under 'Select the Zone Type:', the 'Forward' radio button is selected. Below this is a field for 'Enter the Zone Master IP Address:'. There are two list boxes: 'Available DNS Server(s):' and 'Selected Authoritative DNS Server(s):'. The 'Selected' box contains 'DNS\_oes-dc-1.novell.dsfw'. Between the boxes are buttons for 'Add', 'Remove', 'Add All', and 'Remove All'. Below these is a 'Specify Designated Forwarder DNS Server:' dropdown menu, currently set to 'DNS\_oes-dc-1.novell.dsfw'. At the bottom is a text area for 'Enter Comments:'. Navigation buttons at the bottom include '<< Previous', 'Next >>', 'Cancel', and 'Help'.

Novell iManager  
ADMINISTRATOR  
JULY21\_05FW\_VAL\_NM

Roles and Tasks  
[All Categories]

View/Modify Zone

Selected DNS Zone: win2003ad.com

Select the Zone Type:

☐ Primary  
☒ Forward  
☐ Secondary

Enter the Zone Master IP Address:

Available DNS Server(s):

Selected Authoritative DNS Server(s):  
DNS\_oes-dc-1.novell.dsfw

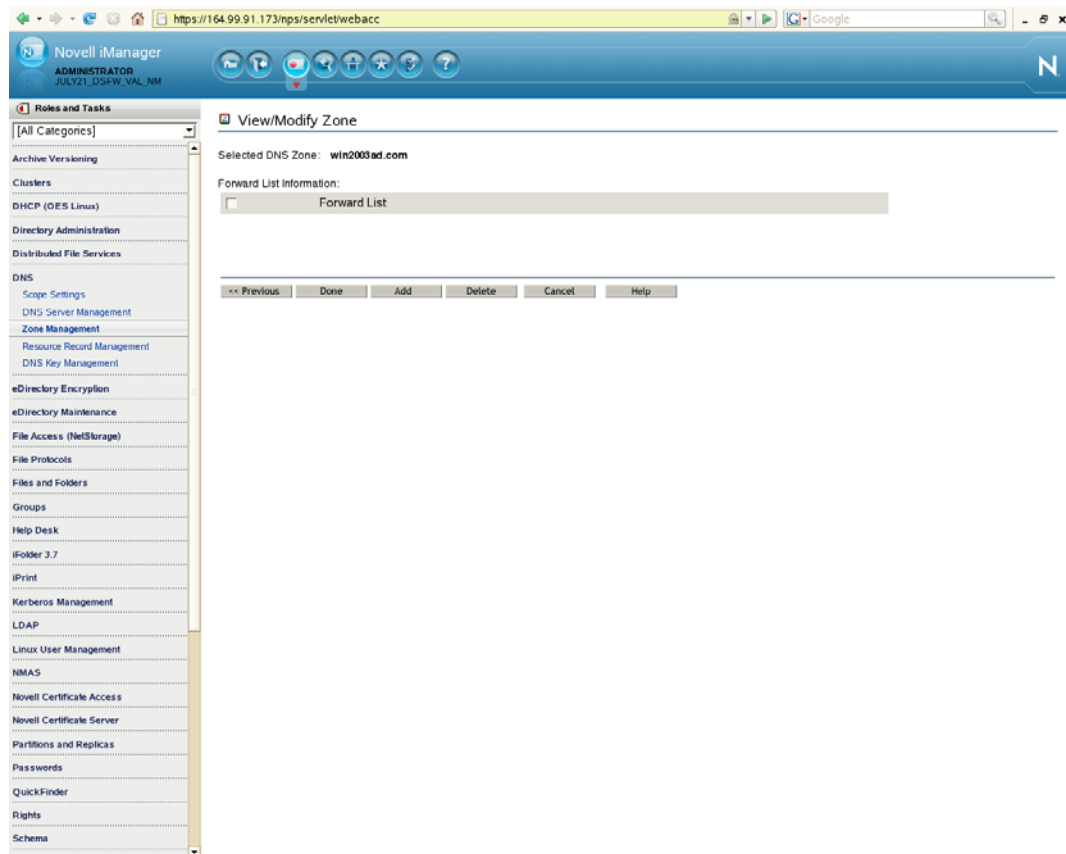
Buttons: Add, Remove, Add All, Remove All

Specify Designated Forwarder DNS Server:  
DNS\_oes-dc-1.novell.dsfw

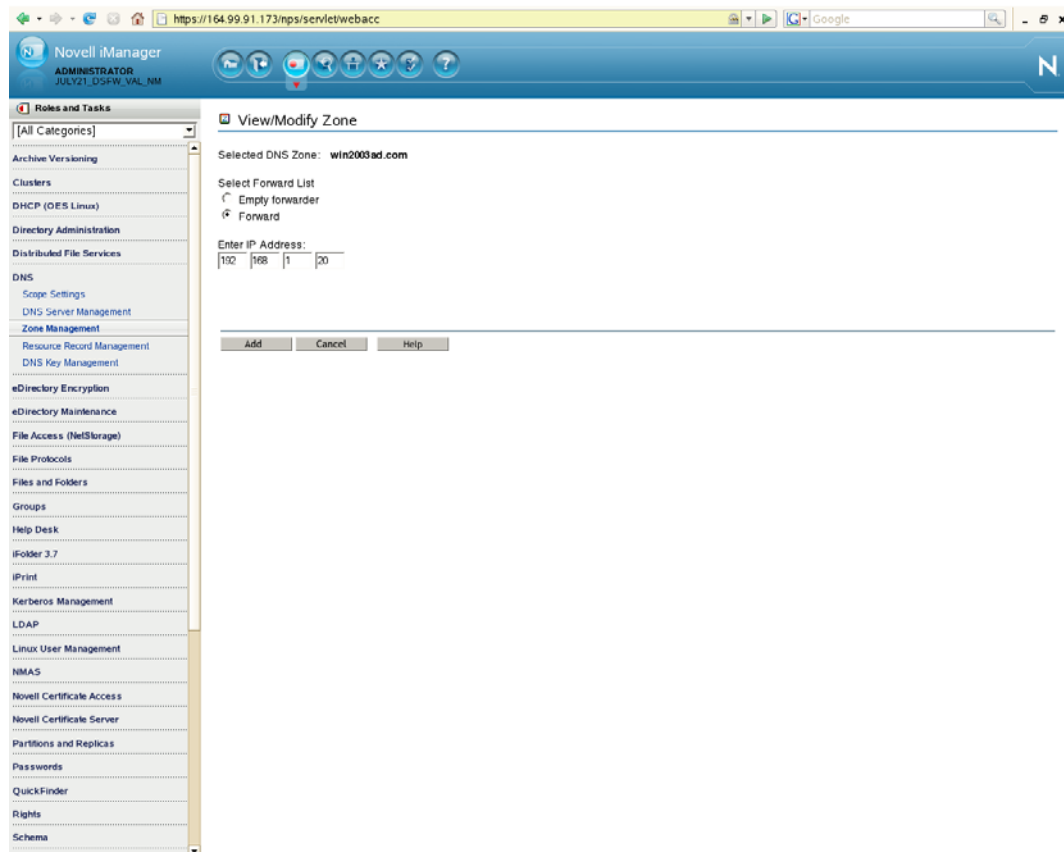
Enter Comments:

<< Previous   Next >>   Cancel   Help

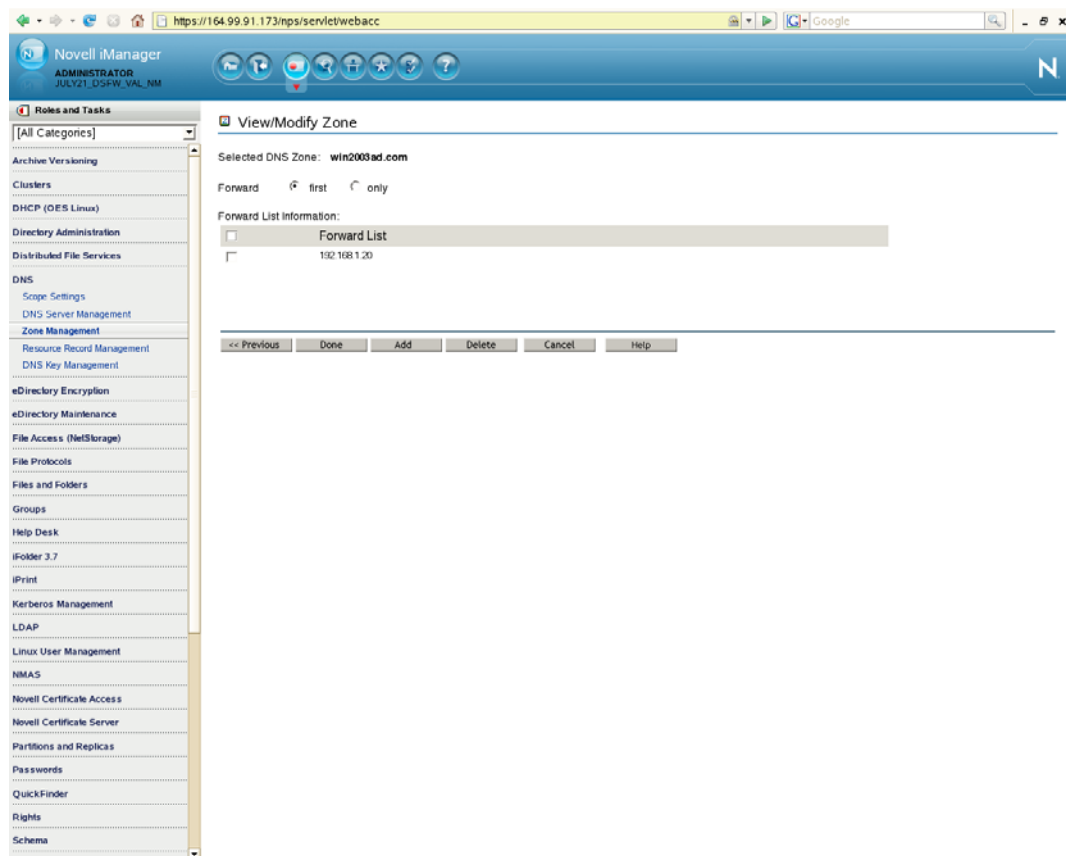
## 7 Click *Add*.



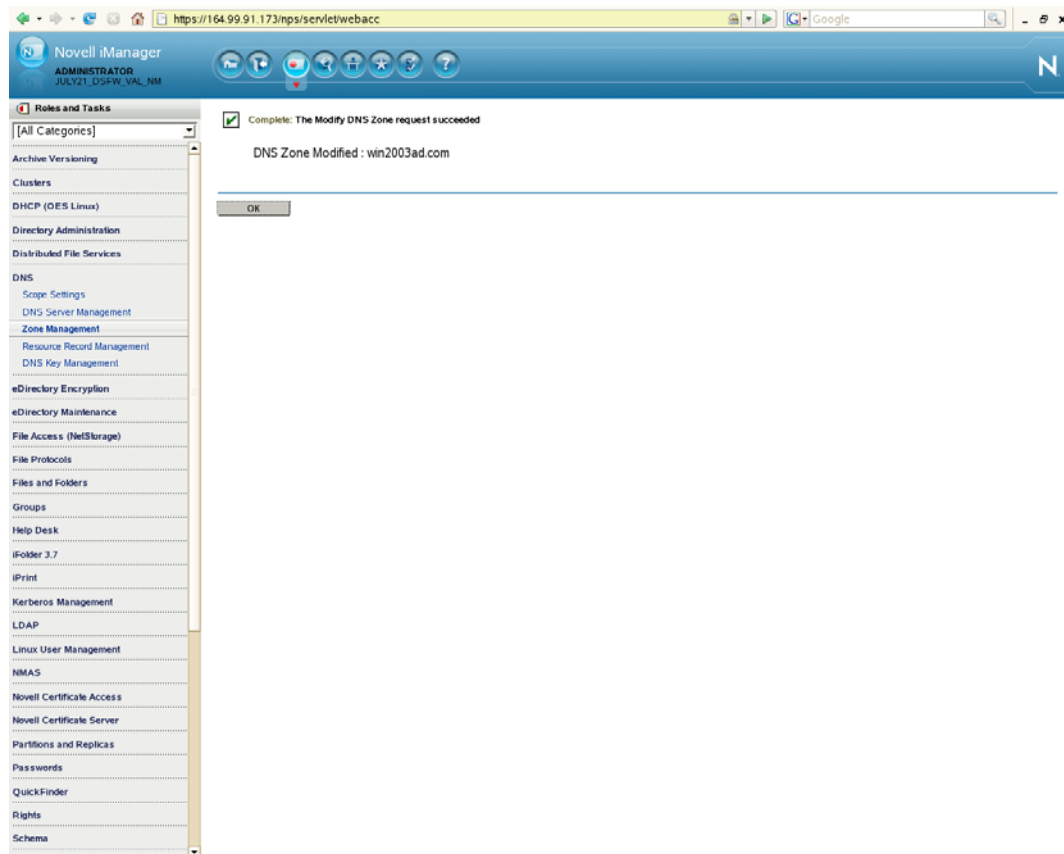
- 8 Select the *Forward* option, then specify the IP address of Active Directory forest's DNS server (in the example, it is 192.168.1.20). Click *Add*.



## 9 Click *Done*.



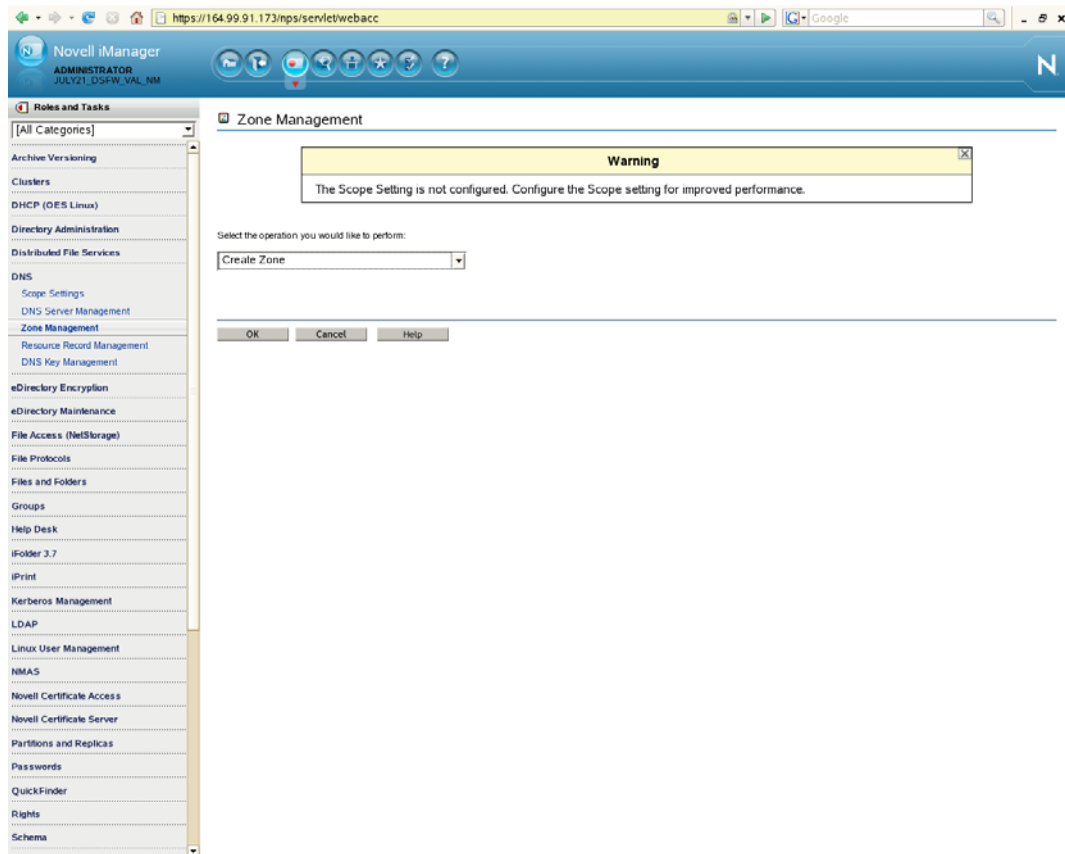
- 10 A message indicates that the new secondary zone has been created. Click *OK*.



## Configuring the Reverse Lookup Zone Forwarder

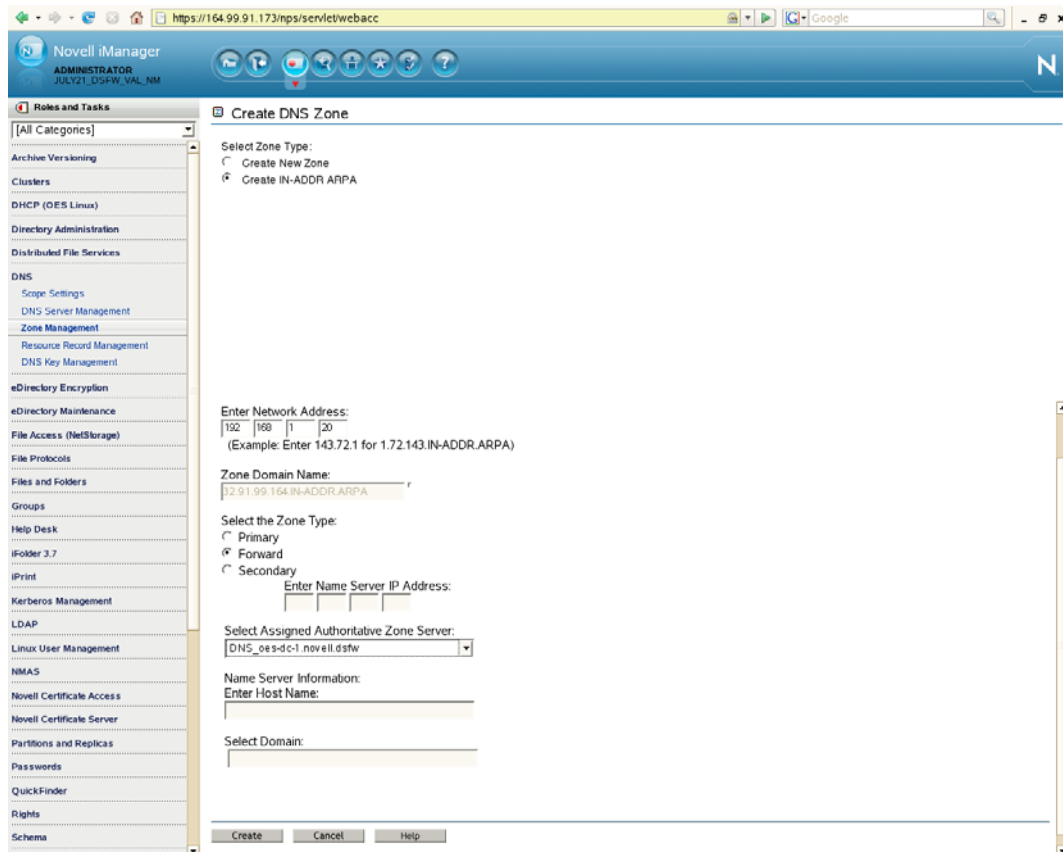
You need to configure a DNS reverse lookup zone for DSfW for a Windows domain.

- 1 After selecting *Zone Management* from the iManager DNS plug-in, select the *Create Zone* option from the drop-down list. Click *OK* to open the Create DNS Zone window.

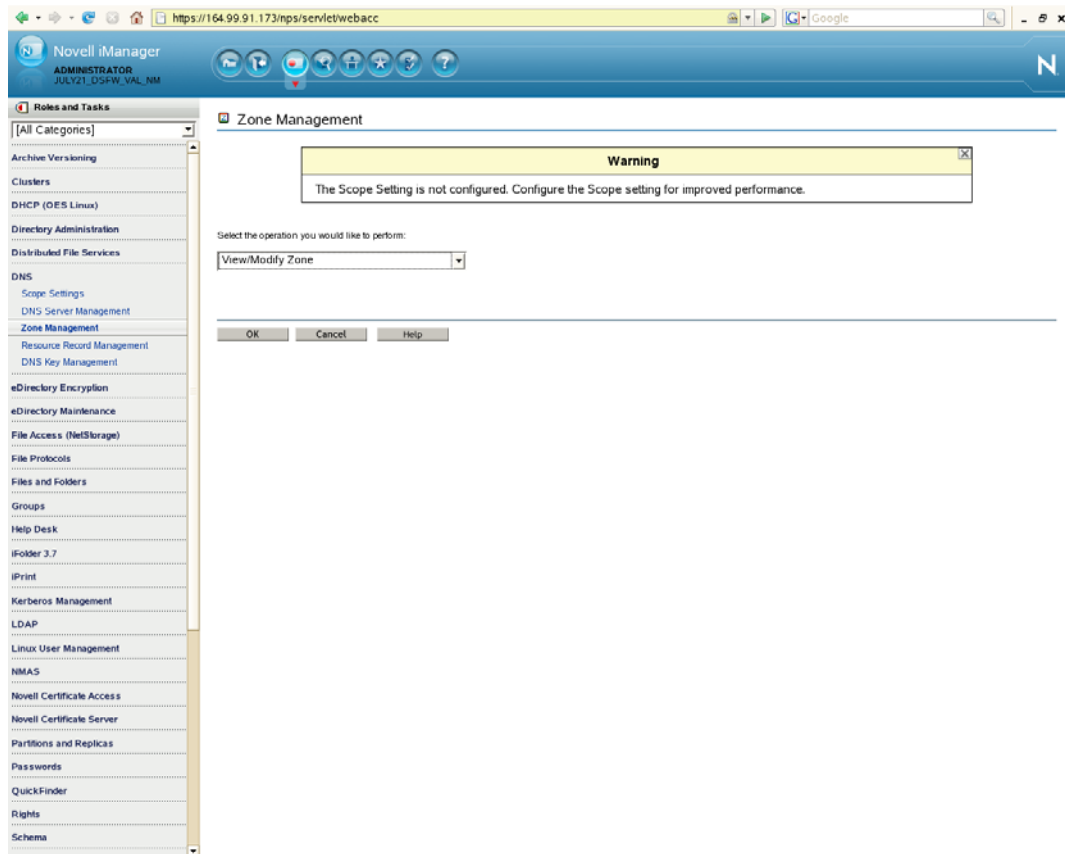


2 Specify the DNS configuration parameters as follows:

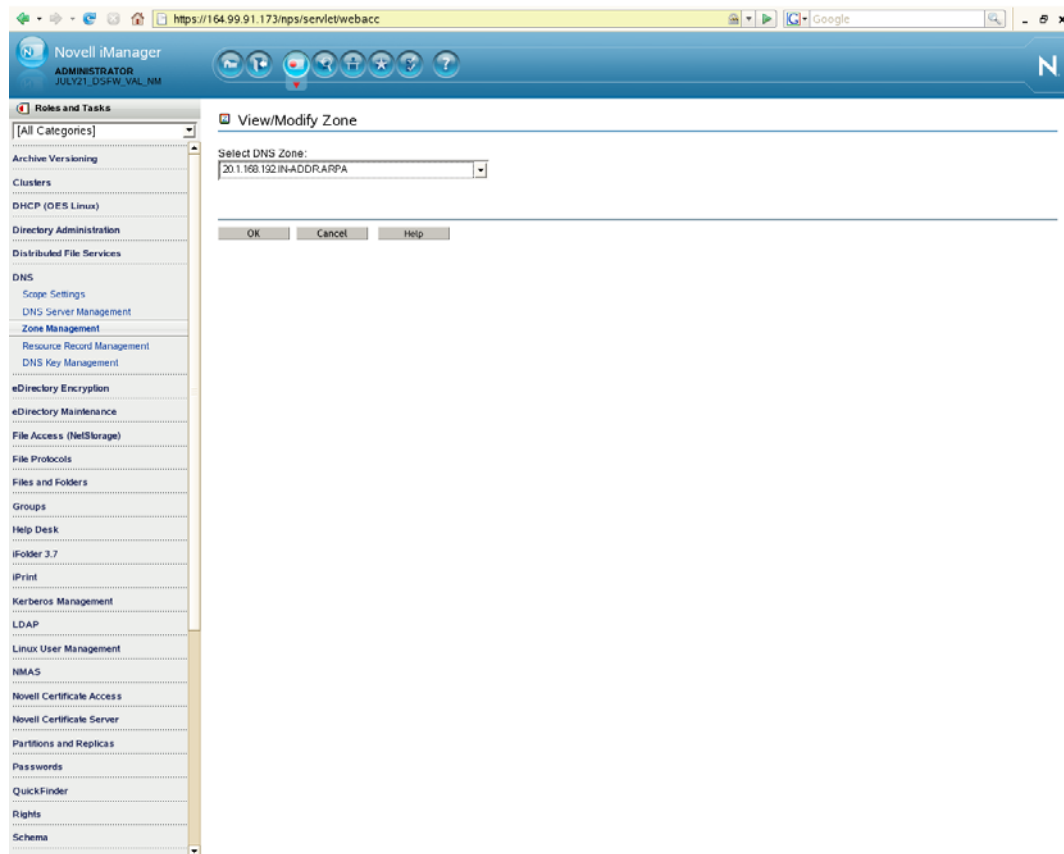




- 2a Select the Create IN-ADDR ARPA option as the *Zone Type*.
  - 2b Specify the network address. This is the IP address of the Active Directory forest's DNS server (in this example, it is 192.168.1.20).
  - 2c Select Forward as the *Zone Type*.
  - 2d Select a DNS server from the *Assigned Authoritative DNS Server* drop-down list. This is the name of the DNS server object (in this example, it is DNS\_oes-dc-1.novell.dsffw).
  - 2e Click *Create*. A message indicates that the zone has been created.
- 3 Select *Zone Management* from the iManager DNS plug-in, then select the *View/Modify Zone* option from the drop-down list and click *OK*.



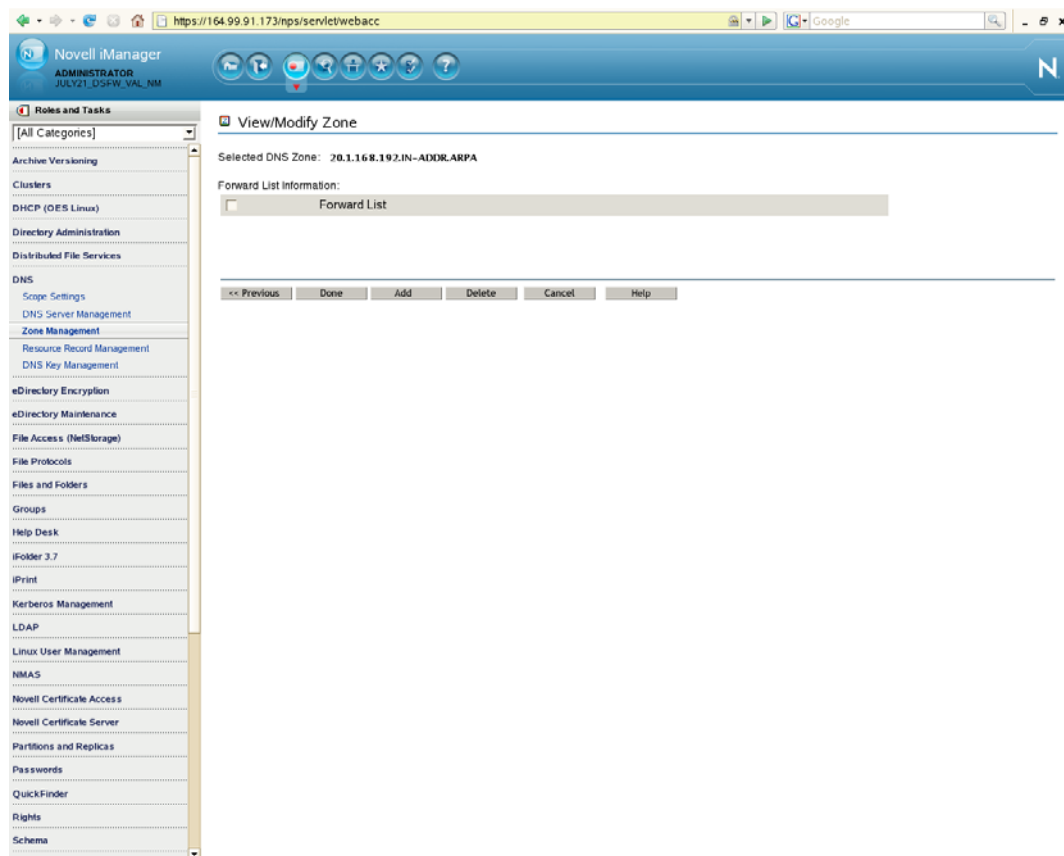
- 4 Select the Active Directory forest's reverse lookup zone from the drop-down list, then click *OK*.



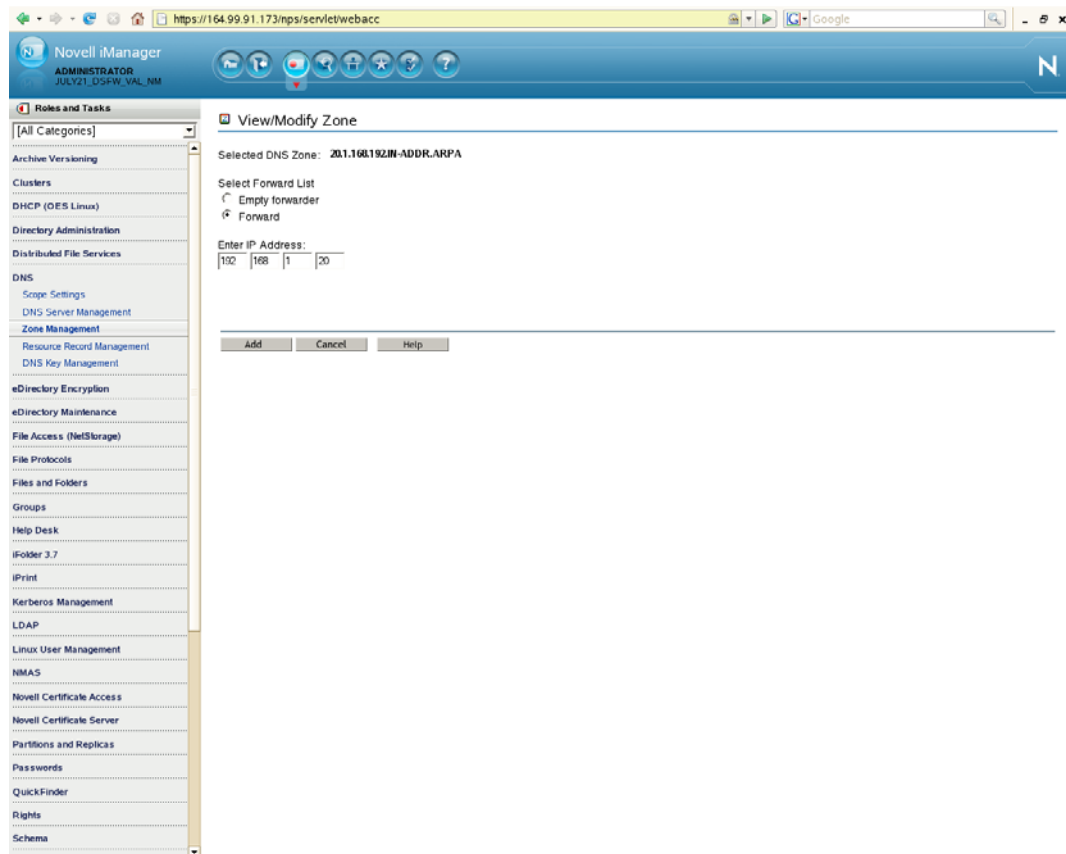
5 Click *Next*.

The screenshot shows the Novell iManager web interface. The browser address bar displays `https://164.99.91.173/nps/servlet/webacc`. The page title is "Novell iManager" with the user "ADMINISTRATOR" and session "JULY21\_05FW\_VAL\_NM". The left sidebar contains a "Roles and Tasks" menu with categories like "Archive Versioning", "Clusters", "DHCP (OES Linux)", "Directory Administration", "Distributed File Services", "DNS", "eDirectory Encryption", "eDirectory Maintenance", "File Access (NetStorage)", "File Protocols", "Files and Folders", "Groups", "Help Desk", "iFolder 3.7", "iPrint", "Kerberos Management", "LDAP", "Linux User Management", "NMAS", "Novell Certificate Access", "Novell Certificate Server", "Partitions and Replicas", "Passwords", "QuickFinder", "Rights", and "Schema". The "DNS" category is expanded, showing sub-items: "Scope Settings", "DNS Server Management", "Zone Management" (selected), "Resource Record Management", and "DNS Key Management". The main content area is titled "View/Modify Zone". It shows the "Selected DNS Zone" as "20.1.168.192.IN-ADDR.ARPA". Under "Select the Zone Type:", the "Forward" radio button is selected. Below this is a field for "Enter the Zone Master IP Address:". There are two list boxes: "Available DNS Server(s)" and "Selected Authoritative DNS Server(s)". The "Selected" list contains "DNS\_oes-dc-1.novell.dsfw". Between the lists are buttons for "Add", "Remove", "Add All", and "Remove All". Below the lists is a "Specify Designated Forwarder DNS Server:" dropdown menu, currently set to "DNS\_oes-dc-1.novell.dsfw". At the bottom is a text area for "Enter Comments:". Navigation buttons at the bottom include "<< Previous", "Next >>", "Cancel", and "Help".

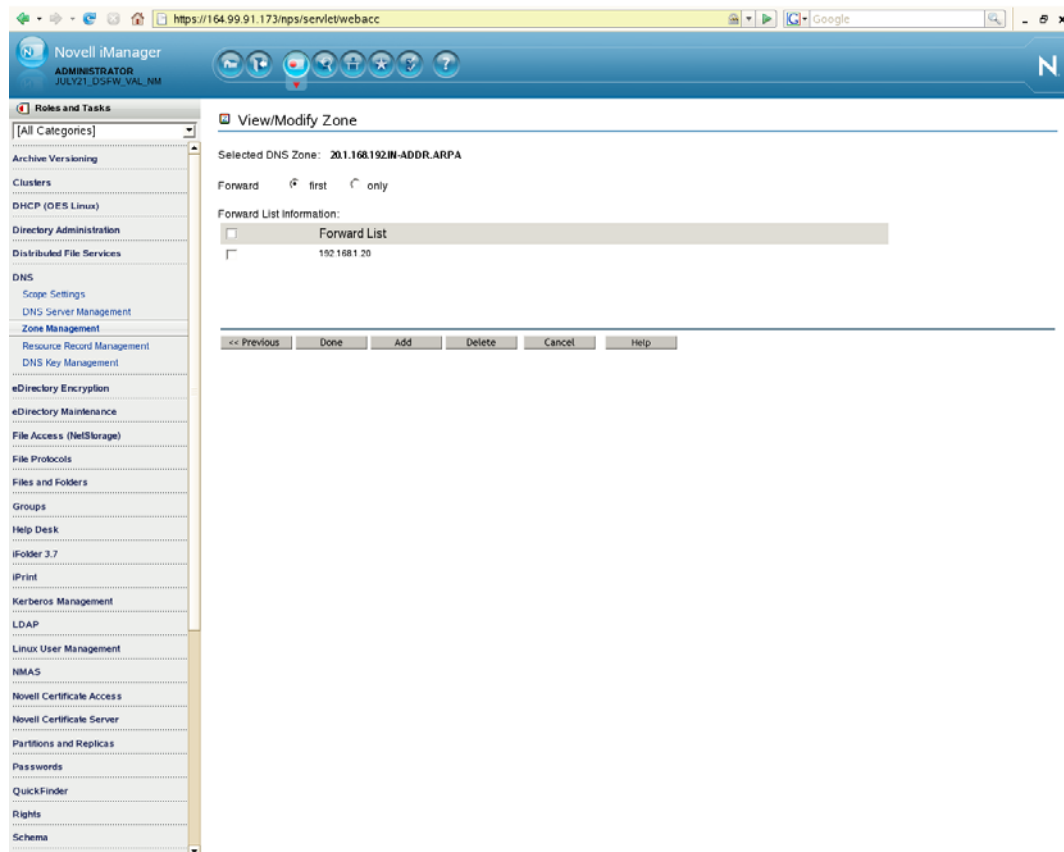
6 Click *Add* to add this DNS server object.



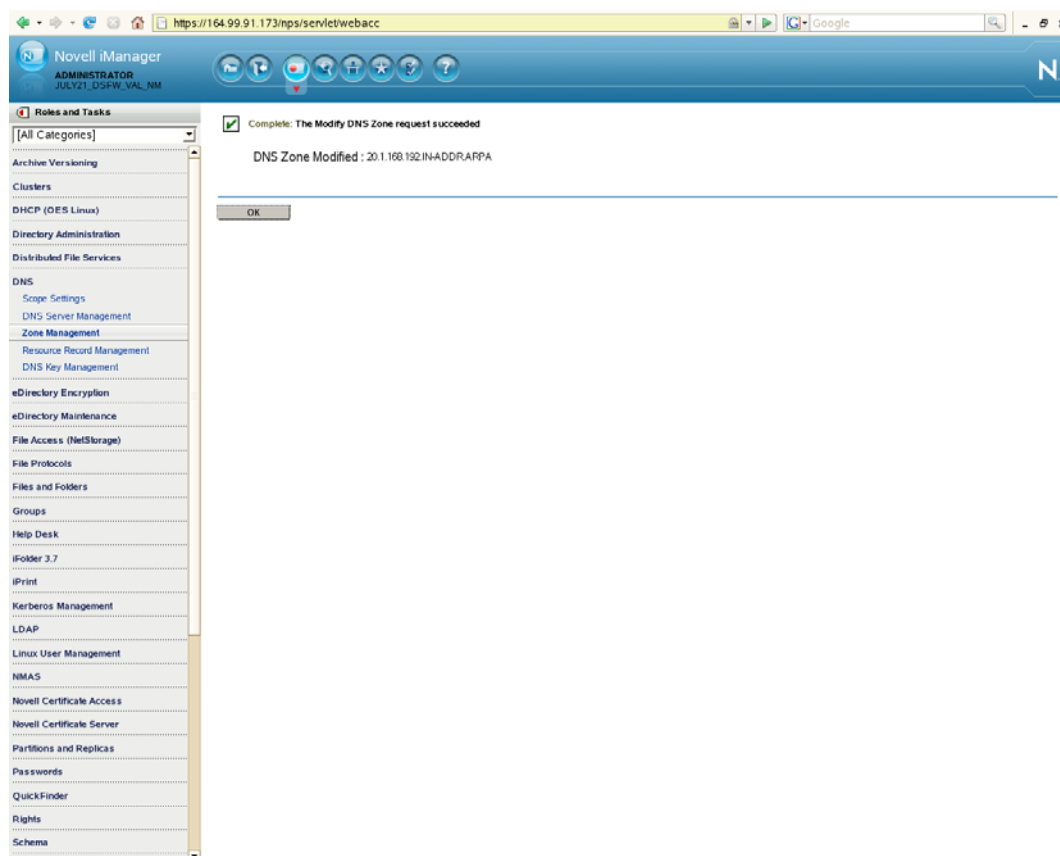
7 Select *Forward List* and click *Add*.



- 8 Select the *Forward* option and specify the IP address of Active Directory forest's DNS server (192.168.1.20 in this example). Click *Add*, then click *Done*.



- 9 A message indicates that a zone has been created. Click *OK*.



- 10 Verify the DNS configuration by trying to resolve the Active Directory domain and its DNS SRV records using `nslookup`, as follows:

```
nslookup -query=any _ldap._tcp.dc._msdcs.<AD domain name>
```

For example:

```
# nslookup -query=any _ldap._tcp.dc._msdcs.win2003ad.com
Server: 192.168.1.10
Address: 192.168.1.10#53

Non-authoritative answer:
_ldap._tcp.dc._msdcs.win2003ad.com service = 0 100 389 osg-dtsrv22.
win2003ad.com.
```

Authoritative answers can be found from:

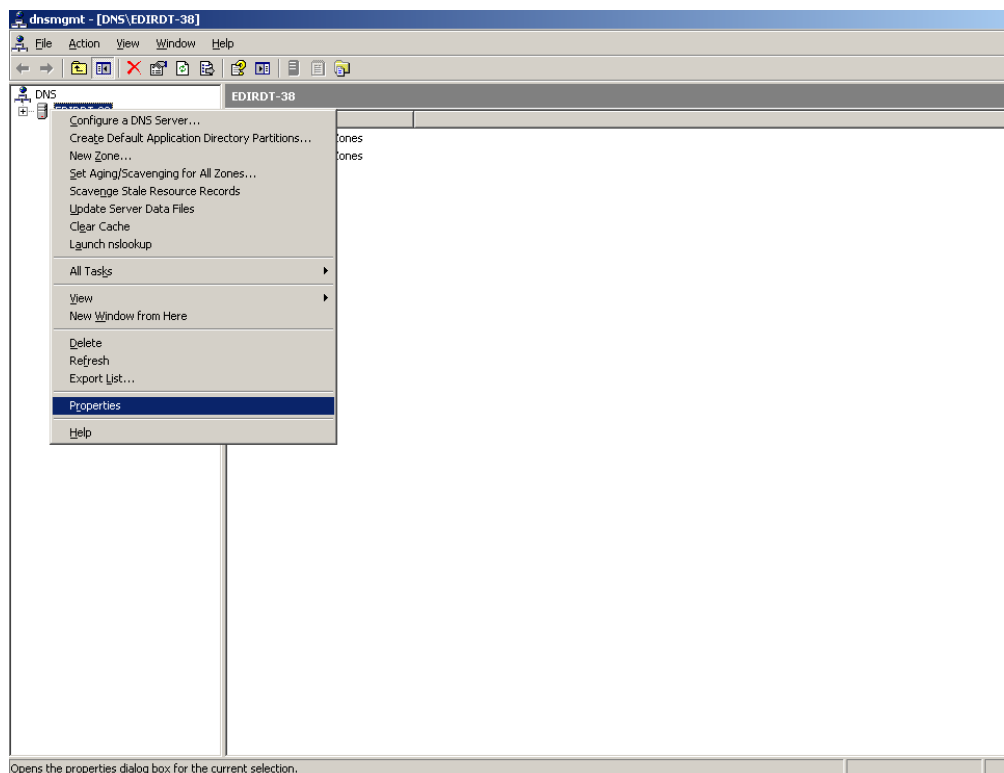
```
osg-dt-srv22.win2003ad.com internet address = 192.168.1.20
```



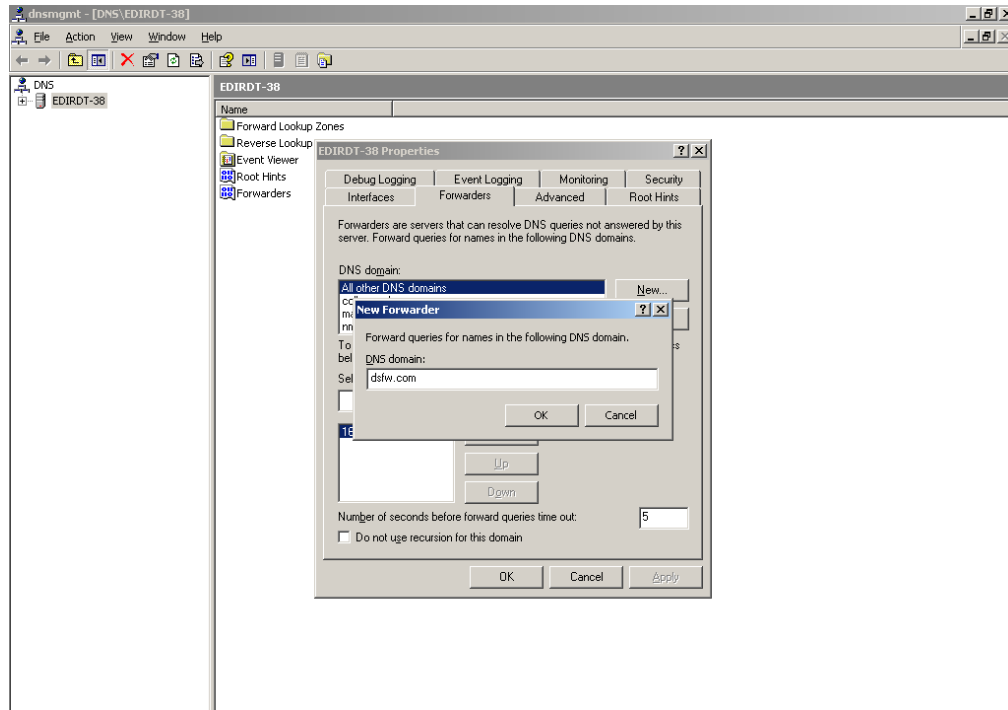
## Configuring the DNS Forward Lookup Zone on the Active Directory Server

To resolve the DSfW forest from the Active Directory forest, you must either create a forward lookup stub zone or a forwarder on the Active Directory forest's DNS server. Use the following steps to create a forwarder for DSfW on the Active Directory DNS server:

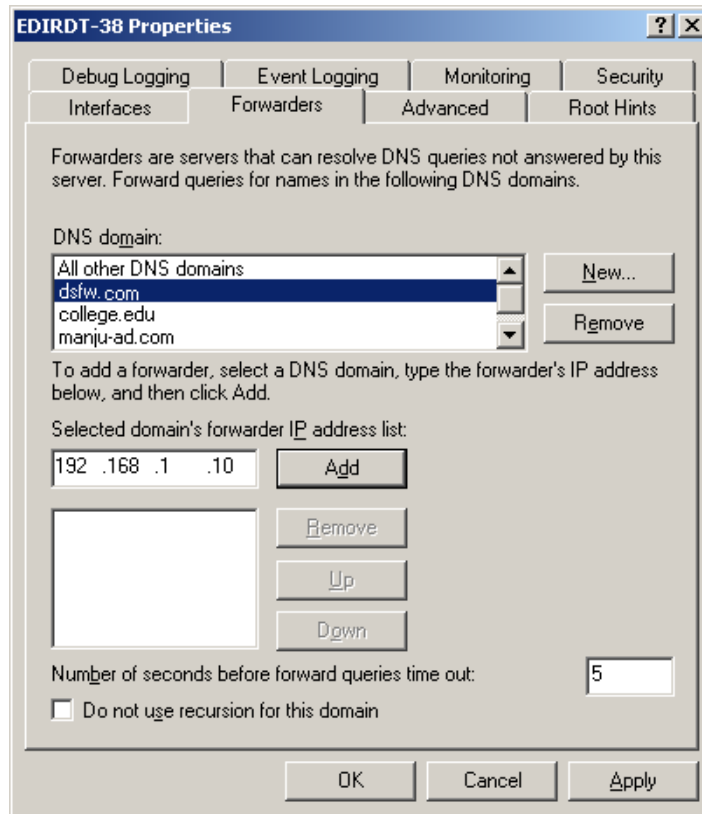
- 1 At your Windows management workstation, click *Start>Run*, enter *mmc* in the text field and click *OK*.
  - 1a Click *File>Add/Remove snap-in*, click *Add* and select DNS snap-in, then click *Add*. Click *Close* to close the window and then click *OK*.



- 1b** Select the *Forwarders* tab, then click *New* and add a new forwarder for the DSfW domain. Specify the DSfW domain name and click *OK*.

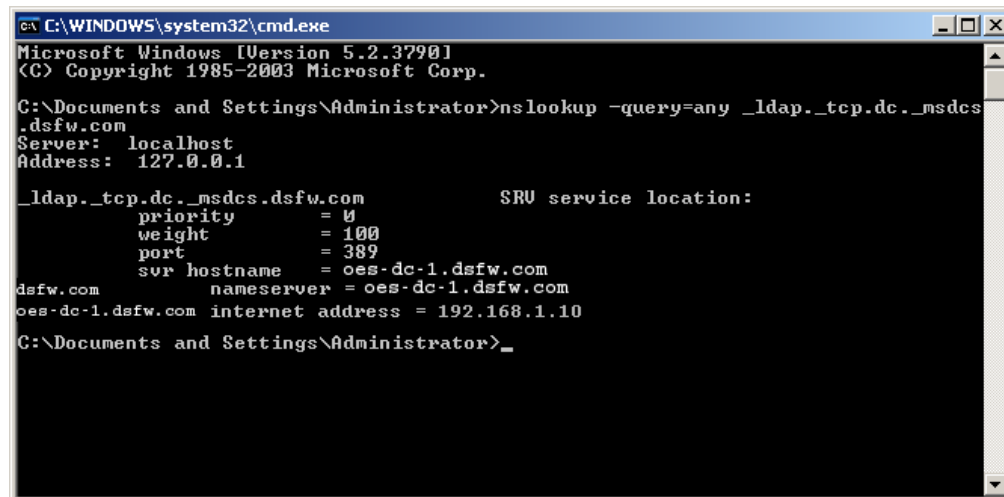


- 1c** Select the new forwarder, specify the IP address of the DNS server of the DSfW domain, then click *Add*.



- 1d** Verify the DNS configuration by using nslookup to resolve the Active Directory domain and its DNS SRV records, as follows:

```
nslookup -query=any _ldap._tcp.dc._msdcs.<DSFW domain name>
```

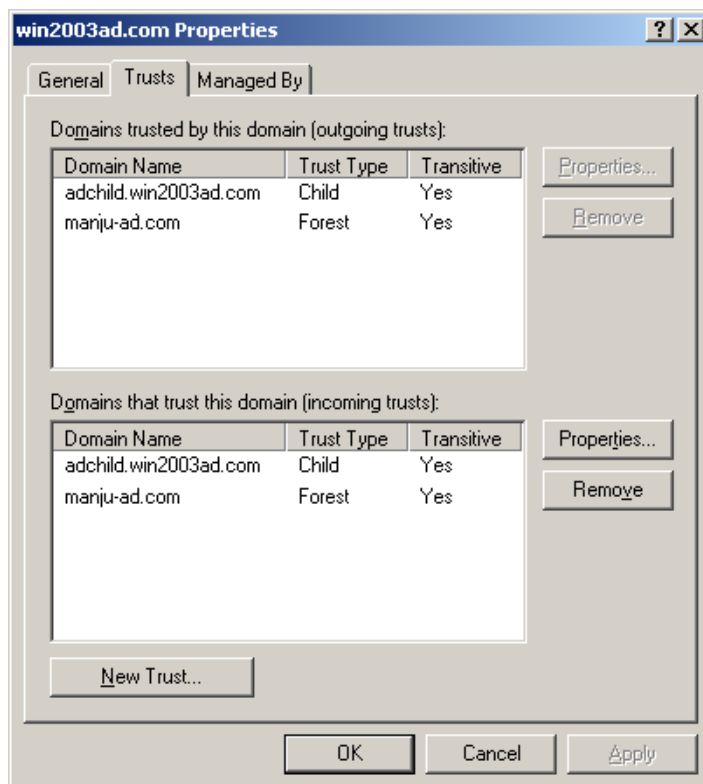


For more information on DNS settings, refer to the [Section 2.2, “DNS Settings in a DSfW Environment,”](#) on page 18.

- 2 If the Active Directory domain's Domain Functional Level is not Windows Server 2003, do the following to raise it:
  - 2a Open Active Directory Domains and Trusts snap-in from the MMC.
  - 2b Right-click the icon representing the Active Directory domain, select *Raise Domain Functional Level* from the menu, then set it to *Windows Server 2003*.
- 3 If the Active Directory forest's Forest Functional Level is not Windows Server 2003, do the following to raise it:
  - 3a Right-click the Active Directory Domains and Trusts snap-in from MMC.
  - 3b Select *Raise Domain Functional Level* from the menu and set it to *Windows Server 2003*.

## Creating the Trust

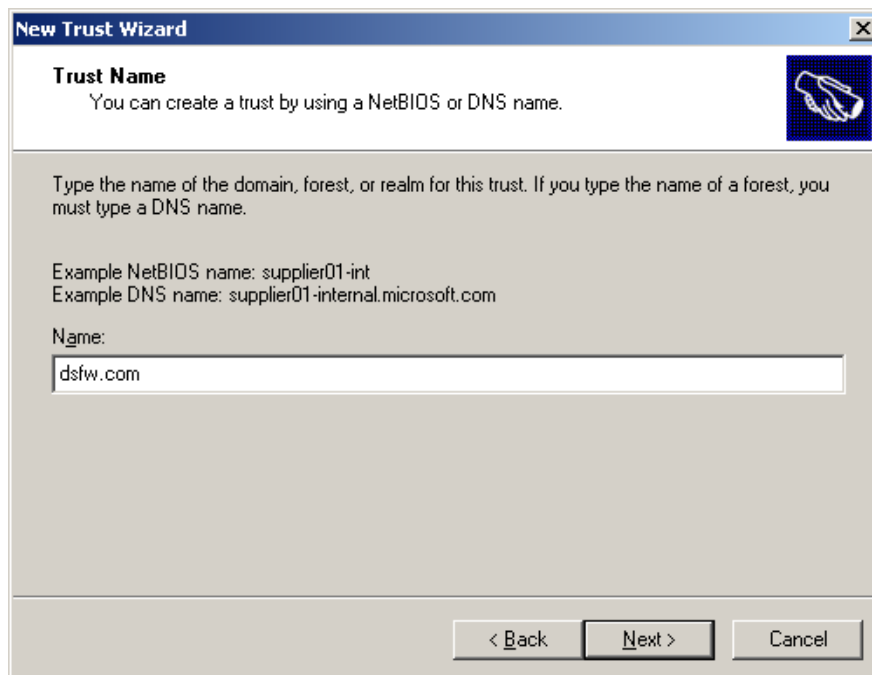
- 1 At your Windows management workstation, click *Start>Run*, enter mmc in the text field and click *OK*.
- 2 Click *File>Add/Remove snap-in*, click *Add* and select Active Directory Domains and Trusts snap-in, then click *Add*.
- 3 Click *Close*, then click *OK*.
- 4 Right-click the DSfW domain, then select *Properties*.
- 5 Select *New Trust* from the *Trusts* tab, then click *OK*.



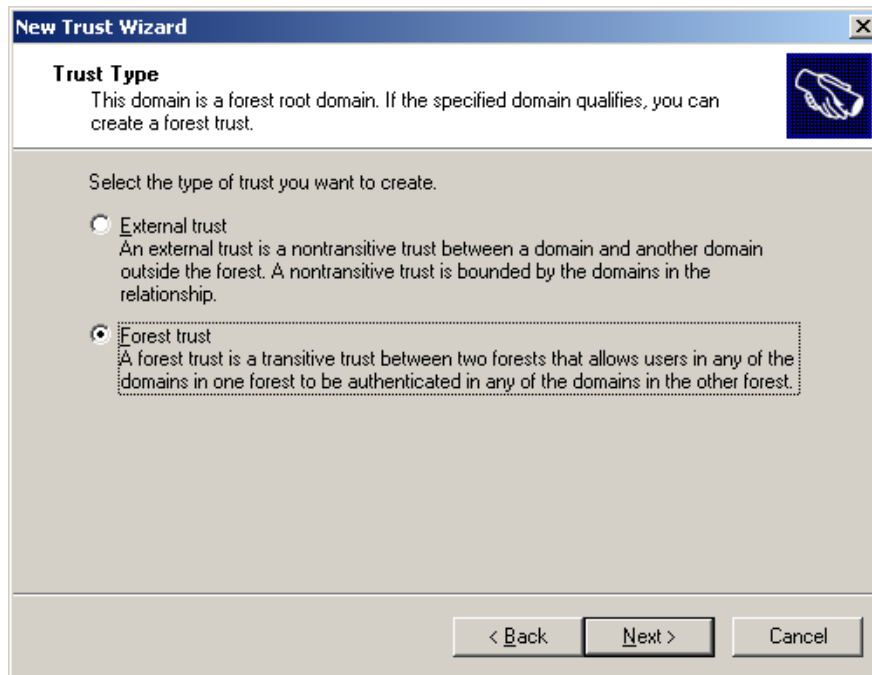
6 Click *Next* to start creating a new trust.



7 Specify the DNS name (or NetBIOS name) of the Active Directory forest, then click *Next*.

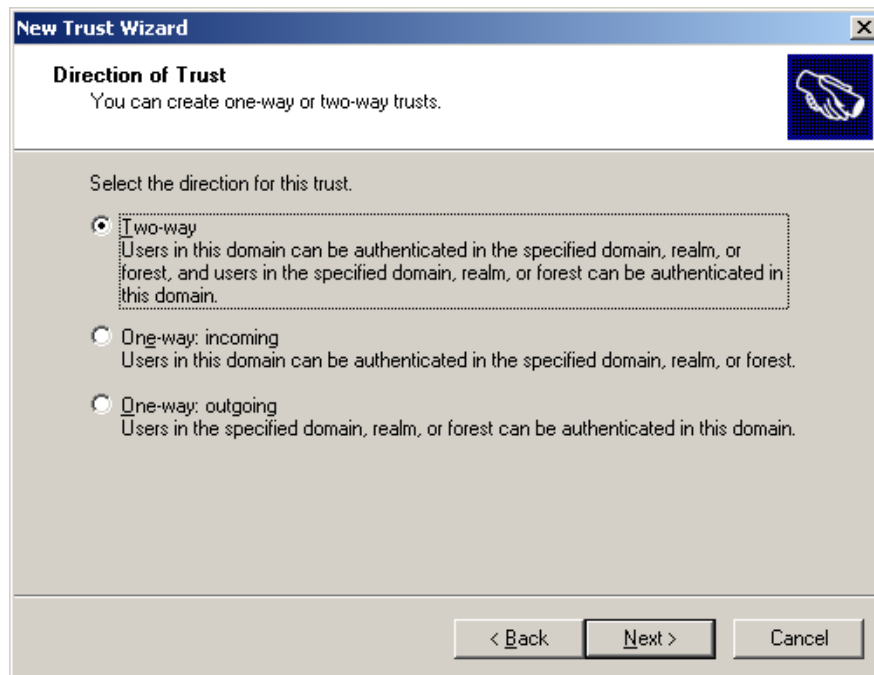


8 Select *Forest trust*, then click *Next*.



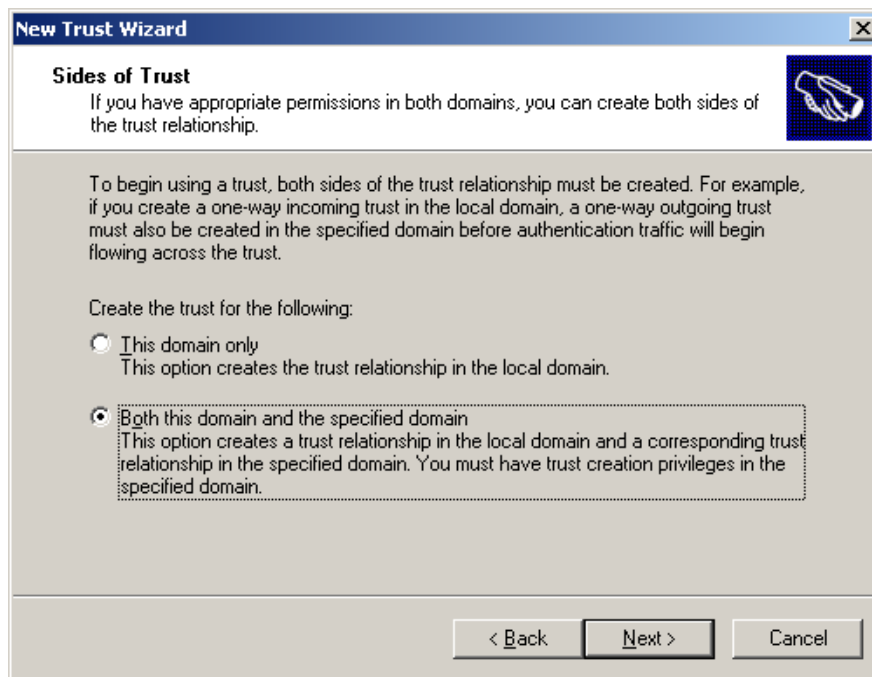
9 To select the direction of trust, do one of the following:

- ♦ Click *Two-way* to create a two-way forest trust.
- ♦ Click *One-way:incoming* to create a one-way incoming forest trust.
- ♦ Click *One-way:outgoing* to create a one-way outgoing forest trust.

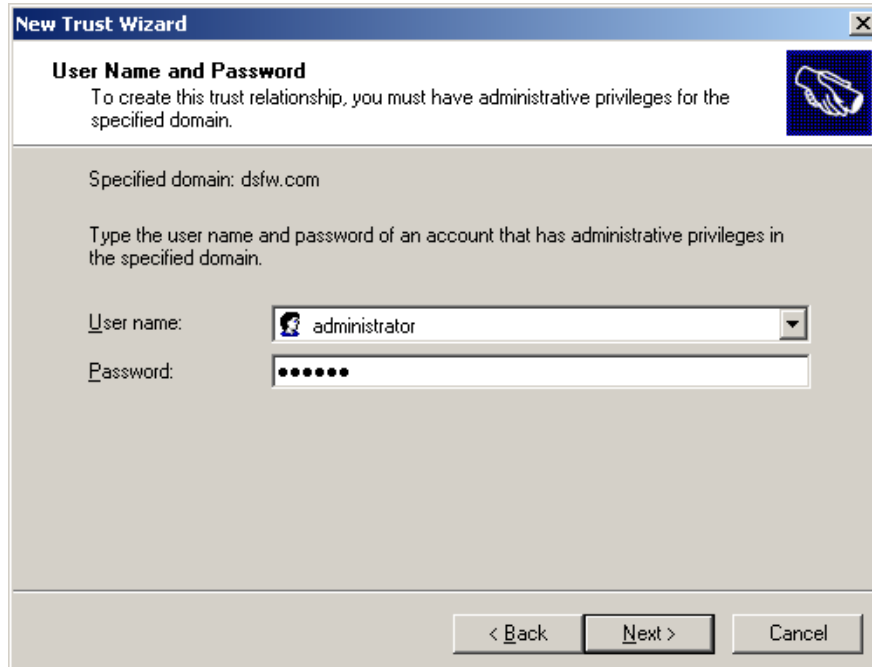


10 Click *Next*.

- 11 Select *Both this domain and the specified domain* and click *Next*.



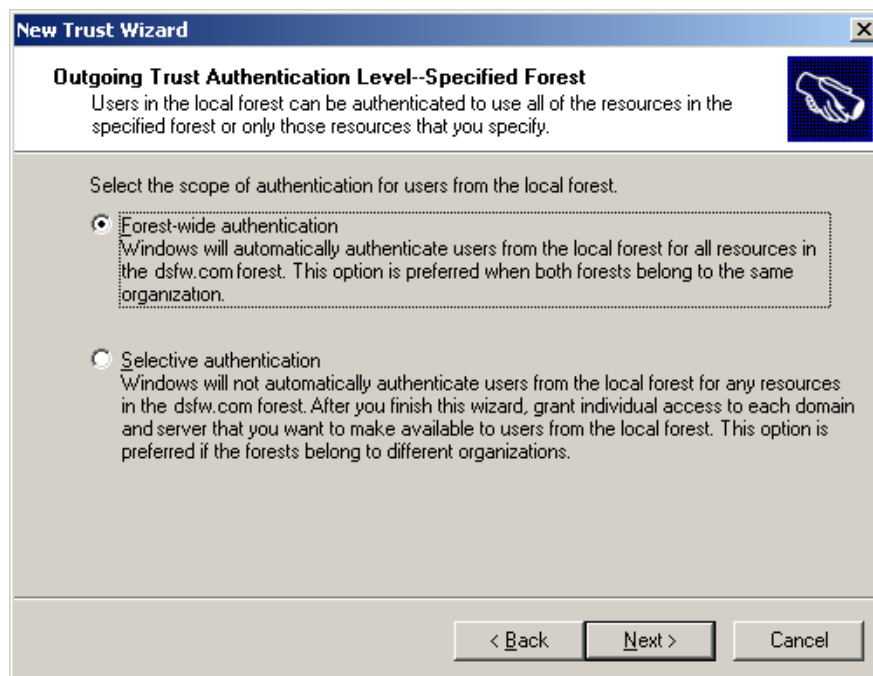
- 12 Specify the user name and password of the Active Directory domain administrator, then click *Next*.



- 13 Select *Forest-wide authentication* to authorize users to use resources in the local forest or those identified by the administrator, then click *Next*.

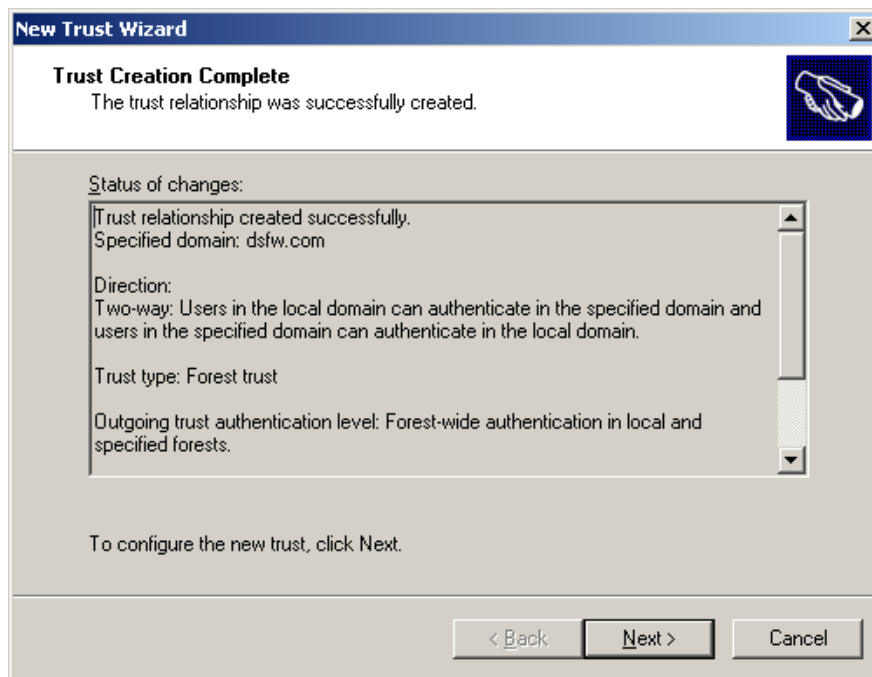


- 14 Select *Forest-wide authentication* to authenticate Active Directory forest users to use resources in the dsfw.com forest or those identified by the administrator, then click *Next*.

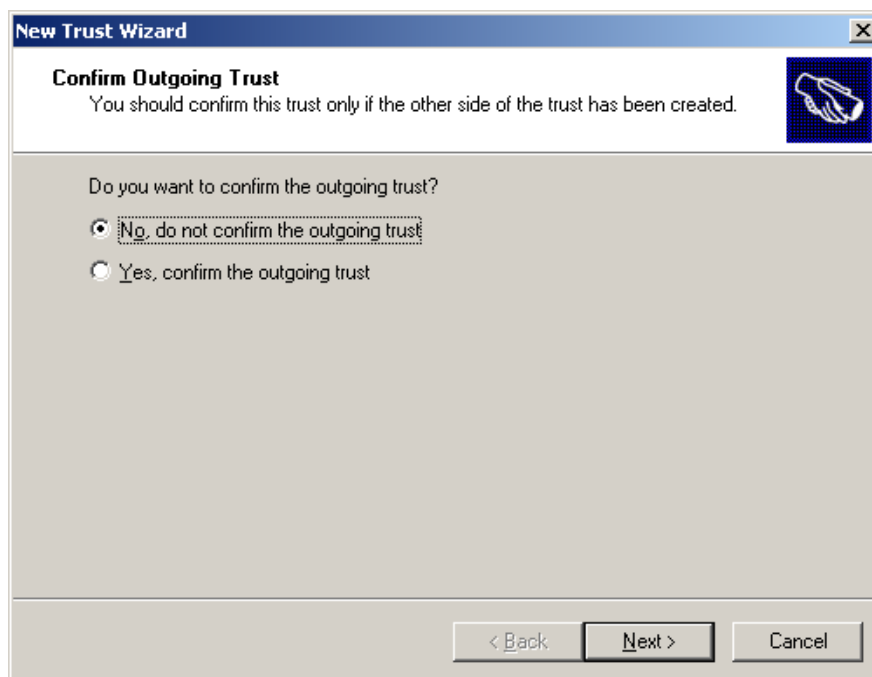




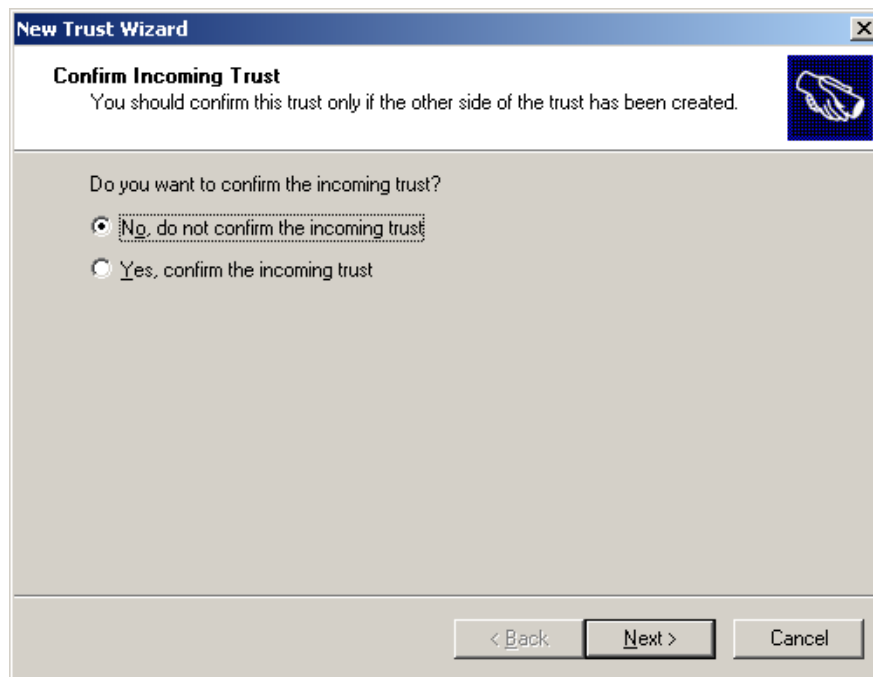
- 15 Review the trust settings and complete the creation of trust by clicking *Next*.



- 16 Click any option depending on your choice, then click *Next*.



- 17 Click any option depending on your choice, then click *Next*.

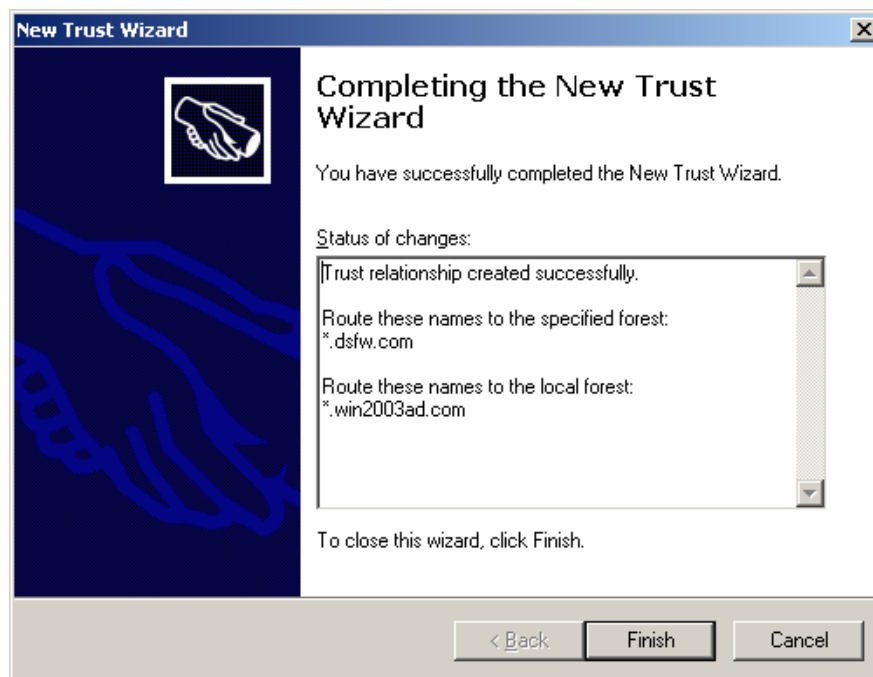


---

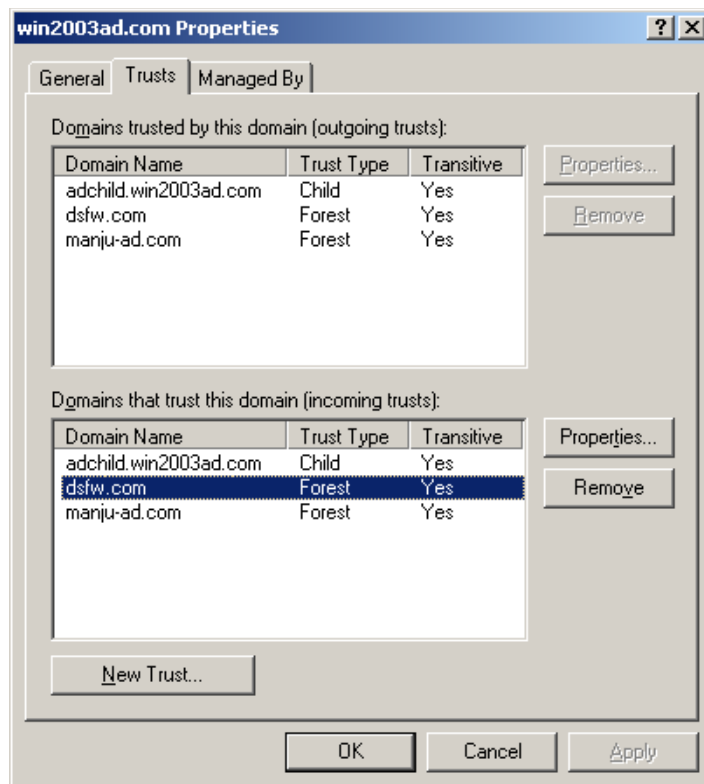
**NOTE:** In **Step 16** and **Step 17**, if you select Yes option to confirm the trust, ensure that you validate the trust later by selecting *Properties>Validate* option.

---

- 18 Complete the trust creation by clicking *Finish*.



19 The new domain summary appears in the Trusts page.



## Verifying the Trust

To verify that the DNS configuration is correct:

- 1 Verify that the *Log on to* drop-down list in the Login window of a Windows machine that is joined to the Domain Services for Windows domain has an entry for the Active Directory domain.
- 2 Try to log on to the Windows machine that is joined to the Domain Services for Windows domain with an Active Directory domain user principal name.
- 3 Verify that the *Log on to* field in the Login window of a Windows machine that is joined to the Active Directory domain has an entry for the Domain Services for Windows domain.
- 4 Try to log on to the Windows machine that is joined to the Active Directory domain with a Domain Services for Windows domain user principal name.

For more information, refer to the [Microsoft Active Directory documentation \(http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.aspx\)](http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.aspx).

## 6.2.2 Shortcut Trusts

DSfW supports shortcut trusts within a tree. The procedure to create and use a shortcut trust is similar to how shortcut trusts are created and used in Microsoft Active Directory. For more information on creating shortcut trusts, refer to the [Administering Active Directory Operations Guide \(http://technet2.microsoft.com/WindowsServer/en/library/a874d75d-09b9-40c6-87d6-75d0733d88301033.mspx\)](http://technet2.microsoft.com/WindowsServer/en/library/a874d75d-09b9-40c6-87d6-75d0733d88301033.mspx).



In Domain Services for Windows (DSfW), the schema is stored in its own partition (the schema partition) in the directory. The attributes and classes are stored in the schema partition as directory objects that are called schema objects. The schema partition is represented by an object that is an instance of the Directory Management Domain (DMD) class. The distinguished name of the schema partition can be expressed as `cn=schema,cn=configuration,dc=ForestRoot DomainName`. By default, every primary domain controller in the forest holds a replica of the schema partition. The attributes of rootDSE identify, among other things, the directory partitions such as domain, schema, configuration directory partitions, and the forest root domain directory partition. The `schemaNamingContext` attribute provides the location of the schema so that applications that connect to any domain controller can find and read the schema.

eDirectory™ administration tools and applications locate the schema by using the distinguished name. However, the NDS® schema still exists and is the real internal representation of the schema from the Directory System Agent (DSA) perspective.

All applications can continue to use the `subschemaSubentry` attribute from the rootDSE. The distinguished name of the subschema subentry container looks like `cn=aggregate,cn=schema,cn=configuration,dc=ForestRootDomainName`.

Ensure that you replicate the configuration and schema partitions to improve the response time and performance of the server.

- ♦ [Section 7.1, “Schema Objects,” on page 125](#)
- ♦ [Section 7.2, “Extending the Third-Party Schema,” on page 132](#)
- ♦ [Section 7.3, “Changing the PAS Status of an Attribute,” on page 133](#)

## 7.1 Schema Objects

A schema object, named `classSchema`, defines each class in the schema. Another schema object, the `attributeSchema` object, defines each attribute in the schema. Therefore, every class is actually an instance of the `classSchema` class, and every attribute is an instance of the `attributeSchema` class.

**Table 7-1** *Some Attributes for the AttributeSchema Object*

Attribute	Syntax	Description
cn	Unicode	Descriptive relative distinguished name for the schema object. cn is a mandatory attribute.
attributeID	Object identifier	Object identifier that uniquely identifies this attribute. attributeID is a mandatory attribute.
IDAPDisplayName	Unicode	Name by which LDAP clients identify this attribute. IDAPDisplayName is not a mandatory attribute.
schemaIDGUID	String (Octet)	GUID that uniquely identifies this attribute. schemaIDGUID is a mandatory attribute.
mAPIID	Integer	Integer by which Messaging API (MAPI) clients identify this attribute. mAPIID is not a mandatory attribute.
attributeSecurityGUID	GUID	GUID by which the security system identifies the property set of this attribute. attributeSecurityGUID is not a mandatory attribute.
attributeSyntax	Object identifier	Syntax object identifier of this attribute. attributeSyntax is a mandatory attribute.
oMSyntax	Integer	Syntax of this attribute as defined by the XAPIA X/Open Object Model (XOM) specification. oMSyntax is a mandatory attribute.
isSingleValued	BOOL	Indicates whether this attribute is a single-value or multivalue attribute. isSingleValued is a mandatory attribute.
<hr/> <p><b>NOTE:</b> Multivalue attributes hold a set of values with no particular order. Multivalue attributes are not always returned in the order in which they were stored (or in any other order).</p> <hr/>		
extendedCharsAllowed	BOOL	Indicates whether extended characters are allowed in the value of this attribute. Applies only to attributes of syntax String (teletex). extendedCharsAllowed is not a mandatory attribute.
rangeLower	Integer	Lower range of values that are allowed for this attribute. rangeLower is not a mandatory attribute.
rangeUpper	Integer	Upper range of values that are allowed for this attribute. rangeUpper is not a mandatory attribute.

Attribute	Syntax	Description
systemFlags	Integer	<p>Flags that determine specific system operations. This attribute cannot be set or modified.</p> <p>The following systemFlags attributes are relevant to the schema objects:</p> <ul style="list-style-type: none"> <li>♦ The attribute is required to be a member of the partial set = 0x00000002</li> <li>♦ The attribute is not replicated = 0x00000001</li> <li>♦ The attribute is a constructed attribute = 0x00000004</li> </ul> <p>systemFlags is not a mandatory attribute.</p>
searchFlags	integer	<p>The searchFlags property of each property's attributeSchema object defines different behaviors, including whether a property is indexed.</p> <p>The seven currently defined bits for this attribute are:</p> <ul style="list-style-type: none"> <li>♦ 1 = Index the attribute only</li> <li>♦ 2 = Index the container and the attribute</li> <li>♦ 4 = Add this attribute to the ambiguous name resolution (ANR) set</li> <li>♦ 8 = Preserve this attribute on logical deletion (not implemented)</li> <li>♦ 16 = Include this attribute when copying a user object</li> <li>♦ 32 = Create a Tuple index for the attribute to improve medial searches (not implemented)</li> <li>♦ 64 = Reserved for future use; the value should be 0.</li> <li>♦ 128 = Mark the attribute confidential (not implemented)</li> </ul> <p>searchFlags is not a mandatory attribute.</p>
isMemberofPartialAttributeSet	BOOL	<p>A Boolean value that defines whether the attribute is replicated to the global catalog. A value of TRUE means that the attribute is replicated to the global catalog.</p> <p>isMemberof PartialAttributeSet is not a mandatory attribute.</p>
systemOnly	BOOL	<p>If TRUE, only the system can modify this attribute. A user-defined attribute must never have the systemOnly flag set. systemOnly is not a mandatory attribute.</p>
objectClass	Object identifier	<p>The class of this object, which is always attributeSchema. objectClass is a mandatory and multivalued attribute.</p>
nTSecurityDescriptor	NT-Sec-Des	<p>The security descriptor on the attributeSchema object itself. nTSecurityDescriptor is a mandatory attribute.</p>

Attribute	Syntax	Description
oObjectClass	String (Octet)	<p>For attributes with object syntax (OM-syntax = 127), this is the Basic Encoding Rules (BER) encoded object identifier of the XOM object class.</p> <p>For more information about BER encoding, see <a href="http://www.ietf.org/rfc/rfc2251.txt">Request for Comments (RFC) 2251 (http://www.ietf.org/rfc/rfc2251.txt)</a> in the IETF RFC Database.</p> <p>oObjectClass is not a mandatory attribute.</p>
LinkID	Integer	<p>The value that determines whether the attribute is a linked attribute. Linked attributes make it possible to associate one object with another object. A linked attribute represents an interobject distinguished-name reference.</p> <p>A forward link references a target object in the directory; a back link refers back to the source object that has a forward link to it.</p> <p>An even integer denotes a forward link; an odd integer denotes a back link.</p> <p>LinkID is not a mandatory attribute.</p>

- ♦ [Section 7.1.1, “Syntaxes,” on page 128](#)
- ♦ [Section 7.1.2, “Attribute Mappings,” on page 129](#)
- ♦ [Section 7.1.3, “Special Attributes,” on page 130](#)
- ♦ [Section 7.1.4, “Class Mappings,” on page 132](#)

## 7.1.1 Syntaxes

The syntax for an attribute defines the storage representation, byte ordering, and matching rules for comparisons. When you define a new attribute, you must specify both the attributeSyntax and the oMSyntax numbers of the syntax that you want for that attribute. The attributeSyntax number is an object identifier, and the oMSyntax number is an integer. oMSyntax is defined by the XOM specification. Using this model, the syntax can provide detailed syntax definitions. For example, distinct oMSyntax attributes distinguish several types of printable strings, according to such factors as the supported character set and whether case is significant.

eDirectory comes with a predefined set of syntaxes. Most of the syntaxes required to support Active Directory applications are supported directly or indirectly by eDirectory. The following table lists the valid syntaxes for attributes in the DSfW schema. It also shows how each DSfW syntax is internally mapped to eDirectory syntax. Refer to the [Section 7.2, “Extending the Third-Party Schema,” on page 132](#) for more information on automating mapping.

**Table 7-2** Mapping Valid Syntaxes for Attributes in the DSFW Schema

Syntax	Attribute Syntax	oMSyntax	eDirectory Syntax	Description
Object(DN-DN)	2.5.5.1	127	SYN_DIST_NAME	The fully qualified name of an object in the directory.



Syntax	Attribute Syntax	oMSyntax	eDirectory Syntax	Description
String (Object-Identifier)	2.5.5.2	6	SYN_CI_STRING	The object identifier.
Case-Sensitive String	2.5.5.3	27	SYN_CI_STRING	General string. Differentiates uppercase and lowercase.
CaseIgnoreString (Teletex)	2.5.5.4	20	SYN_CI_STRING	Teletex. Does not differentiate uppercase and lowercase.
String (Printable), String (IA5)	2.5.5.5	19, 22	SYN_PR_STRING SYN_CE_STRING	Printable string or IA5 string. Both character sets are case sensitive.
String (Numeric)	2.5.5.6	18	SYN_NU_STRING	A sequence of digits.
Object (DN-Binary)	2.5.5.7	127	SYN_PATH	A distinguished name plus a binary large object.
Boolean	2.5.5.8	1	SYN_BOOLEAN	TRUE or FALSE values.
Integer, Enumeration	2.5.5.9	2, 10	SYN_INTEGER	A 32-bit number or enumeration.
String (Octet)	2.5.5.10	4	SYN_OCTET_STRING	A string of bytes.
String (UTC-Time), String (Generalized-Time)	2.5.5.11	23, 24	SYN_TIME	UTC time or generalized time.
String (Unicode)	2.5.5.12	64	SYN_CI_STRING	Unicode string.
Object (Presentation-Address)	2.5.5.13	127	SYN_OCTET_STRING	Presentation address.
Object (DN-String)	2.5.5.14	127	SYN_OCTET_STRING	A DN string plus a Unicode string.
String (NT-Sec-Desc)	2.5.5.15	66	SYN_OCTET_STRING	A Windows NT security descriptor.
LargeInteger	2.5.5.16	65	SYN_INTEGER64	A 64-bit number.
String (Sid)	2.5.5.17	4	SYN_OCTET_STRING	Security identifier (SID).

## 7.1.2 Attribute Mappings

Because eDirectory attributes conflict with DSfW attributes, new attributes and mappings have been introduced. The following table summarizes them.

**Table 7-3** LDAP Attribute Mapping with eDirectory Attributes

LDAP Attribute Name	eDirectory Attribute Name
homeDirectory	mSDS:HomeDirectory

LDAP Attribute Name	eDirectory Attribute Name
mailRecipient	msds:mailRecipient
homePostalAddress	msds:homePostalAddress
objectVersion	msds:objectVersion
unixHomeDirectory	homeDirectory
uid	uniqueID

### 7.1.3 Special Attributes

Some of the following attributes can be used in search query:

- ♦ **allowedAttributes:** Returns the list of attributes that can be present on that entry.
- ♦ **allowedAttributesEffective:** Returns the list of attributes that can be modified by the user (the logged-in entity) on that object.
- ♦ **allowedChildClasses:** Returns the list of classes that can be created subordinate to that entry.
- ♦ **allowedChildClassesEffective:** Returns the list of classes subordinate to an entry that can be created by the user (logged-in entity).

**Table 7-4** *Attributes of a classSchema Object*

Attribute	Syntax	Description
cn	Unicode	Descriptive relative distinguished name for the schema object. cn is a mandatory attribute.
governsID	Object identifier	Object identifier that uniquely identifies this class. governsID is a mandatory attribute.
IDAPDisplayName	Unicode	The name by which LDAP clients identify this class. IDAPDisplayName is a mandatory attribute.
schemalDGUID	String (Octet)	The GUID that uniquely identifies this class. schemalDGUID is a mandatory (but defaulted) attribute.
rDNAttID	Object Identifier	The relative distinguished name type of instances of this class (OU, CN). rDNAttID is not a mandatory attribute.
subClassOf	Object Identifier	The class from which this object inherits attributes. subClassOf is not a mandatory attribute.
systemMustContain	Object identifier	The list of mandatory attributes for instances of this class. This list cannot be changed. systemMustContain is not a mandatory attribute.
mustContain	Object identifier	The mandatory attributes for instances of this class. mustContain is multivalued but not a mandatory attribute.

Attribute	Syntax	Description
systemMayContain	Object identifier	The optional attributes for instances of this class. systemMayContain is multivalued but not a mandatory attribute.
mayContain	Object identifier	The optional attributes for instances of this class. mayContain is not a mandatory attribute.
systemPossSuperiors	Object identifier	The classes that can be parents of this class in the directory hierarchy. After the class is created, this property cannot be changed. systemPossSuperiors is multivalued but not a mandatory attribute.
possSuperiors	Object identifier	The classes that can be parents of this class in the directory hierarchy. For an existing classSchema object, values can be added to this property but not removed. possSuperiors is multivalued but not a mandatory attribute.
systemAuxiliaryClass	Object identifier	The auxiliary classes from which this class inherits its optional (mayContain) and mandatory (mustContain) attributes. After creation of the class, this property cannot be changed. systemAuxiliaryClass is multivalued but not a mandatory attribute.
auxiliaryClass	Object identifier	The auxiliary classes from which this class inherits its optional (mayContain) and mandatory (mustContain) attributes. This is a multivalue property that specifies the auxiliary classes that this class inherits from. For an existing classSchema object, values can be added to this property but not removed. auxiliaryClass is multivalued but not a mandatory attribute.
defaultHidingValue	BOOL	The default hiding state for the class. If you do not want instances of the class displayed in the UI for Active Directory admin tools, New menus, you can define the class as hidden. defaultHidingValue is not a mandatory attribute.
defaultSecurityDescriptor	String (Octet)	The default security descriptor that is assigned to new instances of this class if no security descriptor is specified during creation of the class or is merged into a security descriptor if a security descriptor is specified. defaultSecurityDescriptor is not a mandatory attribute.
objectClassCategory	Integer	<p>The class types are defined as follows:</p> <ul style="list-style-type: none"> <li>♦ Structural = 1</li> <li>♦ Abstract = 2</li> <li>♦ Auxiliary = 3</li> </ul> <p>objectClassCategory is a mandatory attribute.</p>
systemOnly	BOOL	An attribute of a classSchema object. systemOnly is a mandatory attribute.
ObjectClass	Object Identifier	This object's class, which is always classSchema. ObjectClass is a mandatory and multivalued attribute.

Attribute	Syntax	Description
nTSecurityDescriptor	NT-Sec-Desc	The security descriptor on the classSchema object. nTSecurityDescriptor is not a mandatory attribute.
defaultObjectCategory	Distinguished name	<p>The default object category of new instances of this class. If none has been specified, the objectClass value is used.</p> <p>For example, suppose that the the objectCategory attribute for inetOrgPerson is set to Person. This has the effect of returning all user, computer, and inetOrgPerson objects when the filter in a query is objectCategory=Person.</p> <p>defaultObjectCategory is a mandatory attribute.</p>

## 7.1.4 Class Mappings

Because the eDirectory schema conflicts with the DSfW schema, new classes and mappings are introduced. The following table summarizes them:

**Table 7-5** *Attributes for the AttributeSchema Class*

LDAP Classes	eDirectory Classes
ndsComputer	Computer
computer	mSDS:Computer
ndsDmd	dmd
dMD	mSDS:DMD
ndsServer	server
server	mSDS:Server
ndsVolume	volume
volume	mSDS:Volume
organizationalPerson	Organizational Person
organizationalUnit	Organizational Unit
groupOfNames	Group
groupOfUniqueNames	Group
inetOrgPerson	User

## 7.2 Extending the Third-Party Schema

To extend a third-party schema for a DSfW server:

- 1 Export the third-party schema to an LDIF file, such as `schema.ldif`.
- 2 Execute the following command to generate `msschema.sch`:

```
/opt/novell/xad/share/dcinit/aggregateSchema.pl schema.ldif --ndsschema >
msschema.sch
```

---

**IMPORTANT:** You must review `msschema.sch` manually for any containment issues.

---

- 3** Extend this schema to a DSfW server by executing the following command:

```
/opt/novell/eDirectory/bin/ndssch admin-context -t tree-name msschema.sch
```

- 4** Use `ldapadd` or `ldapmodify` to create schema elements in the schema partition.

---

**NOTE:** Update the DN's of the schema elements in the LDIF file as necessary.

---

## 7.3 Changing the PAS Status of an Attribute

DSfW must be restarted on the domain controllers in the forest when the PAS status of an attribute is modified. The PAS status changes appear in the domain controller where it was changed. Make the following LDAP changes to update the schema cache in other domain controllers in the forest:

dn:

changetype:modify

add:schemaupdatenow

schemaUpdateNow:1



# Printing in the Domain Services for Windows Environment

# 8

Novell iPrint is the printing solution for Open Enterprise Server (OES) 2. This section describes how Domain Services for Windows users can set up and use Novell® iPrint on DSfW.

- ♦ [Section 8.1, “Deploying iPrint in a DSfW Partition,” on page 135](#)
- ♦ [Section 8.2, “Setting Up iPrint,” on page 135](#)
- ♦ [Section 8.3, “Special Handling for iPrint on DSfW,” on page 135](#)
- ♦ [Section 8.4, “iPrint Clustering in a DSfW Environment,” on page 136](#)

## 8.1 Deploying iPrint in a DSfW Partition

Deploying iprint on a DSfW partition can happen in one of the following user scenarios:

- Name mapped
- Non-name mapped
- Forest Root Domain (FRD)
- Parent Domain Controller (PDC)
- Additional Domain Controller (ADC)
- Child Domain Controller (CDC)
- Grand Child Domain Controller (GCDC)

For details on Forest, Domain, Domain Controller, and so on, see [Section 1.3, “Basic Directory Services Concepts,” on page 13](#).

## 8.2 Setting Up iPrint

With Domain Services for Windows, you set up iPrint in the same way as for any OES 2 Linux installation. The Novell iPrint pattern is selected automatically when you select the Domain Services for Windows pattern during the OES 2 server installation.

For instructions on how to install and configure iPrint on OES 2 Linux servers, see “[Setting Up iPrint on Your Server](http://www.novell.com/documentation/oes2/iprint_lx/data/akuji88.html) ([http://www.novell.com/documentation/oes2/iprint\\_lx/data/akuji88.html](http://www.novell.com/documentation/oes2/iprint_lx/data/akuji88.html)) in the *OES2: iPrint for Linux Administration Guide*.

## 8.3 Special Handling for iPrint on DSfW

Use these sections to handle the specific conditions during iprint configuration on DSfW:

- ♦ [Section 8.3.1, “Secure and Non-Secure Printing,” on page 136](#)
- ♦ [Section 8.3.2, “Using a Common Driver Store in a DSfW partition,” on page 136](#)

### 8.3.1 Secure and Non-Secure Printing

iPrint supports both secure and non-secure printing.

For non-secure printing, users do not need to be authenticated in order to install and access printers made available through iPrint. They simply use iPrint's browser-based tool to find a nearby printer and install the necessary drivers for the selected printer.

For secure printing, only iPrint printers that the user has rights to can be installed using the browser-based tool.

While accessing secure printer, if a user is not unique in the iPrint client authentication window, then that user needs to provide the complete context in either LDAP or Domain Controller based format for the authentication window. For example, if the user administrator is present in user context for both First Root Domain (FRD) as well as Child Domain Controller (CDC), you need to provide the complete context for the user who needs to be authenticated. Use one of the following format based on the user context:

- The LDAP format is "cn=person,cn=Users,o=<context>,C=<context>"
- The DC format is "cn=person,cn=Users,dc=<context>,dc=<context>"

### 8.3.2 Using a Common Driver Store in a DSfW partition

There is no need to create a separate Driver Store for DSfW partition. You can configure PSM in a DSfW partition to use an existing Driver Store which is outside of the DSfW partition.

## 8.4 iPrint Clustering in a DSfW Environment

- [Section 8.4.1, "iPrint Clustering on NSS Clusters," on page 136](#)

### 8.4.1 iPrint Clustering on NSS Clusters

It is recommended that all NSS Cluster nodes for iPrint reside in the same container of the DSfW partition. This is because, we add 'wwwrun' user and 'www' group as trustee for the iPrint areas on the NSS Volume. These users are created in every container the nodes reside in. So, if the nodes reside in different containers, there will be one set of the above user and group for every container.

If you run the iPrint migration script on a node, the user & group in the container the node resides in is added as a trustee to the same node in the container. If we have any other node - in a different container, then we need to add the respective 'wwwrun' & 'www' objects added as trustees to the iPrint areas on the Cluster NSS Volume.

The location they need to be added as trustee with 'rwcmf' rights is, `var/opt/novell/iPrint` on the specific clustered iPrint NSS Volume.



# Upgrade and Migration Issues

# 9

This section outlines issues relating to server upgrade and migration in a DSfW environment.

- ♦ [Section 9.1, “Upgrading from OES 1.0 Linux,” on page 137](#)
- ♦ [Section 9.2, “Migrating Data to a Domain Services for Windows Server,” on page 137](#)

## 9.1 Upgrading from OES 1.0 Linux

In-place upgrade of an existing OES 1.0 Linux server to a DSfW server is not supported.

You must first install and configure a new OES 2 Linux server with DSfW, then migrate data from the existing OES 1.0 Linux server.

## 9.2 Migrating Data to a Domain Services for Windows Server

The migration of data to an OES 2 Linux server running DSfW is similar to any other data migration to OES 2 Linux:

- ♦ You should use the new OES 2 migration tools.
- ♦ When the source and destination servers are in the same eDirectory™ tree, only the data and trustee rights are migrated.
- ♦ When the source and destination servers are in different eDirectory trees, the data and associated users are migrated.

For information on how to use the OES 2 migration tools for migrating data, see the [OES 2: Migration Tools Administration Guide](#).



With Novell® Open Enterprise Server (OES) 2, you have several options for providing DSfW users with access to network data:

- ♦ [Section 10.1, “Accessing Files by Using Native Windows Methods,” on page 139](#)
- ♦ [Section 10.2, “Accessing Files by Using the Novell Client for Windows,” on page 147](#)
- ♦ [Section 10.3, “Accessing Files in Another Domain,” on page 147](#)

## 10.1 Accessing Files by Using Native Windows Methods

---

**IMPORTANT:** Do not install the Novell Client™ for Windows on a workstation for which you plan to provide native Windows access to DSfW servers. Novell Client access and native Windows access to DSfW servers do not work well together on the same workstation.

The instructions in this section assume that you have already prepared your workstations for accessing the DSfW server by completing the instructions in these prior sections:

- ♦ [Section 3.1, “Joining a Windows Workstation to a DSfW Domain,” on page 77](#)
  - ♦ [Section 3.2, “Logging In to a DSfW Domain,” on page 80](#)
  - ♦ [Chapter 4, “Creating and Provisioning Users,” on page 81](#)
- 

This section discusses the following topics:

- ♦ [Section 10.1.1, “Samba: A Key Component of DSfW,” on page 139](#)
- ♦ [Section 10.1.2, “Samba in the DSfW Environment,” on page 140](#)
- ♦ [Section 10.1.3, “Creating Samba Shares in iManager,” on page 141](#)
- ♦ [Section 10.1.4, “Creating Samba Shares in the smb.conf File,” on page 143](#)
- ♦ [Section 10.1.5, “Assigning Rights to Samba Shares,” on page 143](#)
- ♦ [Section 10.1.6, “Adding a Network Place,” on page 145](#)
- ♦ [Section 10.1.7, “Adding a Web Folder,” on page 146](#)
- ♦ [Section 10.1.8, “Mapping Drives to Shares,” on page 146](#)

### 10.1.1 Samba: A Key Component of DSfW

One of the primary benefits of DSfW is that users can access files on OES 2 Linux servers without having any Novell client software installed. This is accomplished through Samba software that is installed on every DSfW server.

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

OES 2 SP1 customers actually have three Samba configuration options:

- ♦ The open source Samba services that are provided with SUSE® Linux Enterprise Server (SLES)10 SP2 and other Linux distributions.
- ♦ The Novell Samba implementation that has always been included in OES to integrate eDirectory™ authentication with basic Samba file services.
- ♦ The DSfW configuration of Samba.

The [Section 10.1.2, “Samba in the DSfW Environment,” on page 140](#) explains key differences between the Novell Samba configuration in OES 2 SP1 and the configuration that is included with DSfW.

## 10.1.2 Samba in the DSfW Environment

When you install a DSfW server, Samba software is automatically installed on that server. This is the same Samba software that is included in OES 2 SP1, but it is configured differently as outlined in [Table 10-1](#).

**Table 10-1** *Novell Samba in OES 2 SP1 vs. Samba in DSfW*

Item	Novell Samba in OES 2 SP1	Samba in DSfW
Authentication	A Samba-compatible Password Policy is required for compatibility with Windows workgroup authentication.	No Samba-compatible Password Policy is required for DSfW users because the domain is set up as a trusted environment.  DSfW uses Active Directory/Kerberos authentication to ensure that only authorized users can log in to the domain.
File system support	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 Linux server. For instructions on how to set up an NSS volume, see “ <a href="#">Managing NSS Volumes</a> ” in the <i>OES 2 SP1: File Systems Management Guide</i> .	
Samba enablement	Users must be enabled for 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 <a href="#">Chapter 4, “Creating and Provisioning Users,” on page 81</a> .  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.

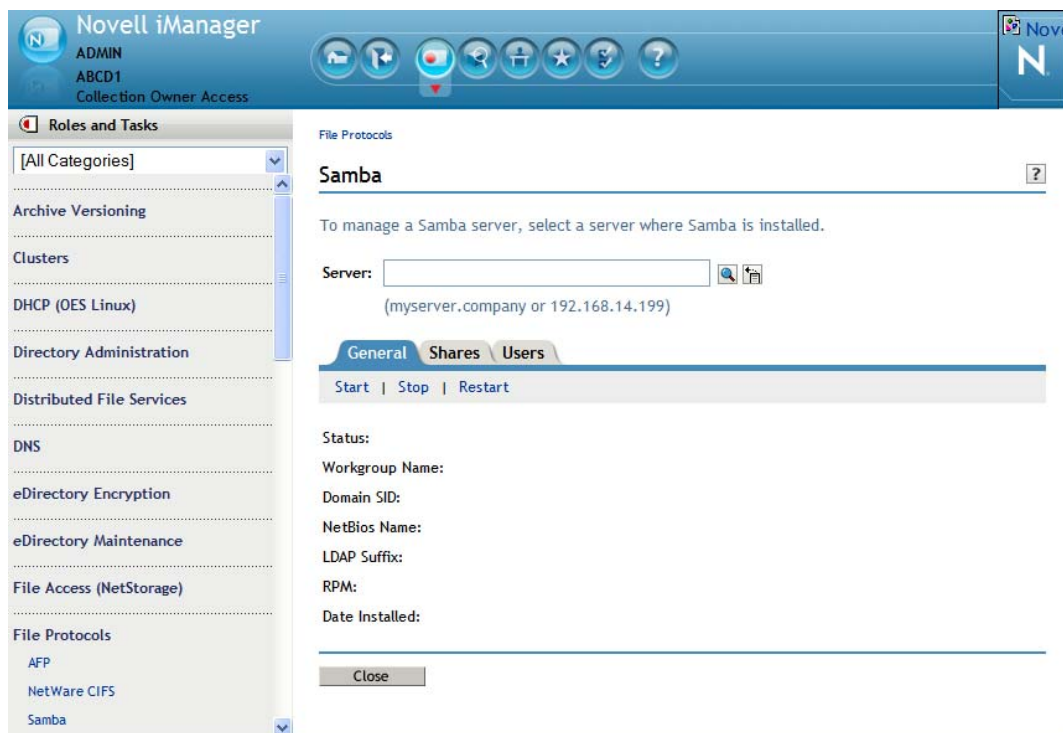
Item	Novell Samba in OES 2 SP1	Samba in DSfW
Username and password	The same username and password must exist on both the Windows workstation and in eDirectory.	eDirectory users in the domain (eDirectory partition) can log into any workstation that has joined the domain. There is no need for a corresponding user object on the workstation.

### 10.1.3 Creating Samba Shares in iManager

To manage Samba shares, iManager must be configured with the necessary plug-ins and role-based services. For information on how to configure iManager, see the *Novell iManager 2.7 Administration Guide*.

To create a Samba share in iManager:

- 1 Open a browser and point to `http://ip_address_of_server/nps/iManager.html`.
- 2 Provide the username, password, and tree information as requested and click *Login*.
- 3 In the Roles and Tasks view, select *File Protocols > Samba*.



- 4 Specify the IP address of the server you want to manage, or use the Object Selector to browse to and select the server.



The NCP Server objects for DSfW servers are located in `.Novell.System.domain_name.com`.

The General page displays Samba-related information about the selected server.

File Protocols

## Samba

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

Server:   

(myserver.company or 192.168.14.199)

**General** | **Shares** | **Users**

[Start](#) | [Stop](#) | [Restart](#)

Status:	Running
Domain Name:	EXAMPLE
Domain SID:	S-1-5-21-1574332969-201364638-299643277
NetBios Name:	OESDC
LDAP Suffix:	N/A
RPM:	samba-3.0.24-2.23
Date Installed:	Fri Jul 13 15:38:52 MDT 2007

[Close](#)

5 Click the *Shares* tab.

6 Click *New* and enter the share name, path, and comment (optional). Click *OK*.

The path you enter must already exist on the OES 2 Linux server's file system. By default, NSS volumes are located in `/media/nss/volume_name`.

File Protocols > Samba

## New Share

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

Share Name:

Path:

(volume mount point, ie: /media/nss/VOL1)

Comment:

☐ Read-Only

☒ Inherit ACLs

[OK](#) [Cancel](#)

The example shown above creates a Samba share called Projects for the NSS volume named PROJECTS. The share name and volume name do not need to be the same, but making them identical can make share management easier. If you want, you can enter a more complete description of the share in the *Comment* field.

The new share is added to the list of shares for this Samba server.

Continue with [Section 10.1.5, "Assigning Rights to Samba Shares," on page 143](#) to assign users rights to access the new share.

## 10.1.4 Creating Samba Shares in the smb.conf File

If you prefer, you can create Samba shares by editing the `/etc/samba/smb.conf` file.

For example, to create a Samba share on an NSS volume named PROJECTS, you would create a share to the `/media/nss/PROJECTS` directory as follows:

- 1 Open the `/etc/samba/smb.conf` file in an editor.
- 2 Create a [projects] share in the `smb.conf` file by inserting the following lines:

```
[projects]
comment = Project folders
path = /media/nss/PROJECTS
browseable = Yes
read only = No
inherit acls = Yes
```

- 3 Save the file and restart Samba.

Continue with [Section 10.1.5, “Assigning Rights to Samba Shares,”](#) on page 143 to assign users rights to access the new share.

## 10.1.5 Assigning Rights to Samba Shares

For domain users to access the Samba shares you have created, you must assign the appropriate rights. You can assign rights to individual users or to groups. If you want all users in the domain to have the same rights to the share, you can assign the rights to the DomainUsers group.

[Table 10-2](#) lists the management tools available for assigning rights to Samba shares created on various file systems.

**Table 10-2** Tools for Managing File System Rights

File System	Rights Management Tools	Notes
Novell Storage Services™ (NSS)	<i>iManager &gt; Files and Folders &gt; Properties &gt; Rights</i>	For more information on assigning file system rights on NSS volumes in iManager, see <a href="#">“Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes”</a> in the <i>OES 2 SP1: NSS File System Administration Guide</i> .
	rights command	The <code>rights</code> command available at the terminal prompt is for working with NSS volumes only. For online help, enter <code>rights</code> with no options. For more information, see <a href="#">“RIGHTS (Linux)”</a> in the <i>OES 2 SP1: NSS File System Administration Guide</i> .

File System	Rights Management Tools	Notes
NCP™ Volume on Linux POSIX* file systems (no NSS)	iManager > Flies and Folders > Properties > <i>Rights</i>	For more information on assigning file system rights on NCP volumes in iManager, see “ <a href="#">Managing File or Directory Trustees and Rights with iManager</a> ” in the <i>OES 2 SP1: NCP Server for Linux Administration Guide</i> .
	<code>ncpcon &gt; rights</code>	The <code>rights</code> command in the <code>ncpcon</code> utility is for working with any NCP volume, including NSS volumes and NCP volumes defined on Linux POSIX file systems. For online help, run <code>ncpcon</code> and enter <code>help rights</code> . For more information, see “ <a href="#">Managing File System Trustees and Trustee Rights for NCP Volumes</a> ” in the <i>OES 2 SP1: NCP Server for Linux Administration Guide</i> .
Linux POSIX file systems (no NSS or NCP)	<code>chmod</code> <code>chown</code> <code>chgrp</code>	For information on assigning POSIX rights, see the <a href="http://www.novell.com/documentation/sles10/sles_admin/data/sec_system_userperm.html">SLES 10 Installation and Administration Guide</a> ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/sec_system_userperm.html">http://www.novell.com/documentation/sles10/sles_admin/data/sec_system_userperm.html</a> ).

### Example: Assigning Rights to Folders on an NSS Volume

The example below continues the steps described in [Section 10.1.3, “Creating Samba Shares in iManager,”](#) on page 141 and [Section 10.1.4, “Creating Samba Shares in the smb.conf File,”](#) on page 143.

- 1 Beneath the `/media/nss/PROJECTS` folder, create subfolders for each project.

For example, you could create folders named `doc` and `code`.

- 2 Assign trustees to the project folders, using either iManager or the `rights` command at a terminal prompt.

For example, suppose you want `user1` to have full rights to `doc` but only read and filescan rights to `code`, and you want `user2` to have full rights to `code` but only read and filescan to `doc`. You could assign the rights by using the following commands:

```
rights add projects:doc user1.full_dir_context all
rights add projects:doc user2.full_dir_context rf
rights add projects:code user2.full_dir_context all
rights add projects:code user1.full_dir_context rf
```

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



## 10.1.6 Adding a Network Place

From a Windows 2000 or XP workstation, you can add a Network Place (also known as a Web folder) that points to a share on the DSfW server.

---

**IMPORTANT:** The directory you are linking to must already exist on the DSfW server and fall within the scope of a defined share.

Share names and the server directories they point to are defined by using the Samba Management plug-in for iManager or by editing the `/etc/samba/smb.conf` file on the OES 2 Linux server. For more information and setting up shares, see [Section 10.1.3, “Creating Samba Shares in iManager,” on page 141](#) and [Section 10.1.4, “Creating Samba Shares in the smb.conf File,” on page 143](#).

---

- 1 Log in to your Windows workstation.
- 2 From your desktop, access *My Network Places*.  
For example, click *Start My > Computer > My Network Places*.
- 3 Click *Add Network Place*.
- 4 On Windows XP, do the following:
  - 4a In the Add Network Wizard dialog box, click *Next*.
  - 4b Select *Choose another network location*, then click *Next*.
  - 4c Click *Browse*.
  - 4d Click *Entire Network > Microsoft Windows Network*.
  - 4e Click the domain, then click the DSfW server.
  - 4f Click the share you want to add.  
Share names and the server directories they point to are defined in the `/etc/samba/smb.conf` file on the OES Linux server. For more information and for instructions on setting up shares, see [Section 10.1.3, “Creating Samba Shares in iManager,” on page 141](#).
  - 4g Click *OK > Next*.
  - 4h (Optional) modify the name of the Network Place to a more intuitive name, such as *My Home Directory*.
  - 4i Click *Next*.
  - 4j Click *Finish*.  
The folder opens, ready for access.
- 5 On Windows 2000, do the following:
  - 5a Click *Browse*.
  - 5b Double-click *Entire Network > Microsoft Windows Network*.
  - 5c Double-click your domain name > your DSfW server.
  - 5d Click the share you want to add.  
Share names and the server directories they point to are defined in the `/etc/samba/smb.conf` file on the OES Linux server. For more information and for instructions on setting up shares, see [Section 10.1.3, “Creating Samba Shares in iManager,” on page 141](#).
  - 5e Click *OK > Next*.

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

**5g** Click *Finish*.

The folder opens, ready for access.

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

## 10.1.7 Adding a Web Folder

You can use the Internet Explorer browser to add a Web folder that points to a share on the DSfW server.

---

**IMPORTANT:** The directory you are linking to must already exist on the DSfW server and fall within the scope of a defined share.

Share names and the server directories they point to are defined by using the Samba Management plug-in for iManager or by editing the `/etc/samba/smb.conf` file on the OES 2 Linux server. For more information and setting up shares, see [Section 10.1.3, “Creating Samba Shares in iManager,” on page 141](#) and [Section 10.1.4, “Creating Samba Shares in the smb.conf File,” on page 143](#).

---

- 1 Log in to your Windows workstation.
- 2 Open Internet Explorer.
- 3 Click *File > Open*.
- 4 Click *Open as Web Folder*.
- 5 In the *Open* field, type the DSfW server name and share name as follows:

`DNS_Name_or_IP\share_name`

where *DNS\_Name\_or\_IP* is the IP address or DNS name of the Samba server and *share\_name* is a share name specified in the `/etc/samba/smb.conf` file (the most common share name is “homes”).

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

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

## 10.1.8 Mapping Drives to Shares

From a Windows 2000 or XP workstation, you can map a network drive letter that points to a share on the DSfW server.

---

**IMPORTANT:** The directory you are linking to must already exist on the DSfW server.

---

- 1 Log in to your Windows workstation.
- 2 From your desktop, access *My Computer > Tools > Map Network Drive*.
- 3 From the *Drive* drop-down menu, select an unused drive letter.
- 4 Click *Browse* and browse to *Entire Network > Microsoft Windows Network*.

- 5 Browse to your domain > the DSfW server > the share you want to map the drive to.
- 6 Click *OK*.
- 7 Click *Finish*.

The folder opens, ready for access.

## 10.2 Accessing Files by Using the Novell Client for Windows

Organizations that have the Novell Client for Windows installed on Windows workstations can continue to use the standard NCP methods, such as Novell drive mappings, to access data that is located on NSS or NCP volumes on DSfW servers.

---

**IMPORTANT:** Do not join workstations that use the Novell Client for Windows to the DSfW domain. Novell Client access and native Windows access to DSfW servers do not work well together on the same workstation.

---

## 10.3 Accessing Files in Another Domain

In Active Directory, there is often a need to share resources between domains. This is accomplished by establishing an inter-domain trust relationship between the domains.

Because DSfW is designed to emulate the Active Directory domain model, it might be necessary to establish trust relationships between DSfW domains in the same eDirectory tree.

- ♦ When you install additional domains in an existing eDirectory tree, you have the option of specifying a parent domain for the child domain you are creating. If you do this, an inter-domain trust is automatically configured between the parent domain and the child domain.
- ♦ If you want users to be able to access files in two DSfW domains in the same tree, but the two domains do not have a parent-child relationship, you must use MMC to establish a trust relationship between those two domains.

You can also use MMC to set up inter-domain trusts between a DSfW domain and an Active Directory domain. After this is done, you can create a share on a Windows server in the Active Directory domain and DSfW users can map a drive to that share and access the files on the Windows server.

---

**NOTE:** It is not possible to set up cross-forest trusts between DSfW domains in different eDirectory trees. OES services cannot grant access to users in one tree from another tree.

---

With DSfW, you can establish a cross-forest trust between a DSfW domain or forest and an Active Directory domain or forest and thereby allow provisioned users to access files on servers in the Active Directory domain.

---

**NOTE:** In this release of DSfW, bidirectional trusts are supported, but resource access is not supported. DSfW users can access servers in an Active Directory domain, but it is not possible for users in an Active Directory domain to access servers in a DSfW domain.

Also, in this release, it is not possible to share print resources between a DSfW domain and an Active Directory domain.

---

For more information on trust relationships, refer to [Chapter 6, “Managing Trust Relationships in Domain Services for Windows,”](#) on page 91.

# Configuring Domain Services for Windows for Novell Cluster Services

# 11

This section outlines information you should be aware of when deploying DSfW servers in a Novell Cluster Services™ (NCS) environment for high availability and failover protection.

---

**NOTE:** DSfW is not supported for clustering with Novell Cluster Services for Linux in the OES 2 SP1 Linux release of DSfW.

---

## 11.1 Services that Can Be Clustered

In a DSfW environment, the following services can be clustered:

- ♦ Novell Storage Services (NSS)

For more information about clustering NSS storage using NCS, see the *OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

- ♦ iPrint

For more information about clustering iPrint services, see “Configuring iPrint with Novell Cluster Services” in the *OES2: iPrint for Linux Administration Guide*.



Use the information in this section to resolve DSfW 1.0 issues.

- ♦ [Section 12.1, “Supported Patterns,” on page 151](#)
- ♦ [Section 12.2, “Troubleshooting DSfW,” on page 151](#)
- ♦ [Section 12.3, “iPrint Issues,” on page 157](#)

## 12.1 Supported Patterns

All users added to or created in a DSfW domain are automatically provisioned as both Active Directory domain users and LUM users (except no LUM-enabling is needed). They are also automatically Samba-enabled.

When you select the DSfW pattern in YaST, the following patterns are selected by default:

- ♦ Novell Backup / Storage Management Service
- ♦ Novell eDirectory
- ♦ Novell iManager
- ♦ Novell iPrint
- ♦ Novell DNS and DHCP
- ♦ Novell Linux User Management (LUM)
- ♦ Novell Remote Manager (NRM)
- ♦ Novell Storage Services (NSS)
- ♦ Novell NCP Server / Dynamic Storage Technology

Some patterns depend on the above patterns:

- ♦ The Novell eDirectory pattern requires the Novell Backup/Storage Management Services pattern
- ♦ The Novell Storage Services (NSS) pattern requires the Novell (LUM) pattern and the Novell NCP Server/Dynamic Storage Technology pattern

An additional OES Services pattern, Novell Cluster Services (NCS), can be selected. It is a non-conflicting pattern.

All other OES Services patterns are set as conflicting and, if selected, cause pattern dependency conflicts. Only the packages and products that are listed above are supported on the DSfW server for this release.

## 12.2 Troubleshooting DSfW

- ♦ [“If administrator and default group objects are accidentally deleted” on page 152](#)
- ♦ [Section 12.2.2, “Tree admin is not automatically granted rights for DSfW administration,” on page 153](#)

- ♦ Section 12.2.3, “DSfW services stop working if the concurrent LDAP bind limit is set to 1,” on page 153
- ♦ Section 12.2.4, “The provision utility succeeds only with the --locate-dc option,” on page 153
- ♦ Section 12.2.5, “Users are not samified when the RID master role is seized,” on page 154
- ♦ Section 12.2.6, “Shared volumes are not accessible,” on page 154
- ♦ Section 12.2.7, “Users cannot join a workstation to a domain,” on page 154
- ♦ Section 12.2.8, “Making the DSfW server working when the IP address is changed,” on page 154
- ♦ Section 12.2.9, “Requirements for Samba/CIFS aAccess to NSS volumes via DSfW,” on page 156
- ♦ Section 12.2.10, “Identifying novell-named hang,” on page 157

## 12.2.1 If administrator and default group objects are accidentally deleted

In Open Enterprise Server, DSfW provisions the administrator to delete the default groups. If the administrator and default groups are accidentally deleted, they can be re-created; however, ensure that objects are created with appropriate SIDs.

You can use the following LDIF files to search the deleted objects:

```
/var/opt/novell/xad/ds/domain/domain.ldif
/var/opt/novell/xad/ds/domain/domain-bl.ldif
/var/opt/novell/xad/ds/domain/nds-domain.ldif
```

The above LDIF files host the information for the following objects:

```
cn=Domain Admins,cn=users,<domain>
cn=Domain Controllers,cn=users,<domain>
cn=Domain Computers,cn=users,<domain>
cn=Domain Users,cn=users,<domain>
cn=Domain Guests,cn=users,<domain>
cn=Domain Group Policy Creator Owners,cn=users,<domain>
```

You can use the following LDIF files to search for the Enterprise Admins group object to restore.

```
/var/opt/novell/xad/ds/domain/forest.ldif
/var/opt/novell/xad/ds/domain/forest-bl.ldif
/var/opt/novell/xad/ds/domain/nds-admin-acls.ldif
```



The above LDIF files host the information for the following objects:

```
cn=Enterprise Admins,cn=users,<domain>
```

The LDIF files generated from this information should be used with `ldapmodify`.

Example command:

```
/usr/bin/ldapmodify -H "ldapi://%2fvar%2fopt%2fnovell%2 fxad%2frun%2fldapi" -x  
-D "cn=Administrator,cn=users, dc=example,dc=com" -f /restore.ldif
```

## 12.2.2 Tree admin is not automatically granted rights for DSfW administration

When you install DSfW in a child domain or grandchild domain, the tree admin identity is not automatically added as an administrator of services on the server unless the tree admin is the identity used during the install. If a different identity is used for installation, the tree admin cannot manage the DSfW services on that server.

The administrator credentials that you entered during the DSfW install are automatically configured to allow that user to manage DSfW and related services on the server. After the install, you can add another administrator by configuring the following for the user:

- ♦ Give the user the Supervisor right to the Server object
- ♦ Linux-enable the user with Linux User Management by adding the user to the LUM-enabled Domain admin group associated with the server.

This applies to any administrator that you want to manage DSfW on that server.

## 12.2.3 DSfW services stop working if the concurrent LDAP bind limit is set to 1

This is an invalid scenario.

If you set the bind limit to 1, services such as kinit, rpcclient, SASL-BIND, and Samba, stop and you cannot join a workstation. For the services to function as expected, change the LDAP bind limit to 0, which is the default.

## 12.2.4 The provision utility succeeds only with the `--locate-dc` option

By default, the Provision utility runs with the `--locate-dc` option only. For other options, it fails with the following message:

```
Failed to establish LDAP connection with <domain name> : Unknown  
authentication method.
```

To execute other options, export `SASL_PATH=/opt/novell/xad/lib/sasl2` and kinit with a valid domain username before using Provision utility. All the options will work.

## 12.2.5 Users are not samified when the RID master role is seized

When the current RID master is down, the users already added to the servers other than DSfW after the RID pools are exhausted are not samified.

To resolve this issue, run `/opt/novell/xad/sbin/dcmake nds_import_samify_existing_objects` on the DSfW server.

## 12.2.6 Shared volumes are not accessible

Workstations might not be able to access shared volumes from a DSfW server after the server is rebooted.

There are a number of components that must be restarted in a specific order, and this doesn't always happen when the server restarts.

To restart the services in the correct order, enter the following command at a terminal prompt:

```
dcmake nds_restart_services
```

## 12.2.7 Users cannot join a workstation to a domain

For joining domains, ensure that SLES10 SP2 is installed first, updated with Samba 3.0.32 patch, and then OES2 SP1 installed.

Joining a workstation to a domain might fail sometimes if the services are down. Execute the following command to verify that DSfW services are running:

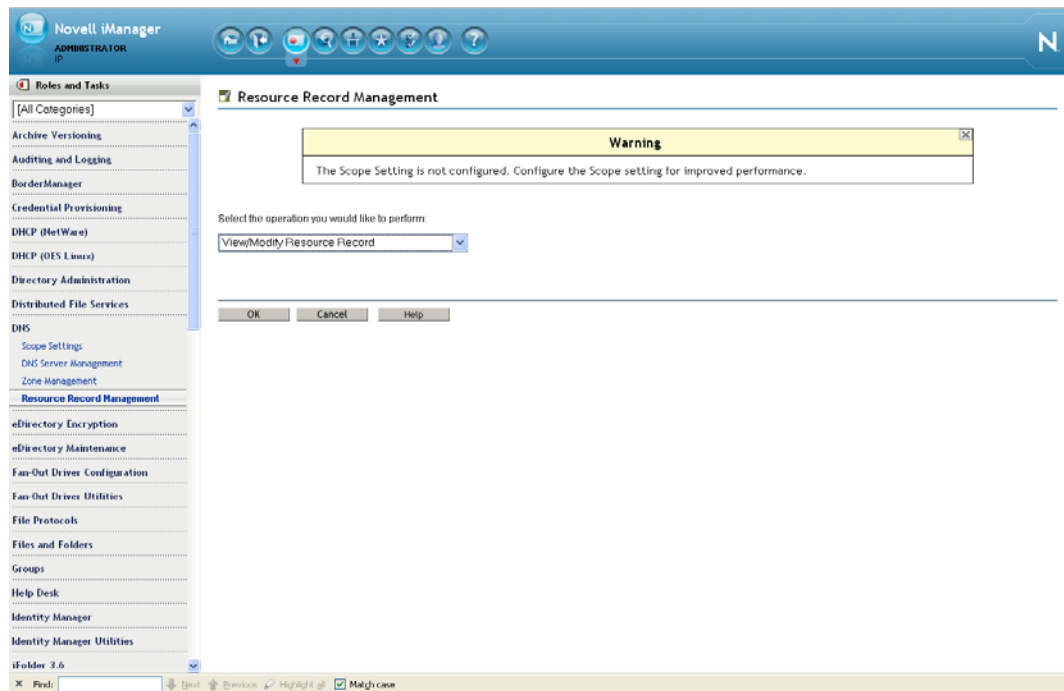
```
xadcntrl status
```

## 12.2.8 Making the DSfW server working when the IP address is changed

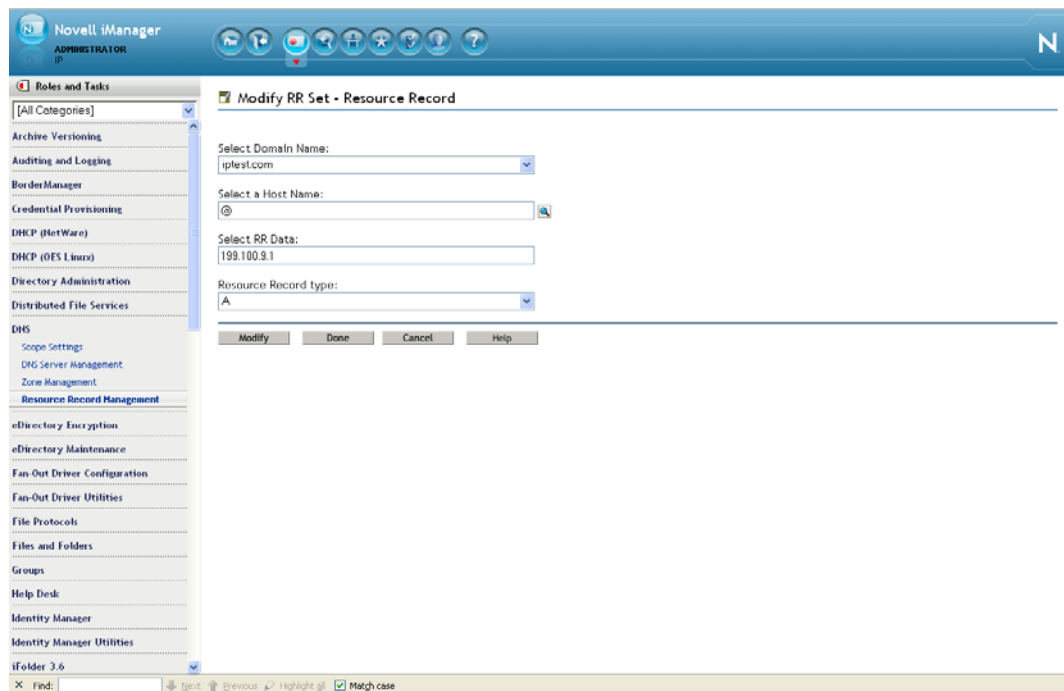
Do these steps to make the DSfW server running when you change the IP address of the server:

- 1 Change the system IP address by using YaST.
- 2 Edit the hosts file that exists in the `/etc`, change the IP address, and then stop the DNS server.

- 3 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.

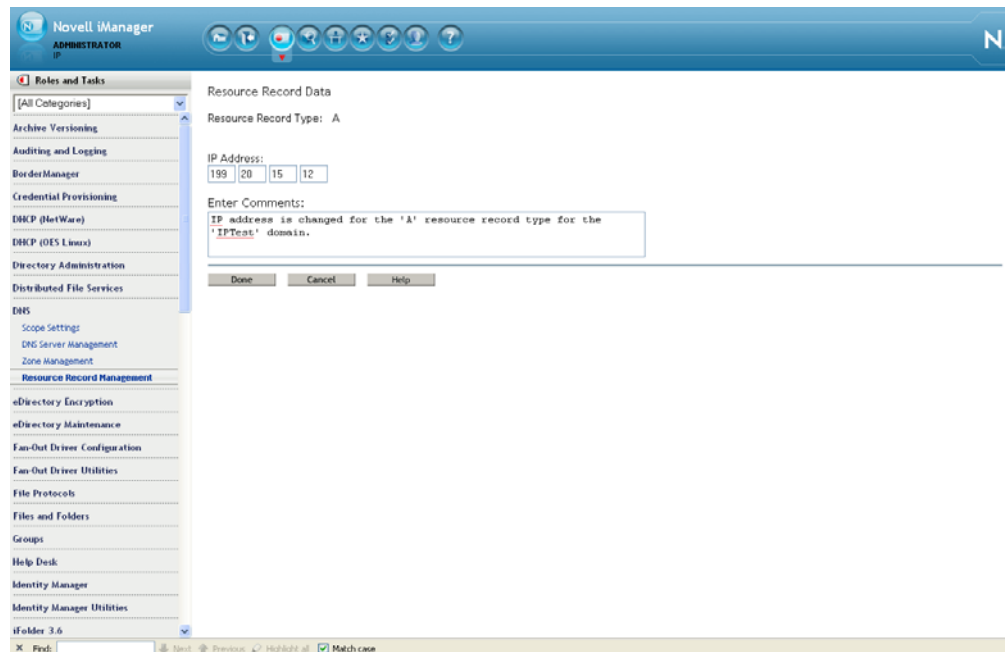


- 4 Select the domain name from the drop-down list, then click *Search*. This is the domain name whose IP address is to be changed (In this example, it is the 'A' record).



- 4a Specify the IP address in the Select RR Data text field.
- 4b Specify the Resource Record Type as 'A'.

- 4c Click *Modify* to open the Resource Record Data window.
- 4d Change the IP address and enter your comments (optional).



- 4e Click *Done*. A message indicates that the A record has been successfully modified.
- 5 Rename the Reverse Lookup object, such as, newipaddress\_in-addr\_arpa(1) by using iManager.
- 6 Change the IP address in the `nds.conf` file.
- 7 Start the DNS server.
- 8 Change the following:
  - 8a Edit the `/etc/nam.conf` file and update the preferred-server.
  - 8b Update the `/etc/resolve.conf` file if the server was acting as the DNS server for the domain.
  - 8c Replace the old IP addresses with the new IP address in the following files:
    - `/etc/opt/novell/eDirectory/conf/nds.conf`
    - `/etc/opt/novell/xad/xad.ini`

---

**NOTE:** For more information on changing the IP address assigned to an OES 2 or OES 2 SP1 Linux server and the services it hosts, refer to “[Changing an OES 2 Linux server’s IP Address](#)” in the *OES 2 SP1: Planning and Implementation Guide*.

---

## 12.2.9 Requirements for Samba/CIFS aAccess to NSS volumes via DSfW

DSfW configures Samba for Samba/CIFS users. Administrators must export NSS volumes over Samba so that domain users (eDirectory™ users in the DSfW domain partition) can access NSS volume over Samba/CIFS.

Samba/CIFS users must be Linux-enabled with Linux User Management in order to access an NSS volumes via this Samba connection. To Linux-enable eDirectory users, use iManager to create a LUM group, then add the users to that group.

NSS uses the NetWare Trustee Model for file access. Users must be made file system trustees and granted trustee rights to data on the NSS volume that you want them to be able to access. Rights management can be done in multiple management tools, including iManager, Novell Remote Manager, the Novell Client™, and the command line.

- ♦ “Administrator not able to create Samba shares” on page 157
- ♦ “Users not able to access NSS volume/Samba shares” on page 157

### Administrator not able to create Samba shares

To create Samba shares, the admin group that the administrator belongs to should be a member of the Unix Workstation Object of the server to which the Samba share is mounted.

- 1 Run `namgroup list -x <o=organization> | grep admin group` to list all the admin groups.
- 2 Add the listed admin groups as a member of Unix Workstation Object of the server to which the samba shares are mounted.

### Users not able to access NSS volume/Samba shares

Ensure the Domain Users group is added to the groupMembership attribute of the Unix workstation Object of the server to which the NSS volume/Samba share is mounted.

## 12.2.10 Identifying novell-named hang

You can perform a nslookup operation to novell-named for an existing zone/domain in the tree. If nslookup hangs, do the following steps to troubleshoot it:

- 1 Run `rcnovell-named stop` to stop the novell-named.
- 2 To disable the dynamic reconfiguration, modify the following entry from the `/etc/init.d/novell-named` file:  

```
startproc -p ${NAMED_PID} ${NAMED_BIN} ${NAMED_ARGS} -u named
```

  
to  

```
startproc -p ${NAMED_PID} ${NAMED_BIN} ${NAMED_ARGS} -u named -r off
```
- 3 Run `rcnovell-named start` to restart the novell-named.

If the novell-named continues hanging, you should restart it to ensure its works properly.

## 12.3 iPrint Issues

- ♦ Section 12.3.1, “Driver store fails to create in a name-mapped FRD,” on page 157

### 12.3.1 Driver store fails to create in a name-mapped FRD

Problem: Creation of driver store (or any other print object) fails with following error:

Internal Server Error

IPP Error: 0xF01F4

HTTP Error: 500

This occurs when a user tries to create a print object that does not exist in the base context set for the LDAP search in the iPrint configuration file.

Assume that two or more peer containers exist at the top, such as, o=abc and o=xyz, and the tree admin exists in the o=abc as shown below:

TREE

```
|__ o=abc
      |__ cn=admin, o=abc
      |__ o=xyz
```

When you setup a DSfW name-mapped forest root domain in o=xyz by using the tree admin (cn=admin, o=abc) and try configuring iPrint by using the domain administrator (o=xyz), you get this error while creating the driver store in o=xyz.

**Why It Happens:** The iPrint installer takes the root context of the user installing iPrint (o=abc) and sets it as default base context for the LDAP search. When you try to create a driver store as a domain administrator of the o=xyz container, the LDAP search fails to find the user creating the driver store. Creating the drive store with the tree admin cn=admin, o=abc succeeds.

**Solution:** The base context for LDAP search is stored in the /etc/opt/novell/iprint/httpd/conf/iprint\_ssl.conf as mentioned below: "

```
AuthLDAPDNURL "ldaps://frd.xyz.com:1636/o=abc??? (objectClass=user)"
```

The above configuration limits that LDAP search to o=abc. Removing the base context completely allows the LDAP search to start from the tree root, as shown below:

```
AuthLDAPDNURL "ldaps://frd.xyz.com:1636/??? (objectClass=user)"
```

This section covers the following topics:

- ♦ [Section 13.1, “Configuring DSfW with Windows DNS server,” on page 159](#)

## 13.1 Configuring DSfW with Windows DNS server

Do the following steps to configure DSfW with Windows DNS server:

- 1 In the new server, add secondary zones for all the existing zones hosted in the DSfW (BIND-based DNS Servers) by using the Windows DNS console.  

---

**NOTE:** While transferring the zones, specify the full name of the Reverse Lookup zone, such as, 127.1.1.1.in-addr.arpa.

---
- 2 After completing the zone transfer, convert the secondary zones to primary zones for the zones that were obtained from the DSfW Server.
- 3 Configure the servers (that were previously primary for DSfW) as secondary servers by using the Novell DNS/DHCP Management Console or iManger.
- 4 Edit the `/etc/resolv.conf` file in the PDC Server of DSfW and change the IP address of the server where the Windows DNS Server is running.
- 5 Stop the Novell DNS server.





# Glossary

## **Access Token**

When a user is authenticated, the Local Security Authority (LSA) creates an access token, which in this case is a primary access token for that user. An access token contains a security identifier (SID) for the user, SIDs for the groups to which the user belongs, and the user's privileges. In Domain Services for Windows (DSfW), a user's SID and group membership are stored in eDirectory™.

When the user logs in to a Windows workstation in a DSfW domain, the Workstation receives this security information from the DSfW domain controller and associates it with the user's login session.

## **Additional Domain**

A child domain for a domain that already exists. Organizations split the data into multiple domains to reduce administrative overhead.

## **Additional Domain Controller**

An added server used to improve the availability and reliability of network services. If you have an additional domain controller, it helps in fault tolerance and balances the load of existing domain controllers. It also provides additional infrastructure support to the sites.

## **ADPH**

Active Directory Provisioning Handler.

Responsible for automatically provisioning all the eDirectory objects in a domain with appropriate Active Directory attributes.

## **Child Domain**

Also known as a subdomain. A child domain is a part of a larger domain name in the DNS hierarchy, which has the root-level domain at the top, followed by second-level domains, then followed by subdomains.

## **Configuration Partition**

Stores the entire eDirectory forest configuration information, which consists of the cross-references and other forest-related information. The data stored in this partition is common to all domains in the eDirectory forest. Each type of configuration information is stored in a container in the configuration partition.

## **Cross-forest Trust**

A feature that enables trust to be automatically managed among multiple DSfW forests or between a DSfW forest and an Active Directory forest. It helps to consolidate operations that result from mergers and acquisitions and enables the users in one forest to seamlessly access services in the other forest.

Cross-forest trusts are transitive. For example, every domain in Forest M has an implicit trust relationship with every domain in Forest N. However, transitivity does not mean that if you have a cross-forest trust between Forest M and Forest N, and a second cross-forest trust between Forest N and Forest O, a trust relationship exists between Forest M and

Forest O. You are required to create a second cross-forest trust between Forest M and Forest O. Cross-forest trusts can be either one-way or two-way, and you need to establish the trust relationship between the forest root domains in each forest.

### **Cross-Reference Objects**

Objects present in the configuration partition of the forest. Each cross-reference object represents a domain partition. They are used by domain controllers to generate referrals to other eDirectory partitions in the forest and to external directories when the object is not local.

Cross-reference objects are created in two ways:

- Internally by the system to refer to known locations that are within the forest.
- Externally by administrators to refer to locations outside of the forest.

### **Domain**

A single partition in the eDirectory tree.

In DSfW, a domain also forms the administrative boundary for a logical group of network resources such as users or computers. Typically, a domain resides in a localized geographic location; however, this might not always be the case. Domains are commonly used to divide global areas of an organization and its functional units.

### **Domain Controller**

In DSfW, an Open Enterprise Service 2 SP1 server that manages user access to a network, which includes logging in, authentication, and access to the directory and shared resources.

### **Existing Domain**

A domain that is already configured in the DSfW forest.

### **Existing Tree**

An eDirectory tree onto which a DSfW server is being added. A domain is created as part of this process.

### **External Trust**

You can create an external trust to form a one-way or two-way nontransitive trust with domains beyond your forest. External trusts are sometimes necessary when users need access to resources located in a Windows NT 4.0 domain or in a domain located within a separate forest that is not joined by a forest trust.

### **Forest**

A set of one or more directory trees that trust each other. All the trees in a forest share a common schema, configuration, and global catalog. When a forest contains multiple trees, the trees do not form a contiguous name space. All the trees in a given forest trust one another through transitive bidirectional trust relationships.

Unlike a tree, a forest does not need a distinct name. A forest exists as a set of cross-referenced objects and trust relationships known to the member trees. Trees in a forest form a hierarchy for the purpose of trust. However, in DSfW, a forest contains a single tree that shares a common schema, configuration, and a global catalog.

**Forest Root Domain (FRD)**

The domain that provides the base (foundation) directory forest. It is usually the first domain that you create in your directory forest and is known as the default forest root domain.

**Group**

A set of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists.

**Group Policy**

An infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings reside in the Group Policy objects (GPOs). GPOs are linked to directory service containers, such as sites, domains, or organizational units (OUs). These settings are then evaluated by the impacted targets, using the hierarchical nature of the directory. A Group Policy allows you to manage user and computer objects.

**Mapped Tree/Setup**

An eDirectory tree where one or more eDirectory partitions are configured as DSfW domains and are mapped as a partition root object to a domain root. The fully qualified domain name of the DSfW forest root domain might be different from the X500 DN of the root of the DSfW forest.

**Non-Mapped Setup**

Creates a new eDirectory tree with the DNS naming format instead of the traditional X.500 naming format. The DSfW domain partitions in the tree are created at the time of provisioning.

**Microsoft Management Console (MMC)**

A component of modern Microsoft Windows operating systems.

It provides system administrators and advanced users with a flexible interface through which they can configure and monitor the system.

**NetBIOS**

Network Basic Input/Output System.

A network operating protocol that the NetBIOS API use to allow applications on different computers to communicate over a local area network. In modern networks, it normally runs over TCP/IP (NBT), giving each computer in the network both a NetBIOS name and an IP address corresponding to a (possibly different) hostname. Older operating systems ran NetBIOS over IPX/SPX or IEEE 802.2 (NBF). NetBIOS provides services related to the session layer of the OSI model.

**Object-Sid**

A single-valued identifier that specifies the security identifier (SID) of the user. The SID is a unique value used to identify the user as a security principal. User objects, group objects and computer objects, among others, are security principals. A SID is a binary value set by the system when the user is created.

**Partition**

1. A logical division of a computer hard disk created in order to have different operating systems on the same hard disk or to create the appearance of having separate hard disks for such activities as file management.
2. A logical group of objects in an eDirectory tree, used to provide better management of the tree.

**Replica**

A copy or instance of a user-defined partition that is distributed to another eDirectory server.

**Relative ID Master (RID Master)**

Every domain controller assigns RIDs to the security principals it creates. The RID master FSMO role holder is the single domain controller responsible for processing RID Pool requests from all DCs within a given domain. It is also responsible for removing an object from its domain and putting it in another domain during an object move. In the DSfW environment, the server holding the master replica of the domain acts as a RID master.

**Root Partition**

A unique partition created when the tree is installed.

**Schema Partition**

A partition that stores the definitions for the type of data that can be held by the directory store. Directory services rely on schema partitions for maintaining data consistency. In addition, applications can refer to the schema partition to determine the type of data that the directory forest allows. The schema can be extended to allow the directory to hold data that is specific to a particular application.

**Shortcut Trust**

A manually created trust that shortens the trust path within a forest to increase the speed at which authentications performed across domains in a forest are processed. This can result in faster authentication times and faster access to resources. A trust path is a chain of multiple trusts that enables trust between domains that are not adjacent in the domain namespace. For example, if users in the eng.novell.com domain need to gain access to resources in the sales.novell.com domain, the novell.com domain must be traversed because it is on the trust path. You can create a shortcut trust between eng.novell.com and sales.novell.com, bypassing novell.com in the trust path.

**Trusted Domain Object**

A critical object that represents the trust relationship between the two domains. It is found in the partition container under configuration partition. It directly relates to the trust relationships displayed in the Active Directory Domains and Trusts administrative tool. If the Trusted Domain Object is not present in DSfW, cross-domain authentication fails and results in errors. Shortcut trust objects are created when there is more than one domain in the forest.

**Trust-Posix-Offset Attribute**

An offset that the system uses to generate POSIX user and group identifiers that correspond to a given SID. To generate a POSIX identifier, the system adds the RID from the SID to the POSIX offset of the trusted domain identified by the SID.