Domain Services for Windows Administration Guide

Open Enterprise Server 2.0 SP3

May 06, 2013

Novell.

Contents

19 Troubleshooting

A Executing Provisioning Tasks Manually

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.

This guide is divided into the following sections:

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/feedback.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).

Additional Documentation

For information about security issues and recommendations for Novell Domain Services for Windows see *OES 2 SP3: Novell Domain Services for Windows Security Guide*

1 Overview of DSfW

Domain Services for Windows (DSfW) is a suite of technologies in Open Enterprise Server (OES) 2 SP1 and later versions that allows Microsoft Windows users to access OES services through native Windows and Active Directory protocols. By allowing OES Linux servers to behave as if they were Active Directory servers, this technology enables companies with Active Directory and Novell eDirectory deployments to achieve better coexistence between the two platforms. Users can work in a pure Windows desktop environment and still take advantage of some OES back-end services and technology, without the need for a Novell Client on the desktop.

Administrators can use either Novell iManager or Microsoft Management Console (MMC) to administer users and groups. Network administrators manage file systems using the native tools of each server, and they can also centrally administer Samba shares on OES Linux/ DSfW servers by using iManager.

Administrators can use MMC to create inter-domain trusts between DSfW domains and Active Directory domains.

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.

Domain Services for Windows is not a meta-directory or a synchronization connector between eDirectory and Active Directory. It does not do desktop emulation. Domain Services for Windows can only run on SUSE Linux Enterprise deployments of Open Enterprise Server 2 SP1 and later.

1.1 Features and Benefits

DSfW is designed to simplify the network infrastructure in mixed Windows/OES 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 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 SP3 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 SP3 and Microsoft Management Console (MMC) for Windows, thus eliminating the need for re-training.

  Network administrators can manage file systems using the native tools of each server, as well as centrally administer Samba shares on OES Linux/DSfW servers using iManager. Administrators can use MMC to create one-way cross-forest trusts between DSfW domains and Active Directory domains. For example, Windows server/workstation policy settings in the domain Group Policies can be changed by using MMC.

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

- **Single Password to Login:** One of the biggest benefits Domain Services for Windows provides end users is it eliminates multiple logins if they need access to both Active Directory- and eDirectory-based services. The trust relationship between eDirectory and Active Directory enables them to employ a single password for the services provided by either directory. From an IT perspective, this also greatly simplifies user management as objects for those users only need to be maintained in one directory repository instead of two.

1.2 Architectural Overview

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

Figure 1-1   *DSfW Components*
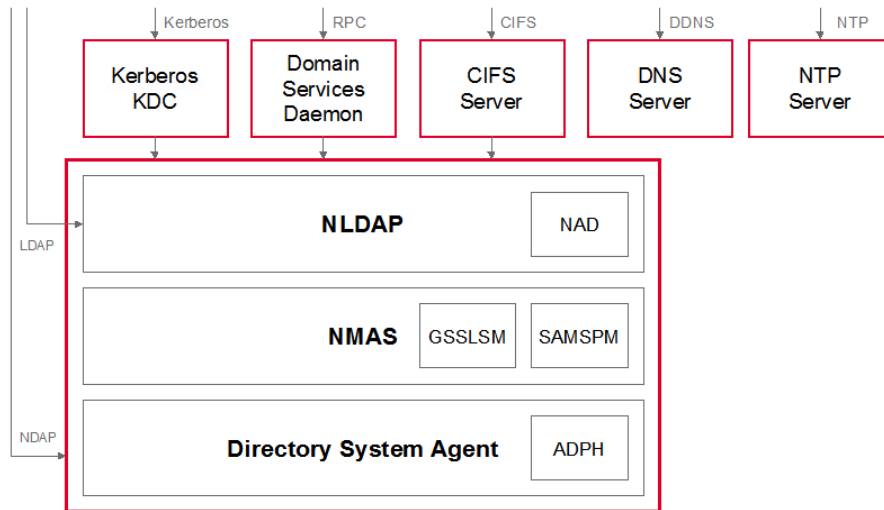
DSfW is made up of the following technologies:

- **eDirectory:** eDirectory 8.8 SP2 and above supports DSfW.

- **Kerberos Key Distribution Center (KDC):** Provides Active Directory-style authentication.

  NOTE: This is a KDC specifically developed for DSfW. It is different from the Novell Kerberos KDC (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 and OES 2.

- **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 14
- Section 1.3.2, "Naming," on page 14
- Section 1.3.3, "Security Model," on page 15
- Section 1.3.4, "Groups," on page 15

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.

Tree A DSfW tree consists of a single domain or multiple domains in a contiguous namespace.

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.

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).

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 Key Differences Between the DSfW LDAP Server and the eDirectory Server

Table 1-1 *Comparison of DSfW LDAP server and eDirectory server*

Function	DSfW LDAP Server	eDirectory Server
LDAP Operations like Search and Modify	Uses Domain Name format. For example: dc=eng, dc= novell.	Uses X.500 format. For example: ou=eng, o=novell.
Ports	When DSfW server is configured LDAP requests, such as Search and Modify, to a DSfW server on port 389 or 636 uses 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.	eDirectory uses ports 389 and 636 for communication purposes. The format used is X.500.
Semantic Controls	LDAP requests along with LDAP semantic controls (2.16.840.1.113719.1.513.4.5) allow LDAP requests to select X.500 or the domain format.	No support for semantic controls

Function	DSfW LDAP Server	eDirectory Server
Schema Addition	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. For more information, Attribute Mappings and Class Mappings.	
Search	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).	The search spans across partitions.
Multiple Instances	Not supported.	Supported.
Support for NT ACLs	No support for NT ACLs.	Directory objects are protected by proven eDirectory ACLs.
Domain Partition	Every DSfW server has a unique domain partition (required by the Active Directory security model).	No concept of domain partition.

For both DSfW server and LDAP server, login authorization and auditing is performed by using NMAS. Data on the wire is encrypted as mandated by the workstations. All keys, including Kerberos and NTLM, are encrypted by using a per attribute NICI key.

2 What's New

This section describes additions to the Novell Domain Services for Windows (DSfW) service for the Novell Open Enterprise Server 2 (OES 2):

2.1 What's New (OES 2 SP3 April 2013 Patches)

Upgrade to eDirectory 8.8.7

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

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

2.2 What's New (OES 2 SP3 November 2012 Patches)

In addition to bug fixes, the DSfW service provides the following enhancement and behavior change in the November 2012 Scheduled Maintenance for OES 2 SP3:

Script to Address NTP-Signed Requests

NTP- signed requests from Windows clients can now be addressed by using the `cross_partition_ntp_setup.pl` script. For more information, see "DSfW Fails to Set Up Signed NTP for Clients to Trust" in the *OES 2 SP3: Domain Services for Windows Administration Guide*.

2.3 What's New (OES 2 SP3 August 2011Patch)

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

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

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

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

2.4 What's New (OES 2 SP3)

- The domain boundary can be extended to include multiple partitions. This can be done either during install or post install. For more information, see Section 5.4, "Extending a Domain Boundary in a Name-Mapped Installation," on page 35.

- The domain name and RDN of a mapped container can be different. For instance, the partition ou=example,o=organization can be mapped to a domain named dsfw.com.

- Beginning OES 2 SP3, after successful mapping of a container to a DSfW domain, you can map any underlying container to a new DSfW child domain and skip any level of containers in between. For more information, see Deploying DSfW by Skipping Containers.

- The administrator name of a domain can be renamed post provisioning using MMC. For more information, see Renaming Administrator Details Using MMC.

- Beginning in OES 2 SP3, the DSfW provisioning wizard will not transfer the master replica of a mapped partition to the first Domain Controller of a DSfW domain. Due to this, there are certain implications on operations that assume the master replica to be present on the DSfW Domain Controller. One such operation is moving users into a DSfW domain. In this case, the moved user is not automatically samified. The samification of this moved user is initiated on the next eDirectory login, for instance using ndslogin.

  Alternatively, the domain administrator or the tree administrator can modify the moved user by setting an optional attribute (for instance description) and then revoking the change to initiate the samification of the moved user immediately. For a bulk move of users, it is recommended to use domaincntrl tool's samify operation to trigger the samification by selecting the partitions that the user's are moved to. For more information on implications of a user move into a domain, see Section 12.4.1, "User Samification Fails On Moving Users into a DSfW Domain," on page 167.

- DNS server can now be configured on a subsequent domain controller.

- Support to join Windows 2008 server as a member server to the domain.

2.5 What's New (OES 2 SP2)

- DSfW Installation and configuration are now handled in a two-step process:
  1. The YaST install prepares the server and the tree for domain users. This part of the process features restructured installation screens.
  2. A Provisioning Wizard, which is a separate utility that configures the DSfW server and supporting services, and completes the installation process.

- The SYSVOL is now located on every domain controller of each domain. This resolves the limitation resulting from having the SYSVOL only on the first domain controller of the domain.

- Support for Upgrade to OES 2 SP2.

3 Use-Cases

This section describes some common usage patterns that will help you in understanding the possibilities and functionalities of DSfW.

3.1 Authenticating to Applications That Require Active Directory-Style Authentication

This use-case can be described using the following scenarios:

3.1.1 Users Located in the DSfW Forest and Accessing Applications Hosted in the Active Directory Forest

In this case DSfW is deployed as an interoperable solution for organizations that have both eDirectory and Active Directory as part of their infrastructure. Most organizations use Active Directory-enabled applications which means that the application vendor has tested and certified his application against Active Directory for authentication and management.

By keeping the users in the DSfW forest and the applications in the Active Directory forest, organizations have the following advantages:

- Manageability is easier as the users reside on a single directory service and are not spread out. The company need not invest in network resources that may be required if the users were spread out.
- Applications can continue to be certified by the vendors for Active Directory as they are hosted on an Active Directory infrastructure. With the users residing on DSfW, there is no need to certify applications.

Figure 3-1   *DSfW users Accessing Resources on Active Directory*

Domain Services for Windows

Users

Cross–forest trust

Active Directory
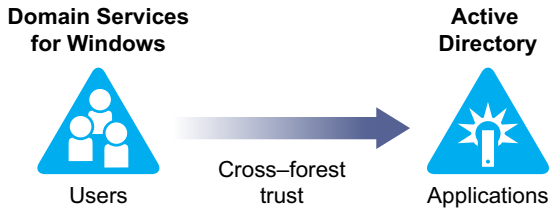
Applications

3.1.2   Users and Applications Hosted in the DSfW Forest

The applications in this use case are hosted in the DSfW infrastructure along with the users. This kind of deployment helps organizations to consolidate their Directory infrastructure.

While most of the application vendors specifically request Active Directory-support, as many applications are LDAP-enabled, the applications work seamlessly on DSfW.

However, some of the applications that have Active Directory-specific schemas may need additional effort in terms of schema extensions to work with DSfW.

Figure 3-2   *Users and Applications in DSfW Forest*

eDirectory

Applications

Users

W

Domain Services for Windows
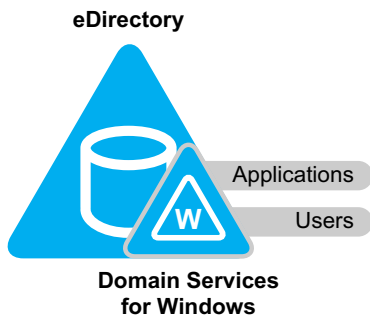
3.2   Working With Windows Systems Without Novell Client

DSfW allows Microsoft Windows users to work in a pure Windows desktop environment and still take advantage of some OES back-end services and technology, without the need for a Novell Client on the desktop.

Administrators can either use Novell iManager or Microsoft Management Console (MMC) to administer users and groups. Network administrators manage file systems using the native tools of each server, as well as centrally administer Samba shares on OES Linux/DSfW servers using iManager. Administrators can use MMC to create cross-forest trusts between DSfW domains and Active Directory domains.

When deployed in an environment that also supports NetWare Core Protocol (NCP), DSfW supports cross-protocol locking. Whether customers decide to use only Windows clients, NCP clients, or a combination of both, access rights for files is enforced by the Novell Storage Services (NSS) file system.

Novell Client does not need to be installed and managed as an extra software on the desktop. This helps in streamlining user experiences in terms of login to the directory and single login facility to both Active Directory applications and eDirectory services.

Figure 3-3 *Accessing applications without Novell Client*
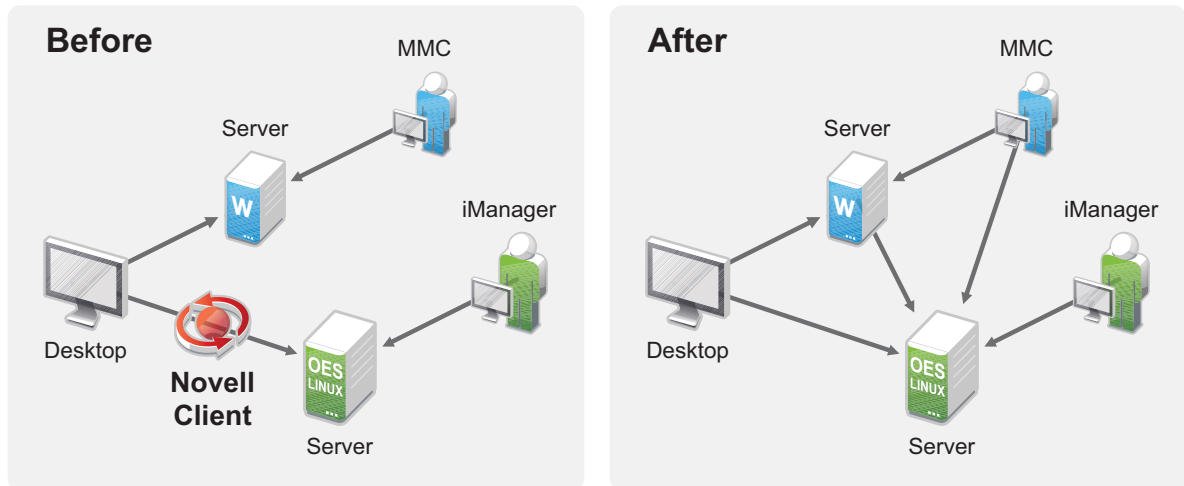
IMPORTANT: Do not install the Novell Client for Windows on a workstation for which you plan to provide native Windows access to DSfW servers. Novell Client access and native Windows access to DSfW servers do not work well together on the same workstation. But if you already have Novell Client installed on your workstation, we recommend that you follow the instructions in Joining a Workstation that Has Novell Client Installed

3.3 Leveraging an Existing eDirectory Setup

If you already have an eDirectory setup but want to install DSfW in your environment, it is recommended you utilise the existing eDirectory setup and install DSfW in a container in the existing eDirectory tree. This way you can utilise all the user information in the eDirectory container. This kind of setup is known as a name-mapped setup.

For more details on name-mapped setup, see Section 5.5.2, "Installation Prerequisites for a Name-Mapped Setup," on page 40 and Section 4.2, "Deploying DSfW in a Name-Mapped Setup," on page 25

3.4 Interoperability Between Active Directory and eDirectory

Trust relationships are key to managing Domain Services for Windows (DSfW). To facilitate communication between Windows and Linux environments you can create a trust to access resources from another domain. When a domain is installed, a trust is automatically established with its parent domain.

To assist you in doing this, 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 3-4 illustrates a typical deployment scenario in a mixed Novell/Microsoft environment.

Figure 3-4 *Cross-Forest Trust between Active Directory and DSfW*
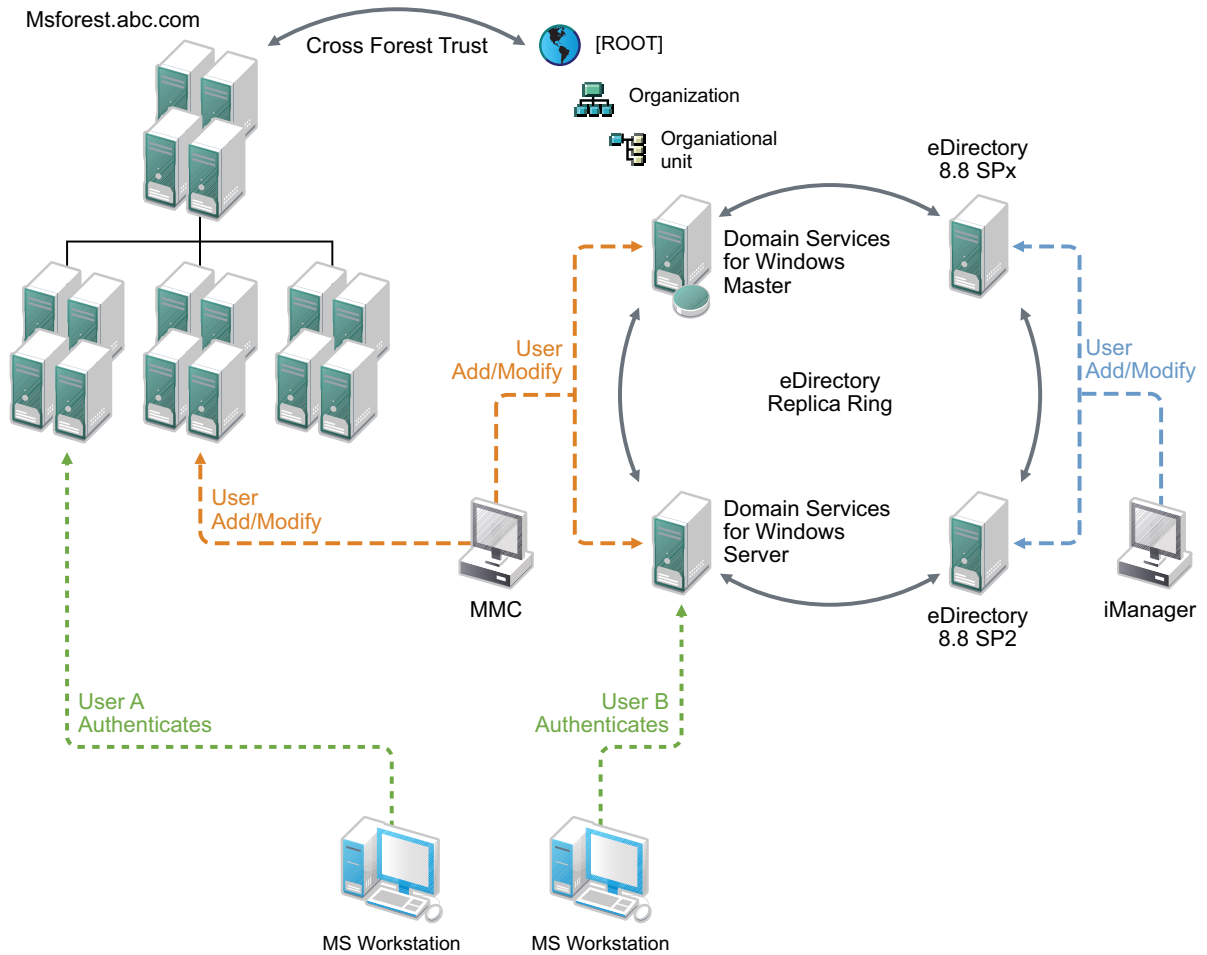
The diagram shows an Active Directory forest and a DSfW forest. Within the DSfW forest are two DSfW servers, an eDirectory 8.8 SP2 server, and an eDirectory 8.8 SPx server, configured in the same replica ring. Novell administrators can manage the domain by using iManager connected to any of these servers, 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 SP2 and above are replicated into the DSfW domain and can therefore access servers in the Active Directory forest.

4 Deployment Scenarios

This section describes deployment scenarios for name-mapped and non-name mapped scenarios:

4.1 Deploying DSfW in a Non-Name-Mapped Setup

A non-name-mapped setup refers to a setup that includes a new eDirectory Tree and a new DSfW forest as part of the DSfW installation. Before you start the process of installation, refer Installation Prerequisites For a Non-Name-Mapped Setup.

The scenarios explained here are only indicative of the various ways in which you can deploy DSfW server in your environment. Here the tree structure overlaps with the DNS namespace. For instance, the domain example.com will be mapped to dc=example,dc=com FQDN.

4.1.1 Deploying as a Single Domain

In this scenario, you have a single domain in the DSfW forest and have multiple DSfW servers acting as domain controllers in the domain.

Figure 4-1 *Deploying DSfW as a Single Domain*
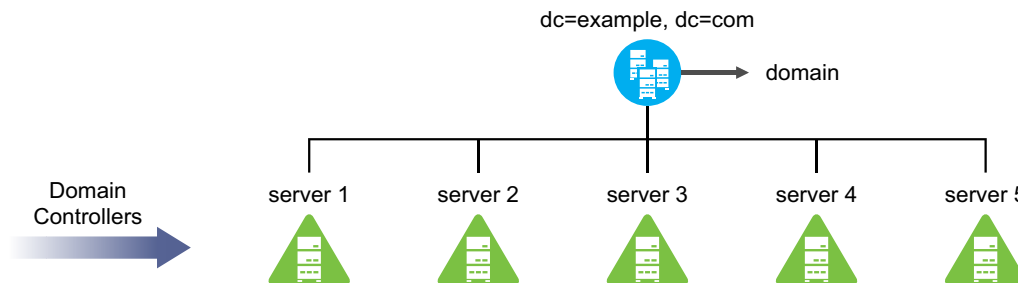
In Figure 4-1 the example.com domain is served by 5 domain controllers.

4.1.2 Deploying as Multiple Domains in a Forest

Width

In this scenario, the DSfW forest is spread out in an horizontal manner. You can have each branch office of the company configured as a separate domain belonging to one single DSfW Forest.

As represented in the figure, example.com is the first domain in the DSfW forest. It represents the head office of the company and the branch offices are represented by domains, America, India, Korea, China and Mexico.

Figure 4-2 *Deploying DSfW in a Horizontally Spread Tree*
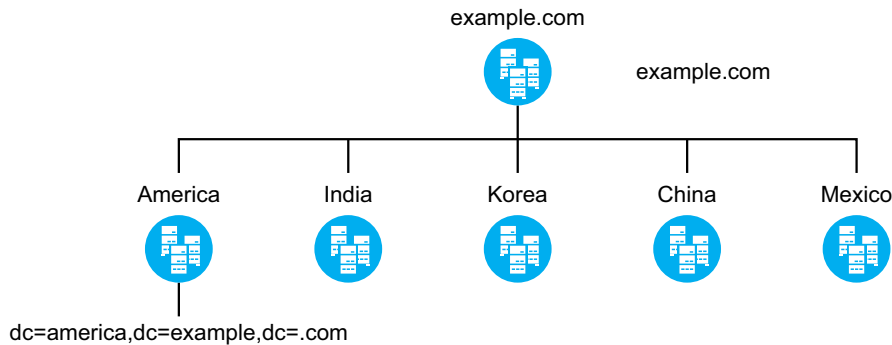
Depth

In this form of structuring, the tree is vertically structured and you can create different DSfW domains corresponding to each engineering and support function in the organization.

Figure 4-3 *Deploying DSfW in a Vertically Structured Tree*
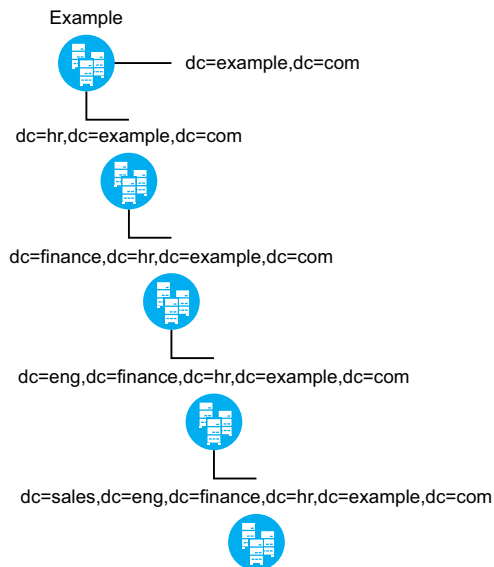
Depth and Width

With this combination you get benefits of a tree that is spread both horizontally and vertically. This is best suited for organizations that have offices locally as well as globally and there is a high requirement for load processing.

Figure 4-4 *Deploying DSfW in a Combination Structure*

dc=example,dc=com

Geographic (Regional)

dc=amerc   dc=pacrim   dc=europe

Geographic (Location)

dc=chi   dc=prv   dc=tkyo   dc=hnkg

Operational

dc=hr   dc=sales
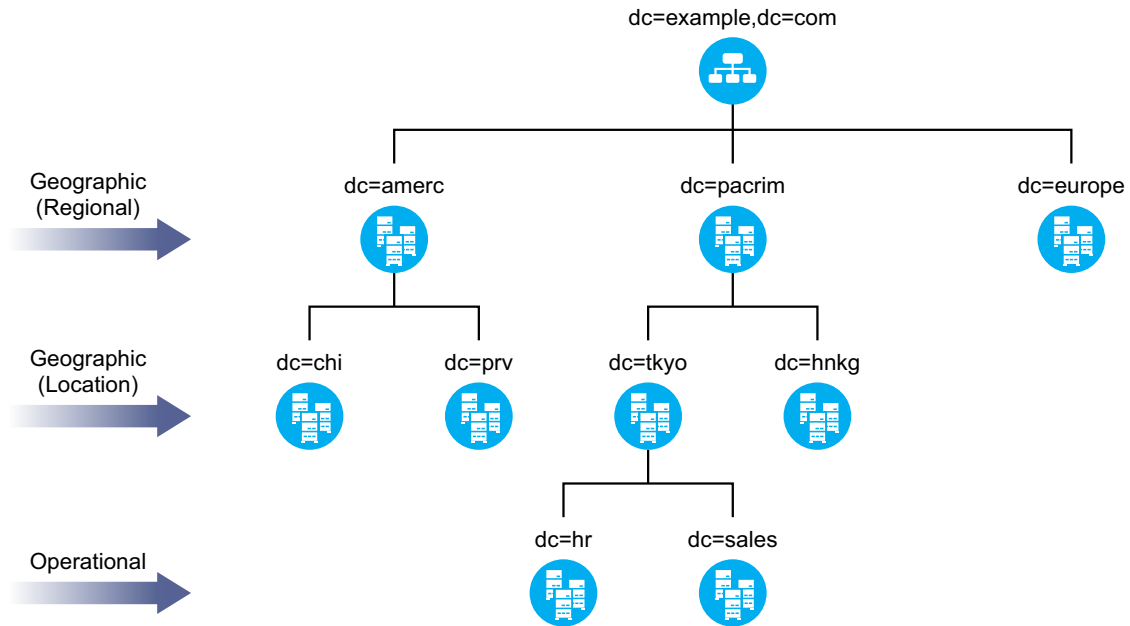
4.2 Deploying DSfW in a Name-Mapped Setup

A name-mapped setup refers to a setup where a new DSfW forest is created on an existing eDirectory tree using either a part or the entire eDirectory tree. This enables you to utilize all the user information and other associations in the eDirectory tree. The creation of a DSfW forest into an existing eDirectory tree starts from a specific container. Association of the DSfW forest to a specific container is called mapping and the container is called a mapped container. Different DSfW domains in the DSfW forest are mapped to different DSfW containers. As a prerequisite, the mapped containers must be partitioned.

Though an already existing eDirectory tree can be used for a name-mapped setup, an OES server already configured as an eDirectory server cannot be used to create a domain controller for a DSfW domain. A new server should be added to configure a DSfW domain controller. Before you start the process of installation, refer Installation Prerequisites for a Name-Mapped Setup.

Figure 4-5 represents an example of a name-mapped setup where an existing eDirectory tree T=Global has organization type containers America, Asia, and Europe. Consider a scenario where the container Asia needs to be mapped to a DSfW domain asia.com. As a prerequisite, you must first partition the Asia container and then introduce a new OES server in your eDirectory tree and install DSfW pattern. With successful installation and provisioning of DSfW, the container O=Asia becomes root partition of the DSfW domain. This allows you to utilize all the preexisting users and associations under the subtree starting from the container Asia.

Figure 4-5 *Deploying DSfW in an Existing eDirectory Tree*
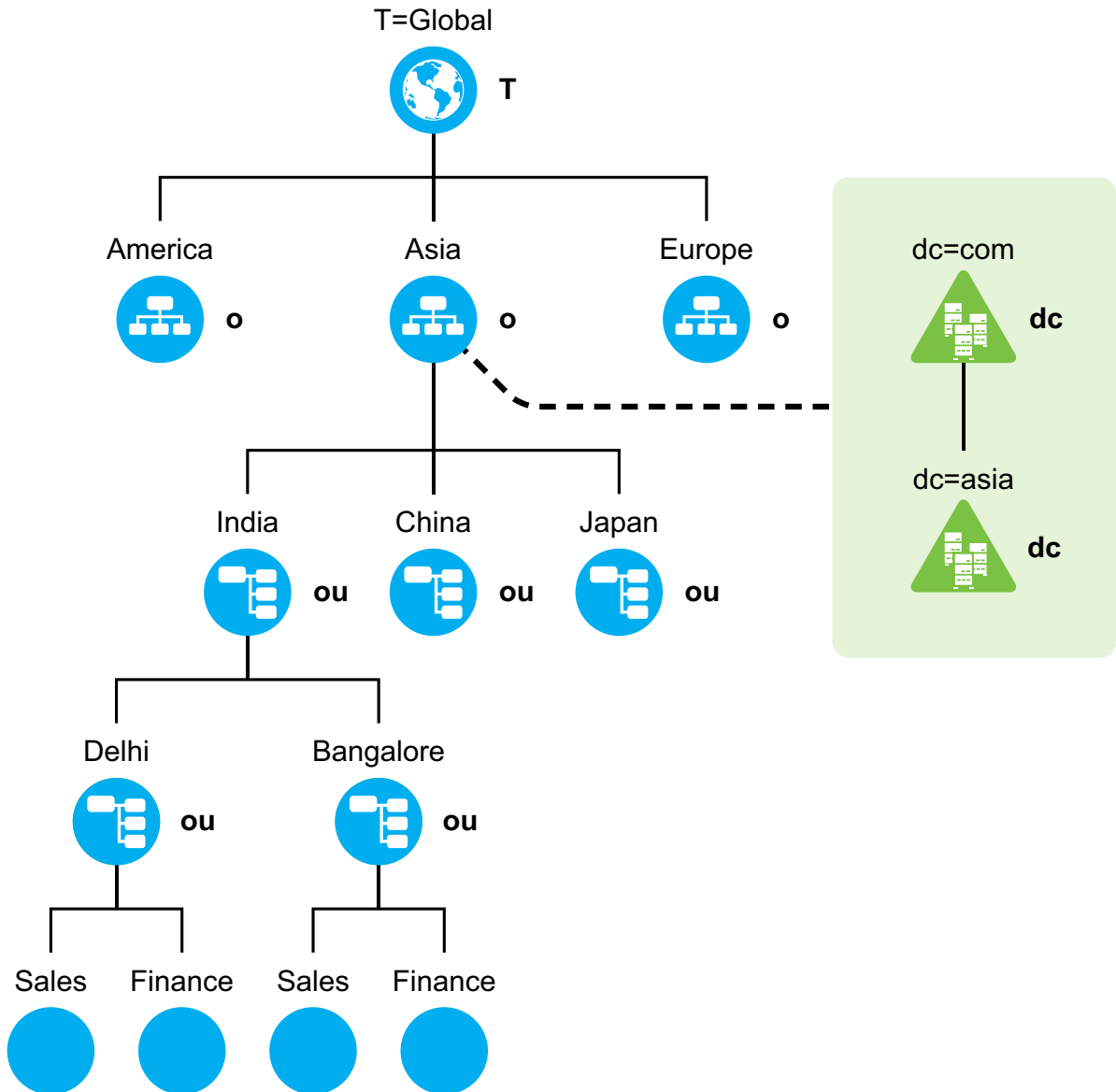
It is also possible to map the partitions underneath O=Asia to a new child domain and skip any levels of containers underneath. Refer section Section 4.2.1, "Deploying DSfW by Skipping Containers," on page 27. So, you can map the OU=India partitioned container to create a new child DSfW domain or directly map OU=Delhi or OU=Sales partitioned container.

Restrictions

Consider the following restrictions while configuring a name-mapped setup:

◆ If you have already mapped a partition to a DSfW domain, then you cannot map the sibling partitions to create a new DSfW domain. Using the example in Figure 4-5, if you have already mapped the O=Asia partition, you cannot map the O=America or O=Europe partitions. However, this restriction is applicable only for the first domain or FRD in a forest. For example, in Figure 4-5, the sibling containers under Asia (ou=India,ou=China, and ou=Japan) can be configured as different child domains in the same instance.

- Installing DSfW in a tree root partition is not supported.

- While designing a DSfW tree, you must ensure that the length of the DN does not exceed 255 characters. During provisioning, DSfW creates some objects and length of the DN of these DSfW-specific objects is included while calculating the length of the DSfW domain's mapped container. The size of longest default object in a DSfW tree is 144. While calculating the length of the mapped container, the length of the hostname is also taken into consideration. For example, if the hostname is myserver, then the mapped container's DN cannot exceed 255-144-8 (length of the hostname myserver)=103 characters. For more information on provisioning, see Chapter 7, "Provisioning Domain Services for Windows," on page 123.

WARNING: If you deploy the forest root domain too deep down in the tree, further child domain installation may be difficult because the DN mapping range will exhaust.

4.2.1 Deploying DSfW by Skipping Containers

For OES releases prior to OES2 SP3, to map any container in a tree, it was essential to map the parent container and skipping a container at any level was disallowed. However, beginning OES2 SP3, after successful mapping of a container to a DSfW domain, you can map any underlying container to a

new DSfW child domain and skip any level of containers in between. For instance, the second level container from a mapped container can be mapped to the immediate DSfW child domain, thus skipping the first level container.

Consider a scenario with an eDirectory tree, as represented in the following figure.

Figure 4-6 *Existing eDirectory Tree*
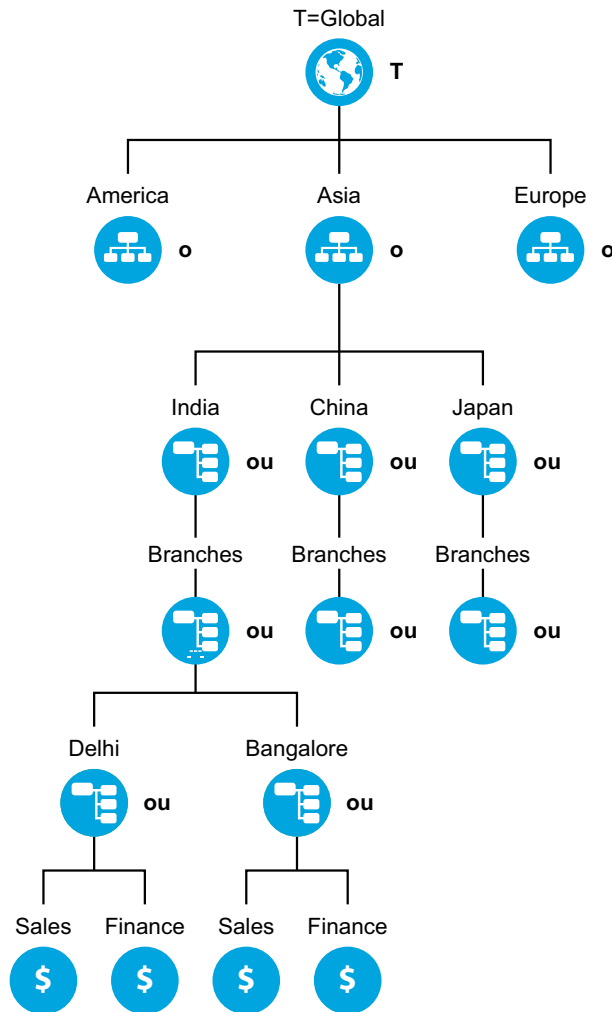
As illustrated in Figure 4-7, a domain named asia.com is created which is mapped to the partition o=asia. Now, you can map the partition ou=bangalore to a child domain named blr.asia.com, by excluding the partitions between the domains asia.com and blr.asia.com. The child domain excludes the partition ou=branches. This provides you with an advantage of avoiding an unnecessary server addition and its management in order to maintain the hierarchy.

Figure 4-7 *Deploying DSfW by Skipping Containers*
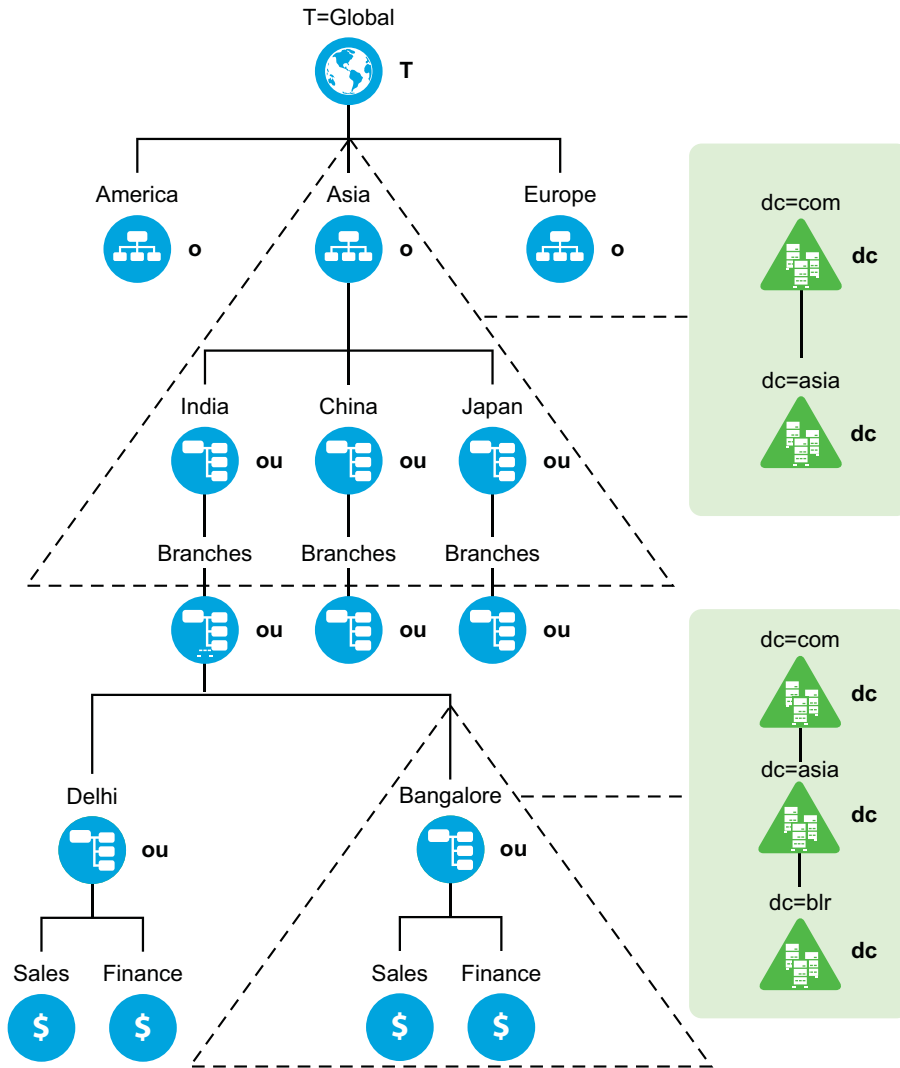
4.2.2 Custom Domain Name

DSfW enables you to choose a domain name that need not match the mapped container's typeless RDN. As illustrated in Figure 4-7, you can map the partition ou=bangalore to a DSfW child domain named blr.asia.com. Here the domain component blr is used to map a container with typeless RDN as bangalore.

5 Planning for DSfW

This section describes requirements and guidelines for using the Novell Domain Services for Windows on a Novell Open Enterprise Server (OES) 2 server.

5.1 Server Requirements for Installing DSfW

To install DSfW, you need a server that meets the system requirements for SUSE Linux Enterprise Server (SLES) 10 SP4 and Open Enterprise Server 2 SP3. For more information, see "Installing OES 2 SP3 as a New Installation" in the *OES 2 SP3: Installation Guide*.

You should have access to the installation media for SLES 10 SP4 and OES2 SP3, either on physical CD/DVD media or on a networked installation source server. For more information about installing OES 2 SP3 from an installation source, see "Setting Up a Network Installation Source" in the *OES 2 SP3: Installation Guide*

NOTE: Ensure that only root account is created during the SLES installation because administrator or other Active Directory account names can conflict with the DSfW users.

5.2 Scalability Guidelines

This section describes the scalability guidelines that can assist you in planning your production environment for DSfW. The following guidelines can enable you to achieve optimal results for your specific environment:

- If the number of users in your environment is high (in thousands), it is recommended to use a dedicated server such as the Novell CIFS server for your file server needs. In such scenarios, the DSfW server should be used only as a domain controller managing domain logins.
- The number of domain controllers allocated per domain should depend on the number of domain users and domain logins made to a domain. For example, if the number of concurrent user domain logins is low, then fewer domain controllers are required. Otherwise, a high number of simultaneous domain logins necessitates the use of increased number of domain controllers.
- Load balancing and fault tolerance needs also determine the number of domain controllers allocated per domain. The guidelines for load balancing and fault tolerance should be applied to deduce the number of domain controllers allocated per domain.
- For enterprises that are spread across different geographical locations or that span different functions, you should configure separate domains for each geographical location or function. For each geographical location or function, you should have a dedicated domain that meets the needs of the particular geographical location or function. Having a dedicated domain helps in reducing the traffic between different geographical locations or functions.
- If you have multiple domains in your enterprise, you can use depth-wise or width-wise deployment. However, for depth-wise deployment, you must ensure that the length of the DN does not exceed 255 characters. For more information on this restriction, refer to "Restrictions" on page 26.

5.3 Deciding between Name-Mapped and Non-Name-Mapped Installation

Name-Mapped Installation: Installing DSfW in a name-mapped setup means you are installing DSfW in an existing eDirectory tree inside a specific container.

Before you install DSfW in an existing container, the container must be partitioned. In Figure 5-1 the existing container Asia is mapped to create a DSfW forest. After the mapping, all of the containers below the O= Asia container become part of the DSfW forest.

If you have mapped an existing container to a domain, you cannot map the sibling containers to create a domain. Using the example in Figure 5-1, if you have already mapped the O=Asia container, you cannot map the O=America or O=Europe containers. However, this restriction is applicable only for the first domain or FRD in a forest.

On the other hand, it is possible to map the containers underneath O=Asia to a domain.

It is not possible to map the tree root partition to create a DSfW forest.

IMPORTANT: In name-mapped installations, you install DSfW in an existing eDirectory tree inside a specific container. However, DSfW must be installed on a separate server and not on the server where eDirectory is installed.

Figure 5-1 *Name-Mapped Installation*
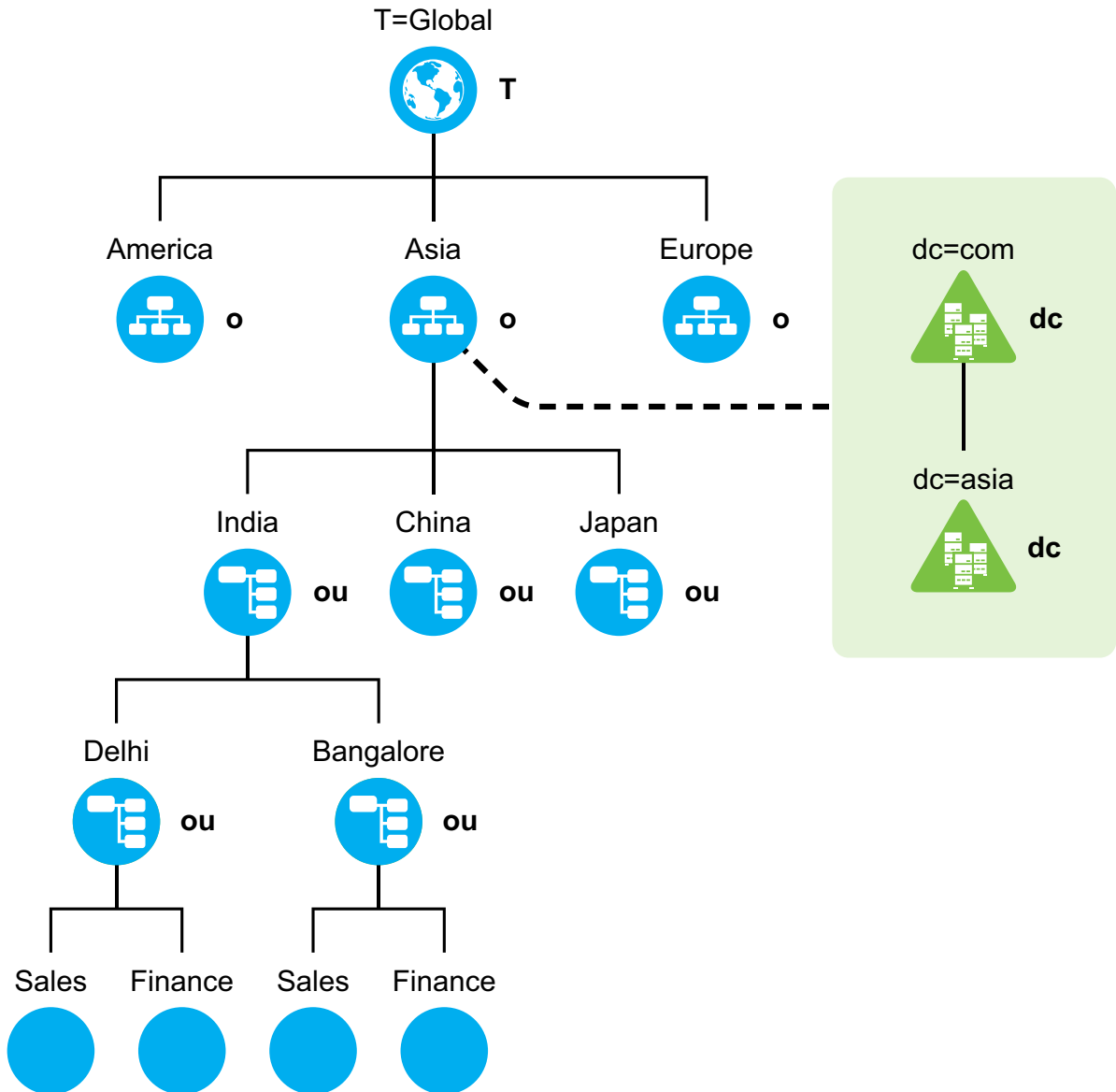
Non-Name-Mapped: In case of installing DSfW in a non-name-mapped setup, you are setting up a new tree in a DSfW forest. Here the tree structure overlaps with the DNS namespace.

Figure 5-2 *Non-Name-Mapped Installation*
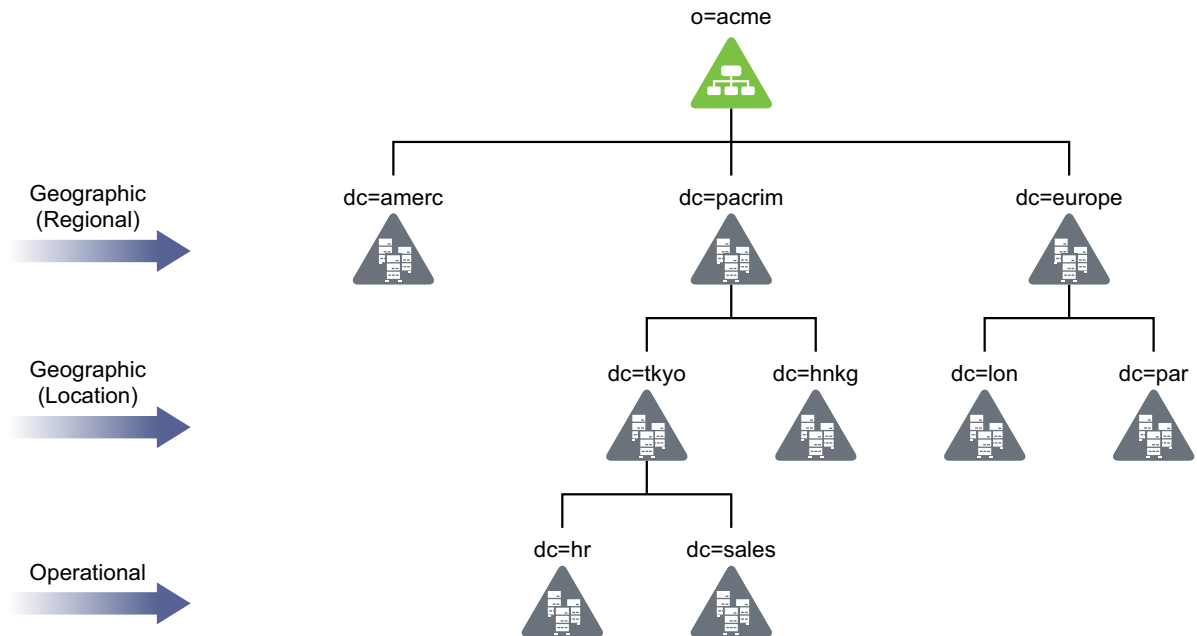
WARNING: A combination of non-name-mapped and name-mapped domain installations is not supported in a single DSfW forest. For example, you cannot install a name-mapped domain in a non-name-mapped installation scenario. To resolve issues arising out of such unsupported scenarios, you need to remove and then re-create the domain with the correct installation type.

5.3.1   Impact of a Name Mapped / Non-Name-Mapped setup on a Tree

This section analyses the various options of setting up a DSfW tree and the associated limitations.

- ◆ "Using a Pyramid Design" on page 34
- ◆ "Using a Flat Design" on page 35

Using a Pyramid Design

With a forest designed in the form of a pyramid, managing and initiating changes to large groups, and creating logical partitions are easier. This structure is best suited for large organizations with operations spread out across the globe.

Using a Flat Design

The alternative to the pyramid design is a flat tree that places all objects at one level of the tree. However, the flat tree design is not supported in DSfW.

DSfW can have only one top level domain and all the other domains need to be organized underneath the top level domain.

If you have mapped an existing container to a domain, you cannot map the sibling containers to create a domain. It is also not possible to partition the root container and map it to create a DSfW forest.

For more information, see Designing the eDirectory Tree (http://www.novell.com/documentation/edir871/?page=/documentation/edir871/edir871/data/a2iiidp.html)

5.4 Extending a Domain Boundary in a Name-Mapped Installation

DSfW enables you to map multiple partitions to a domain. You can extend the partition of a domain by adding existing partitions to it. When you add an existing partition to the domain, the associated users and groups become a part of the DSfW domain. You can map multiple partitions to a domain either during DSfW provisioning or after the provisioning. To map multiple partitions to a domain post provisioning, see Extending the Domain Post Provisioning.

IMPORTANT: Consider the following guidelines:

- If you are extending the domain partition of a domain, ensure that all the domain controllers of the domain are running on OES 2 SP3 server.
- If a DSfW forest has multiple domains and you want to extend the domain partition of a domain, you must ensure that all the domains of the DSfW forest are on OES2 SP3. Otherwise, cross domain access and authentication will not work.
- If you have already mapped a partition to a DSfW domain, then you cannot map the sibling partitions to create a new DSfW domain. However, this restriction is applicable only for the first domain or FRD in a forest.

5.4.1 Prerequisite

After completing the DSfW configuration and before initiating the provisioning process, you must ensure that the required replicas are present on the local server. However, for ADC installation, ensure that all replicas that are already part of the domain are present on the local server.

NOTE: The supported replica type is either read-write or master.

5.4.2 Use Case Scenario

Consider a scenario where you have an existing eDirectory tree with ou=example,o=organization as the partition and you want to map this partition to the example.com domain.

NOTE: The RDN of the mapped partition need not match the domain name. For instance, the partition ou=example,o=organization can be mapped to dsfw.com.

Along with the ou=example,o=organization partition, there are some additional partitions such as ou=foo,ou=example,o=organization and ou=bar, ou=example,o=organization, that need to be mapped to the example.com domain. To add these partitions to the domain:

1 After the DSfW configuration is complete, launch the Provisioning Wizard by selecting the *DSfW Provisioning Wizard* option from YaST. Alternatively, you can execute the following script at the command prompt: `/opt/novell/xad/sbin/provision_dsfw.sh`.

2 Enter the authentication details in the login dialog box, depending on the scenario in which you are provisioning.

3 To customize provisioning, select the *Enable Custom Provisioning* check box, then click *OK*.
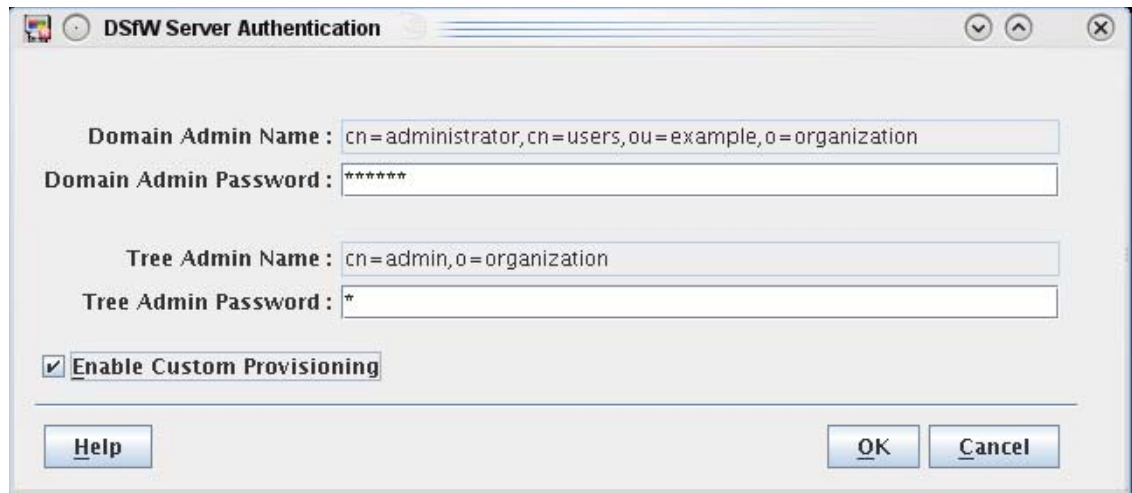
4 Select the partitions that you want to map to the domain. When you select a partition, validation checks are performed on the partition before mapping it to the domain. In this example, select the partitions ou=foo, ou=example,o=organization and ou=bar, ou=example,o=organization.
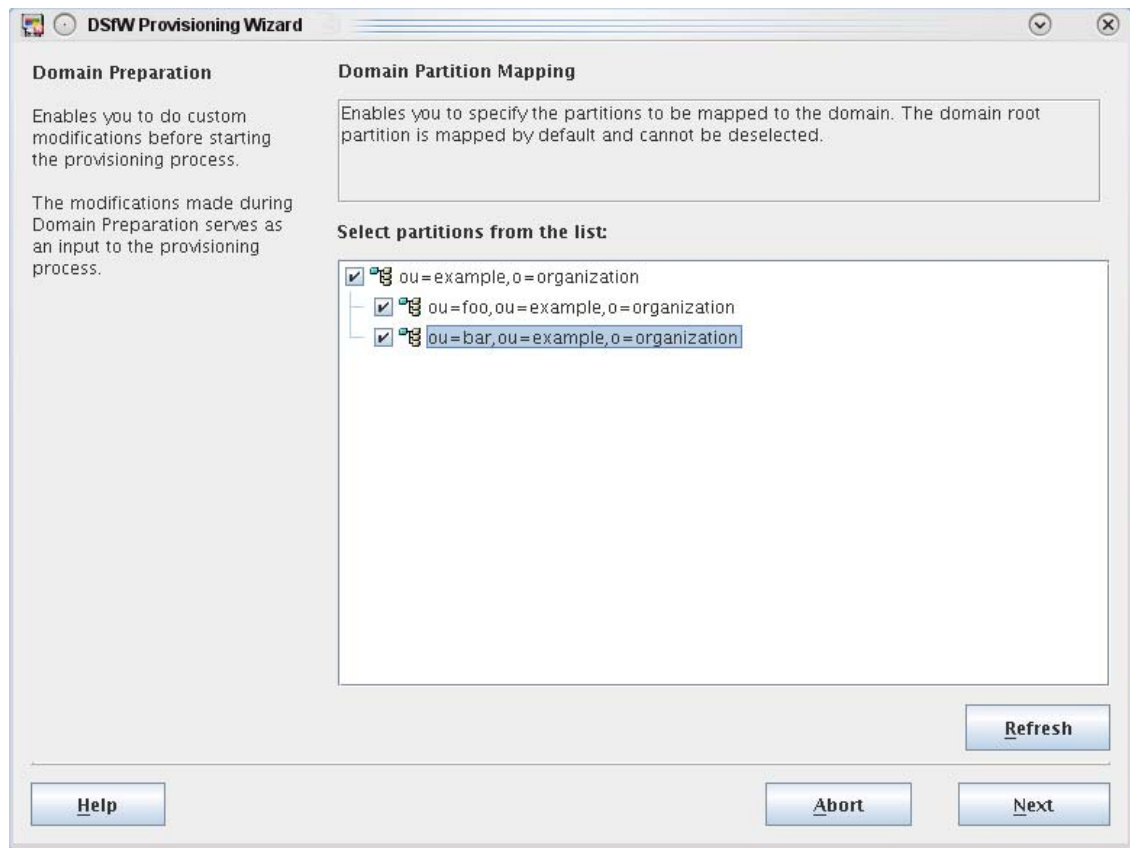
5 Click *Next* to continue with the DSfW provisioning process.

5.4.3 Caveat

While selecting the partitions, you must ensure that there is no gap between the partitions. If you select partitions that introduce gaps, partitions in between will also be selected automatically.

5.5 Meeting the Installation Requirements

Before you start the process of installation, ensure you have met the following prerequisites. These steps can be used to validate the state of the system before beginning the installation process.

- Section 5.5.1, "Installation Prerequisites For a Non-Name-Mapped Setup," on page 37
- Section 5.5.2, "Installation Prerequisites for a Name-Mapped Setup," on page 40

5.5.1 Installation Prerequisites For a Non-Name-Mapped Setup

- "Domain Name and Name Server Configuration is Correct" on page 38
- "DNS Server is Installed" on page 39
- "Time is Synchronized" on page 39
- "Server State in the Replica Ring" on page 40

Domain Name and Name Server Configuration is Correct

Before installing DSfW, ensure the domain name is entered correctly in YaST. To verify and correct the domain name, do the following:

1 Open *YaST>NetWork Configurations*. Select the *Hostname and Name Server* option.

2 Verify that the domain name is correct.

3 Select the *Write Hostnames to /etc/hosts* option to ensure that changes you have made gets added to the `/etc/hosts` files.

4 Verify that the Name Server 1 points to a DSfW domain controller that is also acting as the DNS server. By default the first domain controller of the first domain will always host the DNS server. However, for the first domain controller of the first domain, Name Server 1 must be the IP address of the local server. For details see, "DNS Server is Installed" on page 39.

IMPORTANT: In case of installation of a child domain, make sure you specify the name of the parent domain in the *Domain Search* field for resolving hostnames.

5 Click *OK* to save the changes.

DNS Server is Installed

Ensure that Novell DNS service is installed and the server is up and running to resolve name resolution queries.

In case of a first domain installation, the `/etc/resolv.conf` file must have an entry of the local DNS server. Whereas if it is child domain installation, the `/etc/resolv.conf` file must have the entry of the parent DNS server.

Time is Synchronized

Ensure time is synchronized between all servers in the replica ring by executing the following command:

```
ndscheck -a <bind dn> -w <password>
```

This command in addition to displaying partition and replica health also displays time difference between servers in the replica ring.

If you observe a time difference between the server, ensure that all the servers in the replica ring are referencing the same NTP server. After this is done, restart the NTP server by using the `rcntp restart` command.

Server State in the Replica Ring

Verify that the state of the servers in the replica ring is On by executing the following command:

```
ndsstat -r
```

The `ndsstat` utility displays information related to eDirectory servers, such as the eDirectory tree name, the fully distinguished server name, and the eDirectory version.

5.5.2 Installation Prerequisites for a Name-Mapped Setup

In case of a name-mapped installation, you are installing DSfW in an existing tree. To ensure the installation does not encounter errors, make sure you meet the following prerequisites:

- "Domain Name and Name Server Configuration is Correct" on page 40
- "eDirectory Version" on page 42
- "Container is Partitioned" on page 42
- "DNS Server is Installed" on page 42
- "Time is Synchronized" on page 43
- "Schema is Synchronized" on page 43
- "Server State in the Replica Ring" on page 43
- "Permissions for Objects" on page 43
- "Container Names" on page 43

Domain Name and Name Server Configuration is Correct

Before installing DSfW, ensure the domain name is entered correctly in YaST. To verify and correct the domain name, do the following:

1 Open *YaST>NetWork Configurations*. Select the *Hostname and Name Server* option.

Hostname and Name Server Configuration

Enter the name for this computer and the DNS domain that it belongs to.

Optionally enter the name server list and domain search list.

Note that the hostname is global–it applies to all interfaces, not just this one.

The domain is especially important if this computer is a mail server.

If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing *hostname* command) will be set automatically by DHCP client. You may want to disable this option if you connect to different networks that might each assign a different hostname, because changing the hostname at runtime may confuse the graphical desktop.

If you are using DHCP to get an IP address, your hostname will be written to /etc/hosts and be resolvable as 127.0.0.2 IP address. This is default behavior. If you want to disable this, uncheck this box but your hostname will not be resolvable without active network.

Enter the name servers and domain search list for resolving hostnames. Usually they can be obtained by DHCP.

Hostname and Domain Name (Global)

Hostname: dsfw-dc1

Domain Name: dsfw.com

☐ Change Hostname via DHCP

☒ Write Hostname to /etc/hosts

Name Servers and Domain Search List

Name Server 1: 192.168.108.3

Name Server 2:

Name Server 3:

Domain Search: dsfw.com

☒ Update Name Servers and Search List via DHCP

Back   Abort   OK

---

2 Verify that the domain name is correct.

3 Select the *Write Hostnames to /etc/hosts* option to ensure that changes you have made gets added to the `/etc/hosts` files.

4 Verify that the Name Server 1 points to a DSfW domain controller that is also acting as the DNS server. By default the first domain controller of the first domain will always host the DNS server. However, for the first domain controller of the first domain, Name Server 1 must be the IP address of the local server. For details see, "DNS Server is Installed" on page 39.

IMPORTANT: In case of installation of a child domain, make sure you specify the name of the parent domain in the *Domain Search* field for resolving hostnames.

5 Click *OK* to save the changes.

eDirectory Version

Before installing DSfW, ensure that the eDirectory version is 8.8 SP2 or greater. You must also ensure that the eDirectory version of the servers holding the writable replica of the tree root partition is 8.8 SP2 and above.

Container is Partitioned

The container in which you are installing DSfW must be partitioned.

DNS Server is Installed

Ensure that Novell DNS service is installed and the server is up and running to resolve name resolution queries.

In case of a first domain installation, the `/etc/resolv.conf` file must have an entry of the local DNS server. Whereas if it is child domain installation, the `/etc/resolv.conf` file must have the entry of the parent DNS server.

Time is Synchronized

Ensure time is synchronized between all servers in the replica ring by executing the following command:

```
ndscheck -a <bind dn> -w <password>
```

This command in addition to displaying partition and replica health also displays time difference between servers in the replica ring.

If you observe a time difference between the server, ensure that all the servers in the replica ring are referencing the same NTP server. After this is done, restart the NTP server using the `rcntp restart` command.

Schema is Synchronized

Ensure the schema is synchronized on all the servers in the replica ring by executing the following command on all the servers:

```
ldapsearch -b cn=schema -s base -x attributetypes=<schema attribute>
```

Substitute the schema attribute value with an attribute you have used in the schema.

For example: `ldapsearch -b cn=schema -s base -x attributetypes=`*xad-domain-flag*

Server State in the Replica Ring

Verify that the state of the servers in the replica ring is On by executing the following command:

```
ndsstat -r
```

The `ndsstat` utility displays information related to eDirectory servers, such as the eDirectory tree name, the fully distinguished server name, and the eDirectory version.

Permissions for Objects

When you are installing in a name-mapped setup, ensure that you have adequate permissions for the following objects in the tree:

- Container that is being provisioned
- Permissions for DNS Locator and Group objects
- Permissions to the Security container
- Modify permissions to the NCP servers holding replica of the master server

Container Names

When you are installing DSfW, it creates few default containers. Make sure that the following container names do not already exist under the domain partition:

- cn=Computers
- cn=Users
- ou=Domain Controllers
- cn=DefaultMigrationContainer
- cn=Deleted Objects

- cn=ForeignSecurityPrincipals
- cn=Infrastructure
- cn=LostAndFound
- cn=NTDS Quotas
- cn=Program Data
- cn=System
- cn=Container

5.6 Supported Installation Scenarios

The following installation scenarios are supported:

- Section 6.2.1, "Installing DSfW in a Non-Name-Mapped Setup," on page 49
- Section 6.2.2, "Installing DSfW in a Name-Mapped Setup," on page 85

5.7 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

5.7.1 Installing Other Products in the DSfW Partition

Novell doesn't support installing other Novell products within a Domain Services for Windows (DSfW) partition.

Some products might be supported in name-mapped implementations of DSfW. Consult the product documentation (http://www.novell.com/documentation) and the Novell Support site (http://www.novell.com/support) for confirmation before attempting such installations.

You should assume that an installation is not supported unless these sources indicate otherwise.

NOTE: This section refers to Novell products that are not included with OES 2, such as GroupWise. It doesn't apply to services included with OES 2, such as Novell iPrint.

Limitations for installing OES 2 services on the same server are outlined in Section 5.7, "Unsupported Service Combinations," on page 44.

5.8 Windows Version Support

The following table lists the version of Windows that is supported with DSfW:

Table 5-1 *Windows Version Support*

| OES Version | Member | | Cross Forest Trust Compatibility |
	Server	Client	
OES2 SP2	Microsoft Windows 2003 Server SP1 and SP2	Microsoft Windows 7 Microsoft Windows XP SP1, SP2, and SP3	Microsoft Windows 2003 Server SP1 and SP2 at the Windows Server 2003 forest functional level
OES2 SP3	Microsoft Windows 2003 Server SP1 and SP2 Microsoft Windows 2008 Server SP1 and SP2 Microsoft Windows 2008 R2 Server SP1	Microsoft Windows 7 Microsoft Windows XP SP1, SP2, and SP3	Microsoft Windows 2003 Server SP1 and SP2 at the Windows Server 2003 forest functional level

NOTE: Windows Server 2003 R2 as a member server is not supported. Windows 7 SP1 has not yet been tested with Domain Services for Windows, and therefore is not supported currently.

5.9 Administrative Tools

The following administrative tools are supported in DSfW:

◆ Section 5.9.1, "Windows Administration Tools," on page 45
◆ Section 5.9.2, "Linux Administration Tools," on page 45

5.9.1 Windows Administration Tools

From a Windows workstation the only tool supported to administer DSfW is Microsoft Management Console (MMC).

5.9.2 Linux Administration Tools

For managing DSfW server, use iManager.

5.10 Utilities Not Supported in DSfW

The following eDirectory utilities are not supported on a DSfW server

- ldif2dib - Utility to load data in to the eDirectory server
- ndsmerge - Utility to merge two eDirectory trees.

5.11 Limitations

Consider the limitations in this section when planning to install DSfW.

5.11.1 NETBIOS Names

The NETBIOS names are automatically configured from the DNS name you provide for the domain during the DSfW installation. We recommend you to not change the NETBIOS name.

In case you need to change the NETBIOS names, avoid using the following names:

- security
- schema
- linkengine
- administrator
- ndsschema
- ndscontainer

5.11.2 Installation Issue

DSfW cannot be installed on a server that is already running as an OES server. To install DSfW, you must do a fresh install of OES.

5.12 Restrictions with Domain Names

Domain names that end with `.local` are not supported with DSfW. For instance, avoid specifying a domain name such as `example.local`. This is because when a domain name ends with `.local`, the `.local` top level domain is regarded as a link-local domain and the DNS queries are sent to a multicast address instead of a normal DNS request.

5.13 Enabling Universal Password Policy for DSfW

As part of DSfW provisioning, the Universal Password Policy is enabled on the partition that is being mapped to a domain. Beginning with OES2 SP3, this is extended to cover all the partitions that are mapped to a particular DSfW domain.

However, if the Universal Password Policy is already enabled in your environment and if you don't want to override it, then you must select the *Retain existing Novell Password Policies on Users check box* during DSfW installation. For more information, see Step 9d. Beginning with OES2 SP3, selecting this check box will mean that the already enabled Universal Password Policy in your environment is

applicable to all the partitions that is being planned to be mapped to a particular DSfW domain. If you do not select this check box, then the users belonging to a partition (mapped to a DSfW domain) that does not have Universal Password Policy defined, will not be able to login to the DSfW domain.

For Universal Password Policies defined in your DSfW environment, you must ensure that you select the *Synchronize Distribution Password when setting Universal Password* check box in Novell 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*.

3 Select *Passwords > Password Policies*.

4 Click the password policy, then click *Universal Password > Configuration Options*.

5 Select the *Synchronize Distribution Password when setting Universal Password* check box.

If you do not select this check box, you will experience password synchronization issues.

6 Installing Domain Services for Windows

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

6.1 Prerequisites for Installation

Before you proceed with the installation, please review the details in "Planning for DSfW" on page 31.

6.2 Installation Scenarios

DSfW can be installed in the following scenarios:

6.2.1 Installing DSfW in a Non-Name-Mapped Setup

Installing a Forest Root Domain

Prerequisites: Before proceeding with this non-name-mapped installation, review Installation Prerequisites For a Non-Name-Mapped Setup.

1 In the YaST install for OES from *Software Selections* page, select *Novell Domain Services for Windows* pattern. Click *Accept*.

Ensure that *Novell DNS* is selected along with *Novell Domain Services for Windows*.

Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

For information about the entire OES 2 Linux installation process, see the *OES 2 SP3: Installation Guide*.

2 On the first eDirectory configuration page in YaST, select the *New Tree* option. This indicates that you are installing the first server in the tree:
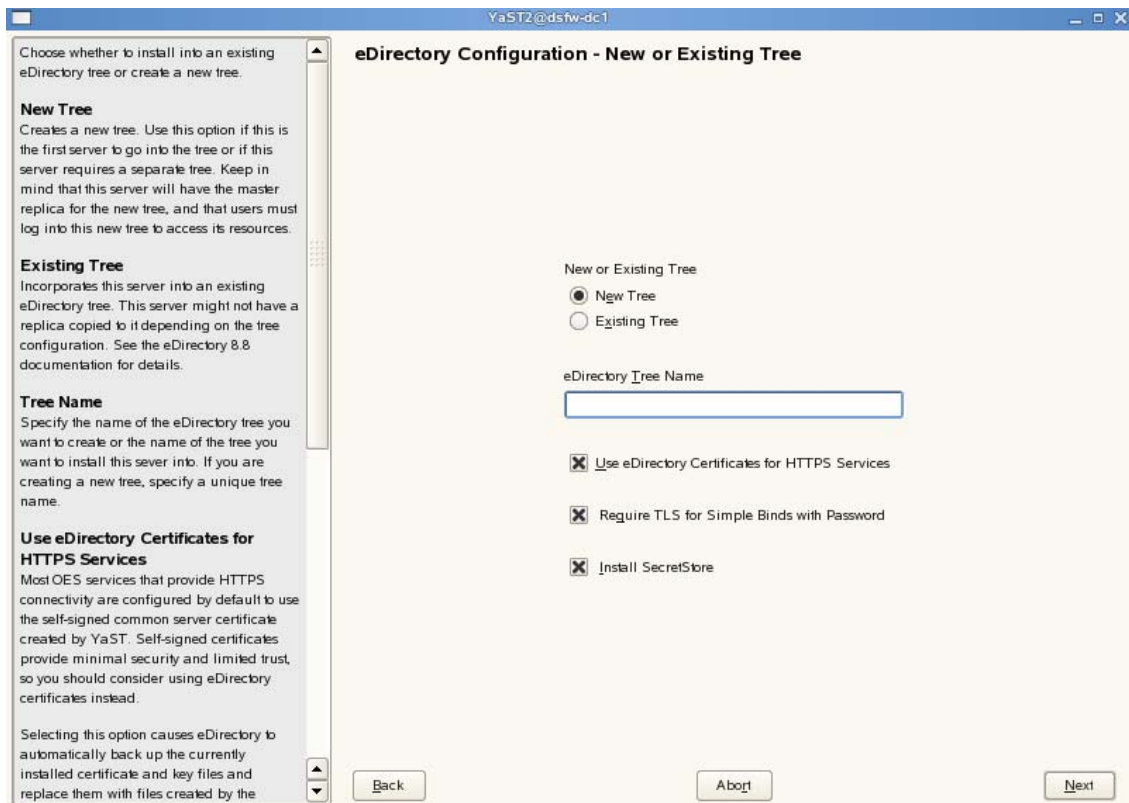
2a Select *New Tree* and specify a name for the tree. For example, DSfW-TREE.

2b 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. This option is selected by default.

2c Select the *Require TLS for Simple Binds with Password* option if you want to disallow clear passwords and other data.This option is selected by default.

2d Select *Install SecretStore* if you want to eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications. This option is selected by default.

2e Click *Next* to continue.

3 Specify the eDirectory administrator password in both fields, then click *Next*.

NOTE: The administrator name is hard-coded. However, after completing DSfW installation and configuration (post provisioning), you can modify administrator details such as the administrator name. For more information, see Section 8.2, "Renaming Administrator Details Using MMC," on page 146.

---

eDirectory Configuration - New Tree Information

FDN Admin Name with Context
Specify the name of the administrative user for the new tree. This is the fully distinguished name of a User object that will be created with full administrative rights in the new directory.

When specifying a context, you can use LDAP (comma delimited) or NDAP (dot delimited) format.

Admin Password
Specify the eDirectory administrator's password. This is the password of the user specified in the prior field.

Verify Admin Password
Retype the password to verify that you previously typed the intended password.

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

cn=Administrator,cn=Users,dc=dsfw,dc=com

Admin Password

•••

Verify Admin Password

•••

Back   Abort   Next
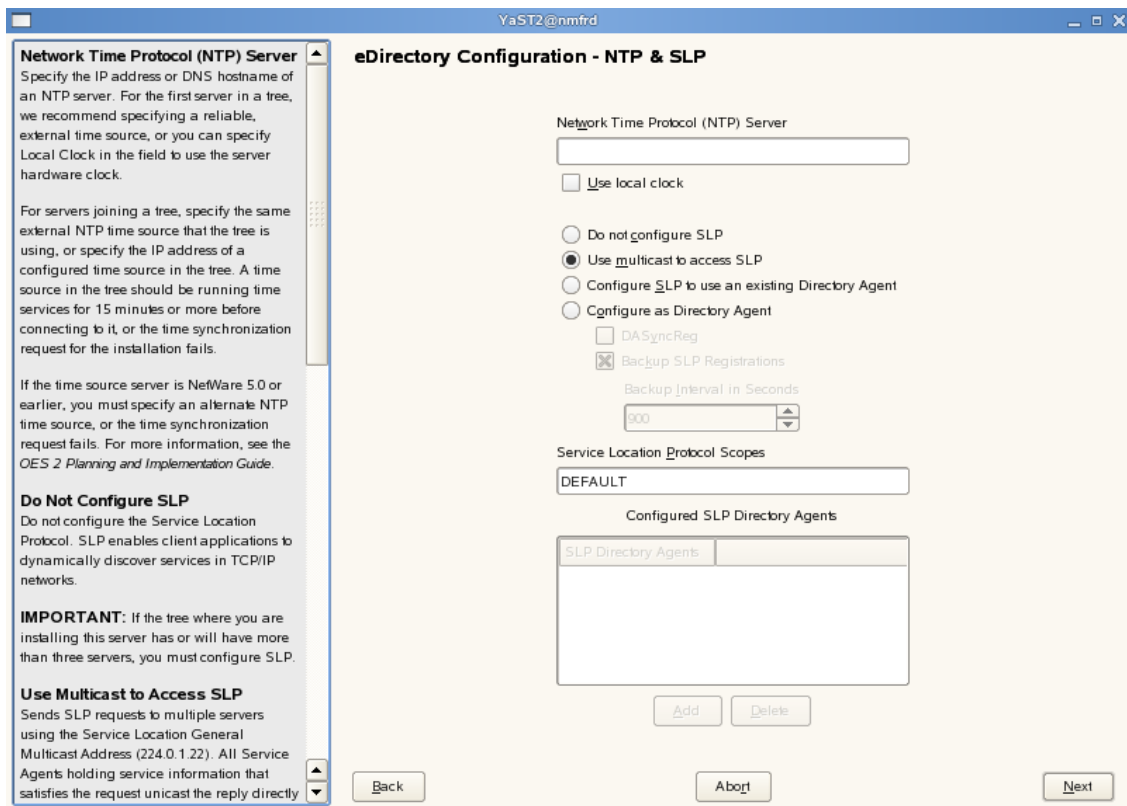
4 Specify the settings to configure the local server in the eDirectory tree.

4a Leave the location of the Directory Information Base (DIB) at the default setting.

4b Leave the *iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4c Leave the *Secure iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4d Click *Next* to continue.

5 Specify details for NTP and SLP.

5a 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.

5b Specify details to configure SLP:

5b1 If you do not want to configure the Service Location Protocol, select the *Do not configure SLP* option.

5b2 Select the *Use multicast to access SLP* option to request SLP information using multicast packet.

5b3 If you have more than three servers in your eDirectory tree, and you already have a Directory Agent running, select the *Configure SLP to use an existing Directory Agent* option.

5b4 Select the *Configure as Directory Agent* option if you want the local server to act as a directory agent.

   - Select the *DASyncReg* check box to enable SLP to query statically configured directory agents for registrations.

   - Select the Backup SLP Registrations check box to enable periodical backup of all registrations. In the *Backup Interval in Seconds* field, specify the time interval (seconds) to perform the backup.

5c Click *Next.*

6 Select the authentication service you want to install.

Click *Next*.

7 Specify details to configure DSfW on eDirectory.
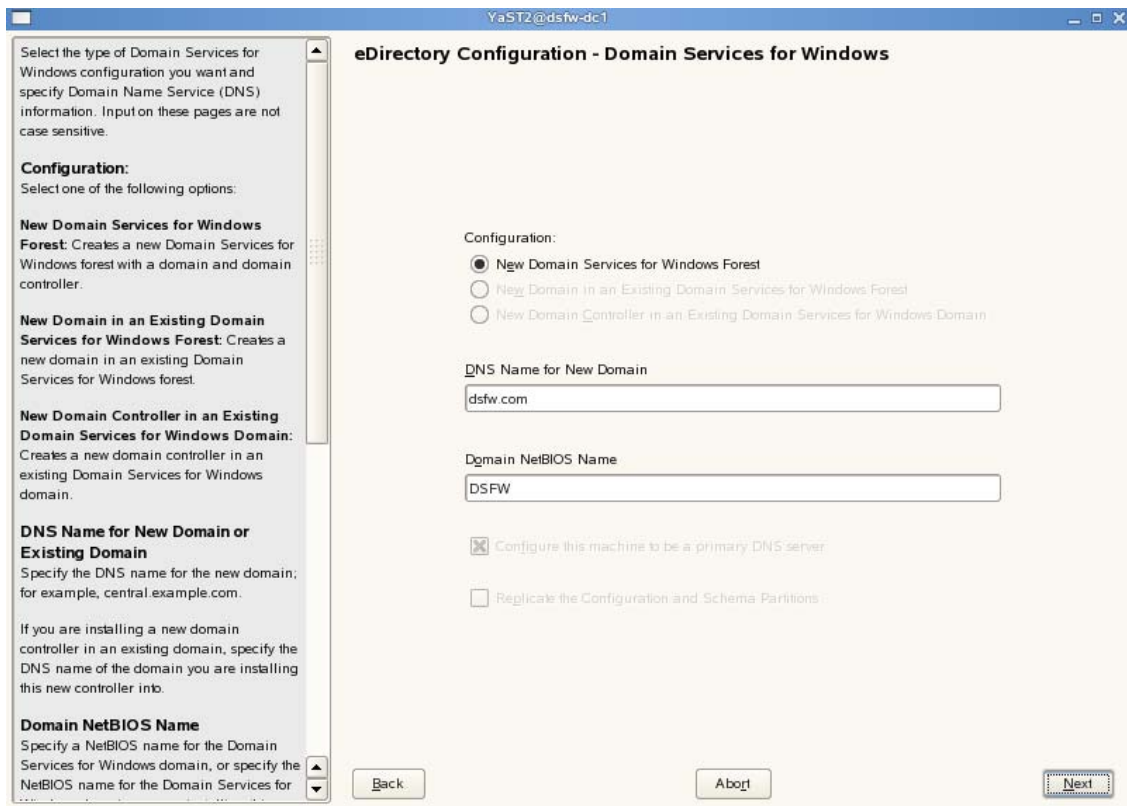
7a Select the *New Domain Services for Windows forest* option. This indicates that you are installing a new DSfW forest.

7b The *DNS Name for the New Domain* is by default taken from the entry in the `/etc/hosts` file. In case you need to change the domain name, make sure you follow the instructions in "Domain Name and Name Server Configuration is Correct" on page 38.

7c We recommend you to leave the NetBIOS name setting at the default, then click *Next* to continue.

For more information, see Section 5.11, "Limitations," on page 46

7d Click *Next* to continue.

8 Specify common proxy details.
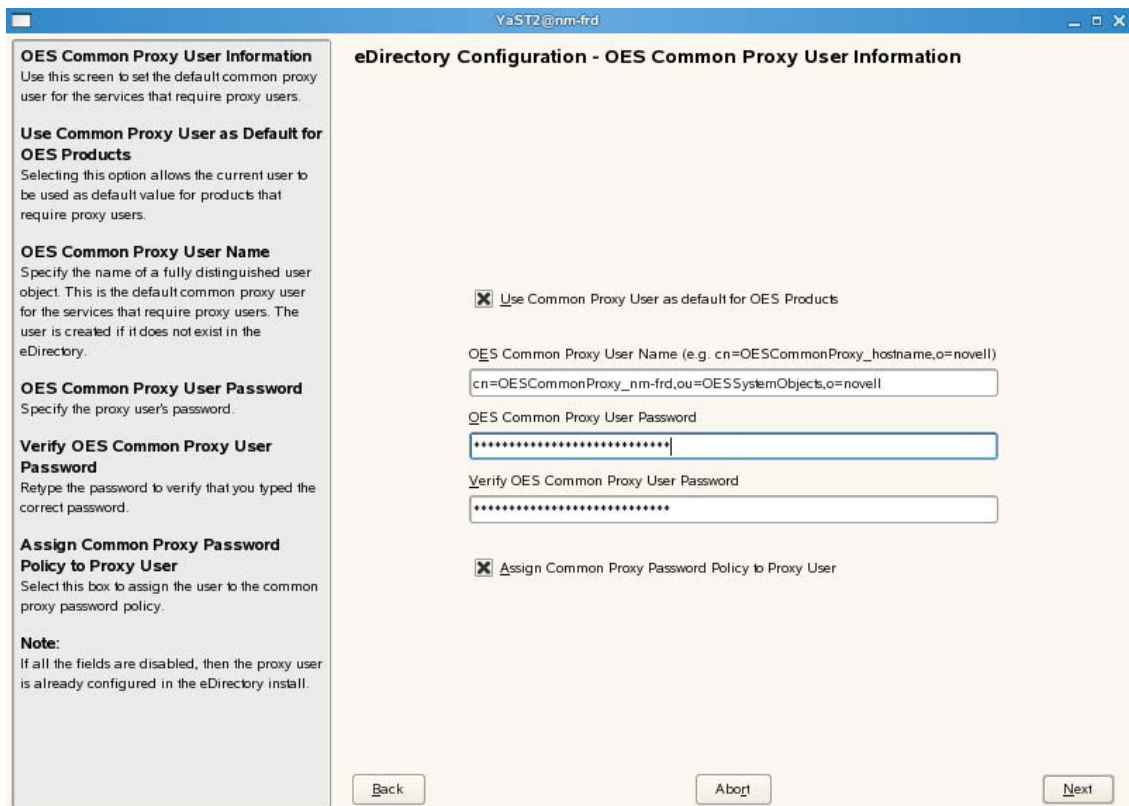
8a To use common proxy for DSfW, select the *Use Common Proxy User as default for OES Products* check box. When this check box is selected, the OES Common Proxy User Name and Password fields get enabled. These fields are populated with system generated user name and password. However, you can change these values. To change these values see Step 8b.

or

If you do not want to use common proxy, clear the check box and click *Next*. Then continue with Step 9.

8b Specify the following information:

- ◆ Common proxy user name in *OES Common Proxy User Name* field. You must specify a fully distinguished name.
- ◆ Proxy user password in *OES Common Proxy User Password* field.
- ◆ Retype the password in the *Verify OES Common Proxy User Password* field.

8c To assign common proxy password policy to proxy user, select the *Assign Common Proxy Password Policy to Proxy User* check box.

8d Click *Next* to continue.

9 Specify details to configure the DNS server.
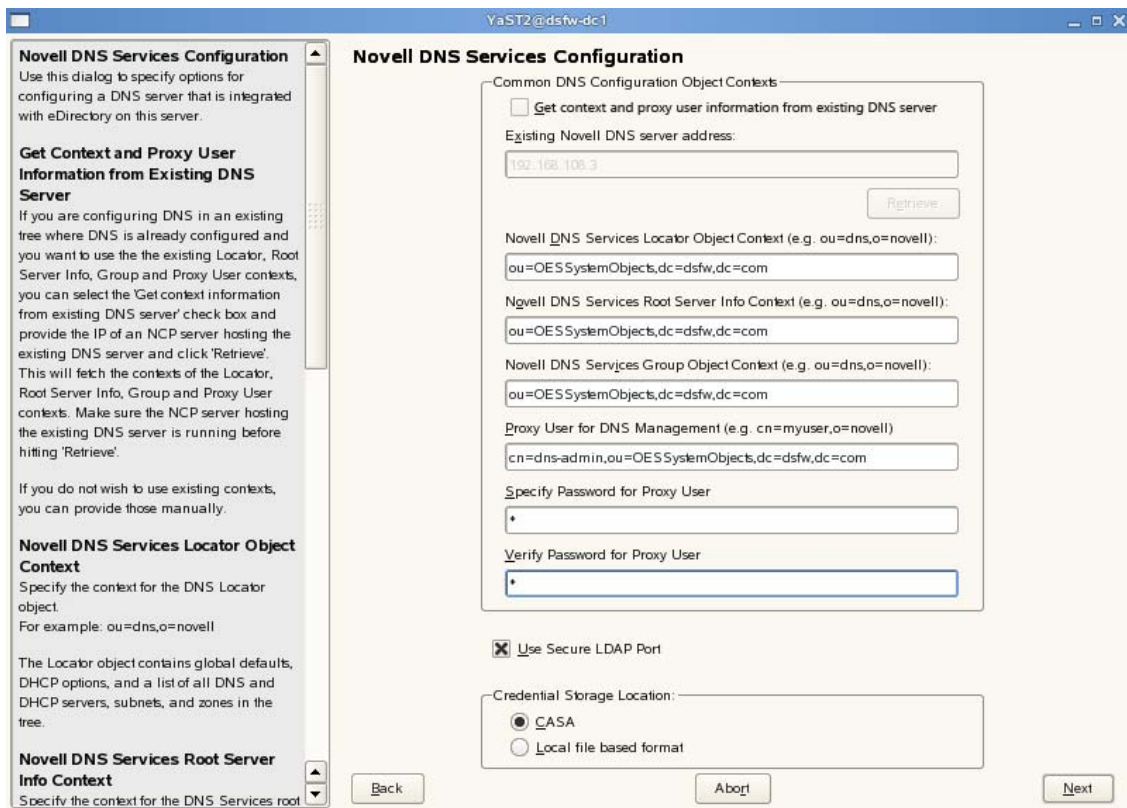
9a Specify the following information:

- Specify the context of the DNS service locator object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

- Specify the context of the DNS Root ServerInfo object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

- Specify the context of the DNS Services Group object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

9b Specify the fully distinguished, typeful name of the proxy user that will be used for DNS Management. For example: `cn=dns-admin,dc=dsfw,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.

9c Specify the password of the proxy user that you specified for accessing DNS.

> **NOTE:** If you have selected the *Use Common Proxy User as default for OES Products* check box in Step 8a, then the proxy user and password fields are populated with common proxy user name and password.

9d *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.

9e Specify the *Credential Storage Location* as CASA.

9f Click *Next* to continue.

10 After the installation is completed, the OES Configuration Summary page is displayed. Review the settings made earlier. Click *Next.*
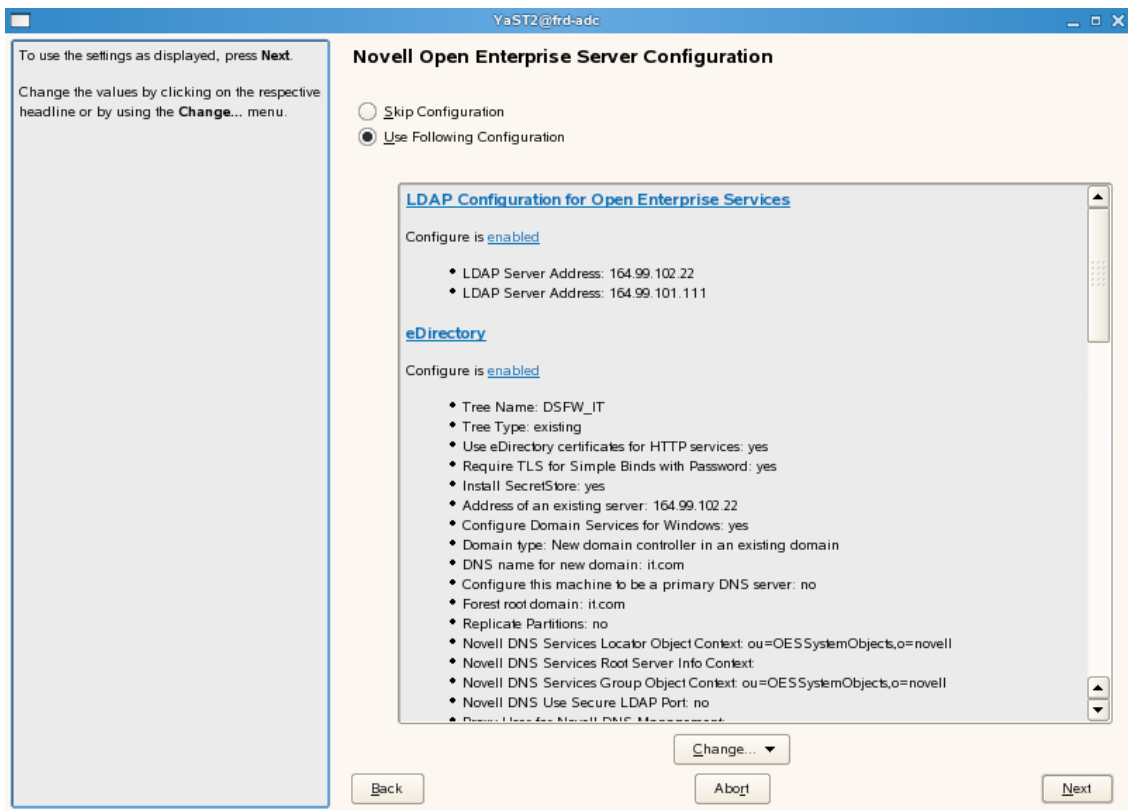
11 This starts the DSfW installation.When the installation is complete, click *Finish*.
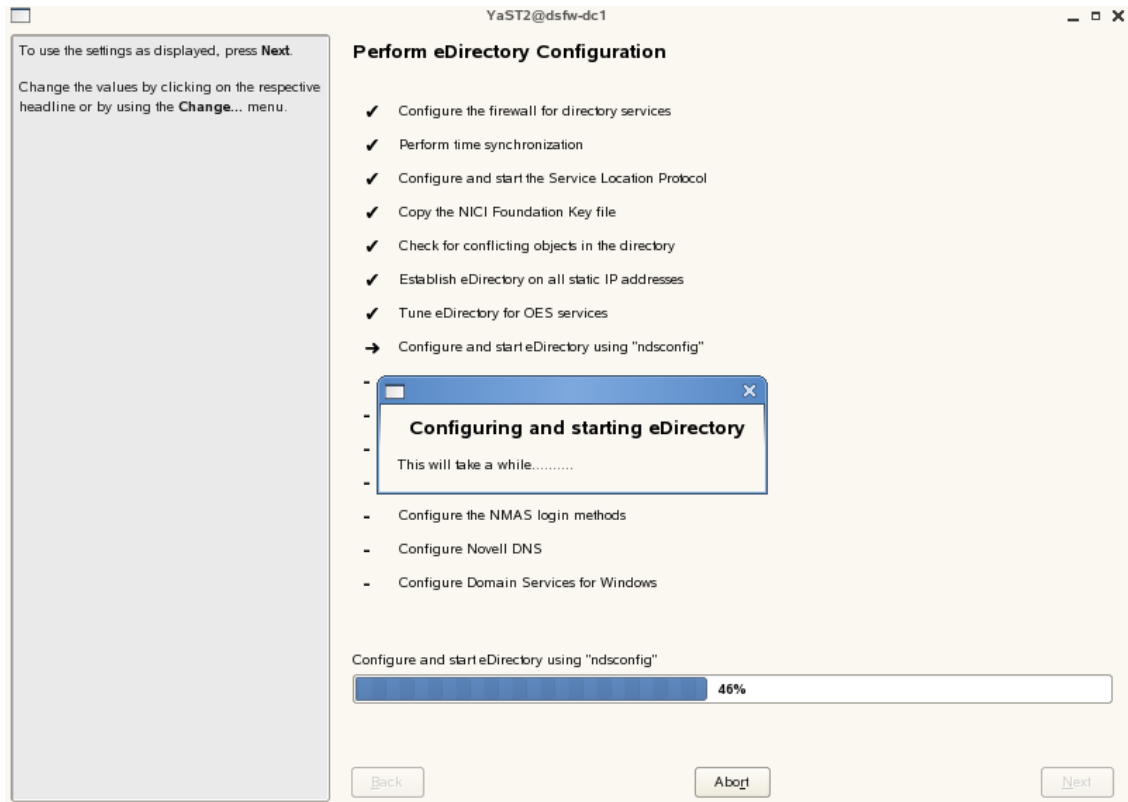
This completes the process of DSfW installation. But the server is not ready for use till you complete configuring DSfW and the supporting services through the process of provisioning.
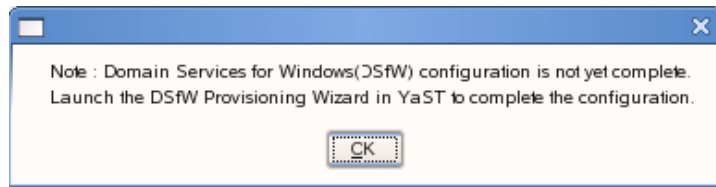
12 To start provisioning, do one of the following:

- ◆ From the terminal, run the `/opt/novell/xad/sbin/provision_dsfw.sh` script.
- ◆ Launch YaST. The DSfW Provisioning Wizard is listed as an option.

To authenticate, enter the password of the current domain.

For more details on Provisioning, see "Provisioning Domain Services for Windows" on page 123

13 The DSfW server is now ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by executing the instructions in Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145.

Installing a Child Domain

Prerequisites: Before proceeding with this non-name-mapped installation, review Installation Prerequisites For a Non-Name-Mapped Setup.

1 In the YaST install for OES from *Software Selections* page, select *Novell Domain Services for Windows* pattern. Click *Accept*.

Ensure that *Novell DNS* is selected along with *Novell Domain Services for Windows*.

Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

For information about the entire OES 2 Linux installation process, see the *OES 2 SP3: Installation Guide*.

2 On the eDirectory configuration page in YaST, select the *Existing Tree* option. This indicates that you are installing the server into an existing eDirectory tree:

2a Select *Existing Tree* and specify the name of the tree. For example, DSFW_TREE.

2b 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.

2c Select the *Require TLS for Simple Binds with Password* option if you want to disallow clear passwords and other data.

2d Select *Install SecretStore* if you want to eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications.

2e Click *Next* to continue.

3 Specify information to access the existing eDirectory Tree.

3a Specify the IP address of the Forest Root Domain.

3b Do not change the NCP Port, LDAP Port and Secure LDAP Port information.

3c Specify the tree admin credentials for the administrator to log into the eDirectory tree.

3d Click *Next*.

4 Select the settings for the local server configuration:

4a Leave the location of the Directory Information Base (DIB) at the default setting.

4b Leave the iMonitor port settings at the defaults unless you need to change them to avoid port conflicts with other services.

4c Leave the Secure iMonitor Port settings at the defaults unless you need to change them to avoid port conflicts with other services.

4d Click *Next* to continue.

5 Specify details for NTP and SLP.

5a 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.

5b Specify details to configure SLP:

5b1 If you do not want to configure the Service Location Protocol, select the *Do not configure SLP* option.

5b2 Select the *Use multicast to access SLP* option to request SLP information using multicast packet.

5b3 If you have more than three servers in your eDirectory tree, and you already have a Directory Agent running, select the *Configure SLP to use an existing Directory Agent* option.

5b4 Select the *Configure as Directory Agent* option if you want the local server to act as a directory agent.

  ◆ Select the *DASyncReg* check box to enable SLP to query statically configured directory agents for registrations.

  ◆ Select the Backup SLP Registrations check box to enable periodical backup of all registrations. In the *Backup Interval in Seconds* field, specify the time interval (seconds) to perform the backup.

5c Click *Next.*

6 Select the authentication service you want to install.

6a Click *Next*.

7 Specify details to configure DSfW on eDirectory.

7a Select the *New Domain in an Existing Domain Services for Windows forest* option. This indicates that you are installing a new domain in an existing DSfW forest.

7b The *DNS Name for the New Domain* is by default taken from the entry in the `/etc/hosts` file. In case you need to change the domain name, make sure you follow the instructions in "Domain Name and Name Server Configuration is Correct" on page 38.

7c Select *Configure this machine to be a primary DNS server* if you want the machine being configured to function as a DNS server.

> **IMPORTANT:** If you want to configure the child domain controller to act as a primary DNS server, ensure the DNS servers of the forest root domain and the child domain controller act as passive primary DNS servers of each other's zones, else the installation of an subsequent domain controller to the child domain controller fails.
>
> Also make sure you configure the forward lookup zone and the reverse lookup zone for this DNS server. For more information, see "Zone Management" in the *OES 2 SP3: Novell DNS/ DHCP Administration Guide*.

7d We recommend you to leave the NetBIOS name setting at the default, then click *Next* to continue.

For more information, see Section 5.11, "Limitations," on page 46

7e Click *Next* to continue.

8 Specify the name of the forest root domain in which you want to create the child domain.
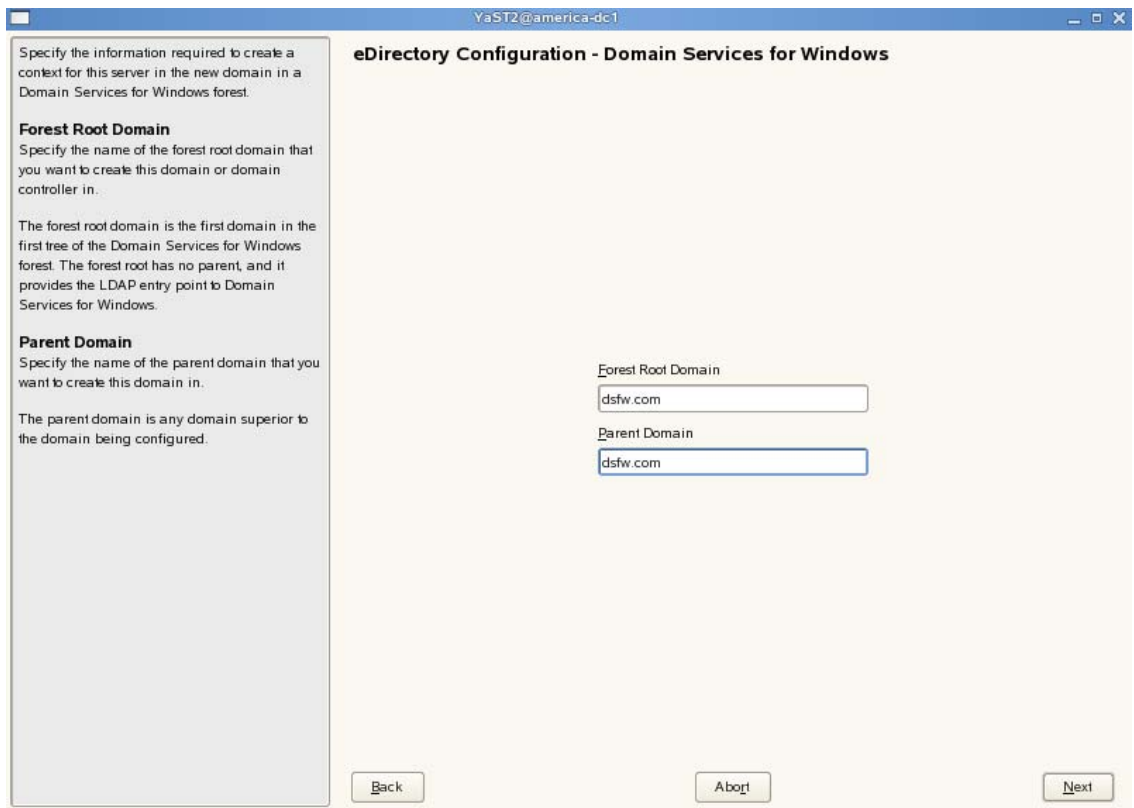
9 Specify the IP address of the parent domain, the administrator name and password.

> **NOTE:** The *New Domain Administrator Name* is hard-coded. However, after completing DSfW installation and configuration (post provisioning), you can modify administrator details such as the administrator name. For more information, see Section 8.2, "Renaming Administrator Details Using MMC," on page 146.

eDirectory Configuration - Domain Services for Windows

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

IP Address of Parent Domain
Specify the IP address of the domain that will be 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 Adminstrator 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.

New 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 the Administrator account shown in the previous field.

Verify Administrator Password
Retype the password to verify that you previously typed the intended password.

IP Address of the Parent Domain
192.168.108.3

LDAP Secure Port for the Parent Domain Server
636

Parent Domain Administrator Name
cn=Administrator.cn=Users.dc=dsfw.dc=com

Enter Administrator Password
•••

New Domain Administrator Name
trator.cn=Users.dc=america.dc=dsfw.dc=com

Specify Administrator Password
•••••

Verify Administrator Password
•••••

Back   Abort   Next

10 This screen is used when you need to map a new domain to an existing eDirectory container. As this is a non-name-mapped installation scenario, click *Next* to skip this screen.

NOTE: This screen is not displayed if the child domain is installed when the parent domain is on OES2 SP3.

11 Specify common proxy details.

11a To use common proxy for DSfW, select the *Use Common Proxy User as default for OES Products* check box. When this check box is selected, the OES Common Proxy User Name and Password fields get enabled. These fields are populated with system generated user name and password. However, you can change these values. To change these values see Step 11b.

or

If you do not want to use common proxy, clear the check box and click *Next*. Then continue with Step 13.

11b Specify the following information:

- Common proxy user name in *OES Common Proxy User Name* field. You must specify a fully distinguished name.

- Proxy user password in *OES Common Proxy User Password* field.

- Retype the password in the *Verify OES Common Proxy User Password* field.

11c To assign common proxy password policy to proxy user, select the *Assign Common Proxy Password Policy to Proxy User* check box.

11d Click *Next* to continue.

12 This screen is displayed if you have not selected the *Configure this machine to be a primary DNS server* check box in Step 7c. If you have selected this check box, continue with step Step 13.
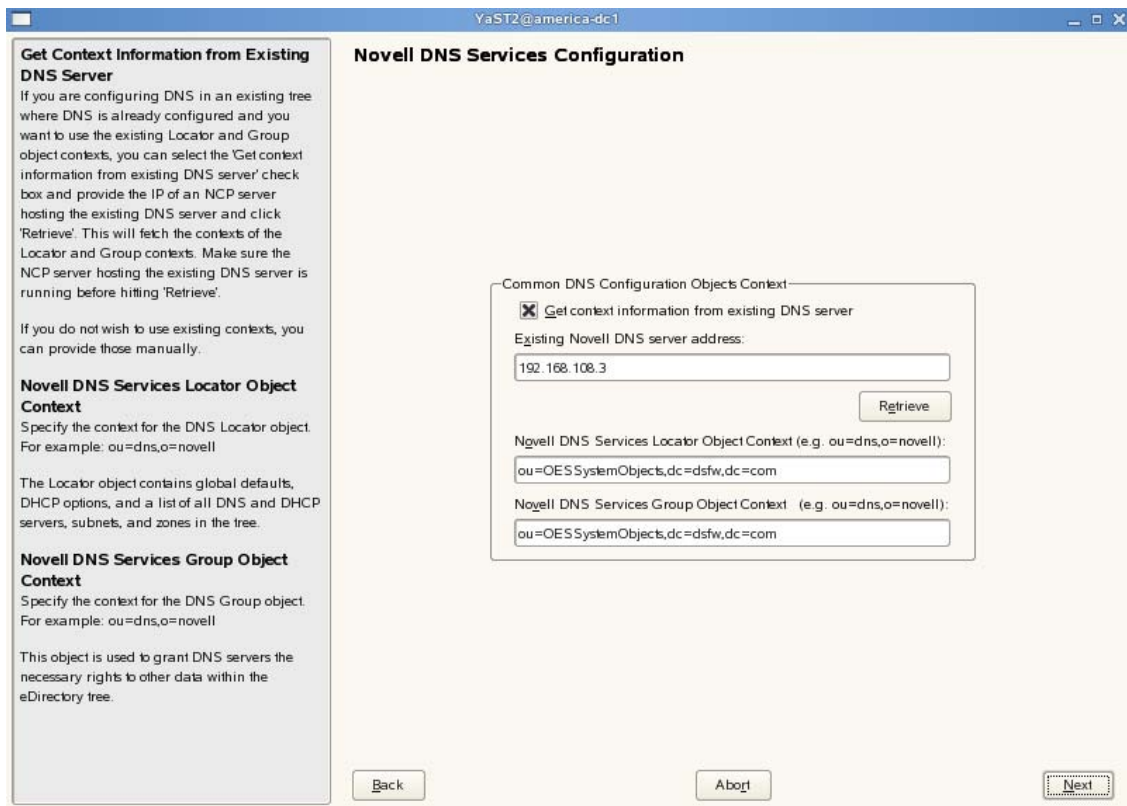
12a If you already have an DNS server configured in your tree, select the *Get context information from existing DNS Server* option and provide the IP address of an existing DNS server and select *Retrieve*.

This will fetch the contexts of the existing Locator and Group objects. If you do not wish to use the existing contexts, you can manually enter the details.

12b Specify the context of the DNS Locator object.

12c Specify the context of the DNS Group object.

Click *Next* and proceed with Step 14.

13 Specify details to configure the DNS server.

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 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: ou=dns,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

Novell DNS Services Configuration

Common DNS Configuration Object Contexts

☐ Get context and proxy user information from existing DNS server

Existing Novell DNS server address:
192.168.108.3

Retrieve

Novell DNS Services Locator Object Context (e.g. ou=dns,o=novell):
ou=OESSystemObjects, dc= child, dc=dsfw,dc=com

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

Novell DNS Services Group Object Context (e.g. ou=dns,o=novell):
ou=OESSystemObjects, dc= child, dc=dsfw,dc=com

Proxy User for DNS Management (e.g. cn=myuser,o=novell)
cn=dns-admin,ou=OESSystemObjects,dc= child, dc=dsfw,dc=com

Specify Password for Proxy User
*

Verify Password for Proxy User
*

☒ Use Secure LDAP Port

Credential Storage Location:
◉ CASA
○ Local file based format

Back   Abort   Next

13a If you are configuring DNS in an existing tree where DNS is already configured, select the *Get context and proxy user information from existing DNS server* check box. Specify the IP address 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. However, the proxy user password is not retrieved. Therefore, you must first retrieve the proxy user password and then specify the password manually in the proxy user password field. To retrieve the proxy user password, run the following command from the existing novell DNS server:

`/opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred password`

13b Specify the following information:

- Specify the context of the DNS service locator object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).
- Specify the context of the DNS Root ServerInfo object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).
- Specify the context of the DNS Services Group object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

13c Specify the fully distinguished, typeful name of the proxy user that will be used for DNS Management. For example: `cn=dns-admin,dc=dsfw,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.

13d Specify the password of the proxy user that you specified for accessing DNS.

NOTE: If you have selected the *Use Common Proxy User as default for OES Products* check box in Step 11a, then the proxy user and password fields are populated with common proxy user name and password.

13e *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.

13f Specify the *Credential Storage Location* as CASA.

13g Click *Next* to continue.

14 After the installation is completed, the OES Configuration Summary page is displayed. Review the settings made earlier. Click *Next*.

15 This starts the DSfW installation.When the installation is complete, click *Finish*.

This completes the process of DSfW installation. But the server is not ready for use till you complete configuring DSfW and the supporting services through the process of provisioning.

16 To start provisioning, do one of the following: For details on Provisioning, see

- ◆ From the terminal, run the `/opt/novell/xad/sbin/provision_dsfw.sh` script.
- ◆ Launch YaST. The DSfW Provisioning Wizard is listed as an option.

To authenticate, enter the password of the current domain, the parent domain and the tree admin.

For more details on Provisioning, see "Provisioning Domain Services for Windows" on page 123.

17 The DSfW server is now ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by executing the instructions in Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145.

Installing DSfW as a Subsequent Domain Controller in a Domain

Prerequisites: Before proceeding with this non-name-mapped installation, review Installation Prerequisites For a Non-Name-Mapped Setup.

1 In the YaST install for OES from *Software Selections* page, select *Novell Domain Services for Windows* pattern. Click *Accept*.

Ensure that *Novell DNS* is selected along with *Novell Domain Services for Windows*.

Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

For information about the entire OES 2 Linux installation process, see the *OES 2 SP3: Installation Guide*.

2 On the first eDirectory configuration page in YaST, select the *Existing Tree* option. This indicates that you are installing the server into an existing eDirectory tree.

2a Select *Existing Tree* and specify the name of the tree. For example, DSfW-TREE.

2b 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.

2c Select the *Require TLS for Simple Binds with Password* option if you want to disallow clear passwords and other data.

2d Select *Install SecretStore* if you want to eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications.

2e Click *Next* to continue.

3 Specify information to access the existing eDirectory Tree.

3a Specify the IP Address of the Forest Root domain.

3b Do not change the NCP Port, LDAP Port and Secure LDAP Port information.

3c Specify the tree admin credentials for the administrator to log into the eDirectory tree.

3d Click *Next*.

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

4a Leave the location of the *Directory Information Base (DIB)* at the default setting.

4b Leave the *iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4c Leave the *Secure iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4d Click *Next* to continue.

5 Specify details for NTP and SLP.

5a 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.

5b Specify details to configure SLP:

5b1 If you do not want to configure the Service Location Protocol, select the *Do not configure SLP* option.

5b2 Select the *Use multicast to access SLP* option to request SLP information using multicast packet.

5b3 If you have more than three servers in your eDirectory tree, and you already have a Directory Agent running, select the *Configure SLP to use an existing Directory Agent* option.

5b4 Select the *Configure as Directory Agent* option if you want the local server to act as a directory agent.

   ◆ Select the *DASyncReg* check box to enable SLP to query statically configured directory agents for registrations.

   ◆ Select the Backup SLP Registrations check box to enable periodical backup of all registrations. In the *Backup Interval in Seconds* field, specify the time interval (seconds) to perform the backup.

5c Click *Next*.

6 Select the authentication service you want to install.

6a Click *Next*.

7 Specify details to configure DSfW on eDirectory

    7a Select the *New Domain Controller in an Existing Domain Services for Windows Domain* option. This indicates that you are installing a new DSfW forest.

7b Select *Configure this machine to be a primary DNS server* if you want the machine being configured to function as a DNS server.

> **IMPORTANT:** If you want to configure DNS on an additional domain controller in a domain that already has a parent or a child domain, you must ensure that the additional domain controller's DNS server and the parent or child domain's DNS server act as passive primary DNS server for each other's zones. This ensures that the additional domain controller is resolved from a parent or child domain's DNS server and the parent or child domain is resolved from the additional domain controller.
>
> Also, make sure you configure the forward lookup zone and the reverse lookup zone for this DNS server. For more information, see "Zone Management" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

7c The configuration partition is forest-specific and by default the first domain controller of every domain gets a replica. The subsequent domain gets the replica of this partition if you select the *Replicate schema and configuration Partitions* option.

> **NOTE:** We recommend that you select this option to replicate the schema and configuration partition to the subsequent domain controller

8 Specify administrator name and forest root domain details.

When 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.

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.

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 the Administrator account shown in the previous field.

eDirectory Configuration - Domain Services for Windows

Forest Root Domain

dsfw.com

Existing domain administrator name

cn=Administrator,cn=Users,dc=dsfw,dc=com

Specify Administrator Password

•••

Back   Abort   Next

8a Specify the name of the forest root domain in which you want to create the domain controller.

8b Specify the password for the domain administrator.

8c Click *Next*.

9 Specify common proxy details.

9a To use common proxy for DSfW, select the *Use Common Proxy User as default for OES Products* check box. When this check box is selected, the OES Common Proxy User Name and Password fields get enabled. These fields are populated with system generated user name and password. However, you can change these values. To change these values see Step 9b.

or

If you do not want to use common proxy, clear the check box and click *Next*. Then continue with Step 11.

9b Specify the following information:

- ◆ Common proxy user name in *OES Common Proxy User Name* field. You must specify a fully distinguished name.

- ◆ Proxy user password in *OES Common Proxy User Password* field.

- ◆ Retype the password in the *Verify OES Common Proxy User Password* field.

9c To assign common proxy password policy to proxy user, select the *Assign Common Proxy Password Policy to Proxy User* check box.

9d Click *Next* to continue.

10 This screen is displayed if you have not selected the *Configure this machine to be a primary DNS server* check box in Step 7b. If you have selected this check box, continue with step Step 11.

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: ou=dns,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: ou=dns,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

[X] Get context information from existing DNS server

Existing Novell DNS server address:

192.168.108.7

Retrieve

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

ou=OESSystemObjects,ou=india,o=asia

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

ou=OESSystemObjects,ou=india,o=asia

Back   Abort   Next

10a If you already have an DNS server configured in your tree, select the *Get context information from existing DNS Server* option and provide the IP address of an existing DNS server and select *Retrieve*.

This will fetch the contexts of the existing Locator and Group objects. If you do not wish to use the existing contexts, you can manually enter the details.

10b Specify the context of the DNS Locator object.

10c Specify the context of the DNS Group object.

Click *Next* and proceed with Step 12.

11 Specify details to configure the DNS server.

11a If you are configuring DNS in an existing tree where DNS is already configured, select the *Get context and proxy user information from existing DNS server* check box. Specify the IP address 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. However, the proxy user password is not retrieved. Therefore, you must first retrieve the proxy user password and then specify the password manually in the proxy user password field. To retrieve the proxy user password, run the following command from the existing novell DNS server:

```
/opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred password
```

11b Specify the following information:

- ◆ Specify the context of the DNS service locator object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

- ◆ Specify the context of the DNS Root ServerInfo object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

- ◆ Specify the context of the DNS Services Group object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

11c Specify the fully distinguished, typeful name of the proxy user that will be used for DNS Management. For example: `cn=dns-admin,dc=dsfw,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.

11d Specify the password of the proxy user that you specified for accessing DNS.

NOTE: If you have selected the *Use Common Proxy User as default for OES Products* check box in , then the proxy user and password fields are populated with common proxy user name and password.

11e *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.

11f Specify the *Credential Storage Location* as CASA.

11g Click *Next* to continue.

12 After the installation is completed, the OES Configuration Summary page is displayed. Review the settings made earlier. Click *Next*.

13 This starts the DSfW installation.When the installation is complete, click *Finish*.

This completes the process of DSfW installation. But the server is not ready for use till you complete configure DSfW and the supporting services through the process of provisioning.

14 To start provisioning, do one of the following:

- From the terminal, run the `/opt/novell/xad/sbin/provision_dsfw.sh` script.
- Launch YaST. The DSfW Provisioning Wizard is listed as an option.

To authenticate, enter the password of the current domain.

For more details on Provisioning, see "Provisioning Domain Services for Windows" on page 123

15 The DSfW server is now ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by executing the instructions in Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145.

6.2.2 Installing DSfW in a Name-Mapped Setup

- "Installing a Forest Root Domain" on page 86
- "Installing a Child Domain" on page 97
- "Installing DSfW as a Subsequent Domain Controller in a Domain" on page 109

Installing a Forest Root Domain

Prerequisites: Before proceeding with this name-mapped installation, review Installation Prerequisites for a Name-Mapped Setup

1 In the YaST install for OES from *Software Selections* page, select Novell Domain Services for Windows pattern. Click *Accept*.

Ensure that *Novell DNS* is selected along with *Novell Domain Services for Windows*.

Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

For information about the entire OES 2 Linux installation process, see the *OES 2 SP3: Installation Guide*.

2 On the eDirectory configuration page in YaST, select the *Existing Tree* option. This indicates that you are installing the server into an existing eDirectory tree:

2a Select *Existing Tree* and specify the name of the tree. For example, DSFW-TREE.

2b 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.

2c Select the *Require TLS for Simple Binds with Password* option if you want to disallow clear passwords and other data.

2d Select *Install SecretStore* if you want to eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications.

2e Click *Next* to continue.

3 Specify information to access the existing eDirectory Tree.

3a Specify the IP address of the existing eDirectory server.

3b Do not change the NCP Port, LDAP Port and Secure LDAP Port information. However, if the administrator has configured existing eDirectory server with non-default ports then the installation will fail.

3c Specify the tree admin credentials for the administrator to log into the eDirectory tree.

3d Click *Next*.

4 Select the settings for the local server configuration:

4a Leave the location of the Directory Information Base (DIB) at the default setting.

4b Leave the iMonitor port settings at the defaults unless you need to change them to avoid port conflicts with other services.

4c Leave the Secure iMonitor Port settings at the defaults unless you need to change them to avoid port conflicts with other services.

4d Click *Next* to continue.

5 Specify details for NTP and SLP.

5a 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.

5b Specify details to configure SLP:

5b1 If you do not want to configure the Service Location Protocol, select the *Do not configure SLP* option.

5b2 Select the *Use multicast to access SLP* option to request SLP information using multicast packet.

5b3 If you have more than three servers in your eDirectory tree, and you already have a Directory Agent running, select the *Configure SLP to use an existing Directory Agent* option.

5b4 Select the *Configure as Directory Agent* option if you want the local server to act as a directory agent.

  ◆ Select the *DASyncReg* check box to enable SLP to query statically configured directory agents for registrations.

  ◆ Select the Backup SLP Registrations check box to enable periodical backup of all registrations. In the *Backup Interval in Seconds* field, specify the time interval (seconds) to perform the backup.

5c Click *Next*.

6 Select the authentication service you want to install.

6a Click *Next*.

7 Specify details to configure DSfW on eDirectory.

7a Select the *New Domain Services for Windows Forest* option. This indicates that you are installing a DSfW server in an existing forest.

7b The *DNS Name for the New Domain* is by default taken from the entry in the `/etc/hosts` file. In case you need to change the domain name, make sure you follow the instructions in "Domain Name and Name Server Configuration is Correct" on page 38.

7c We recommend you to leave the NetBIOS name setting at the default, then click *Next* to continue.

For more information, see Section 5.11, "Limitations," on page 46

7d Click *Next* to continue.

8 Specify the password for the domain administrator in both fields, then click *Next*.

NOTE: The administrator name is hard-coded. However, after completing DSfW installation and configuration (post provisioning), you can modify administrator details such as the administrator name. For more information, see Section 8.2, "Renaming Administrator Details Using MMC," on page 146.

---

9 Specify details to map the existing eDirectory container to the new domain.

> **IMPORTANT:** 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.
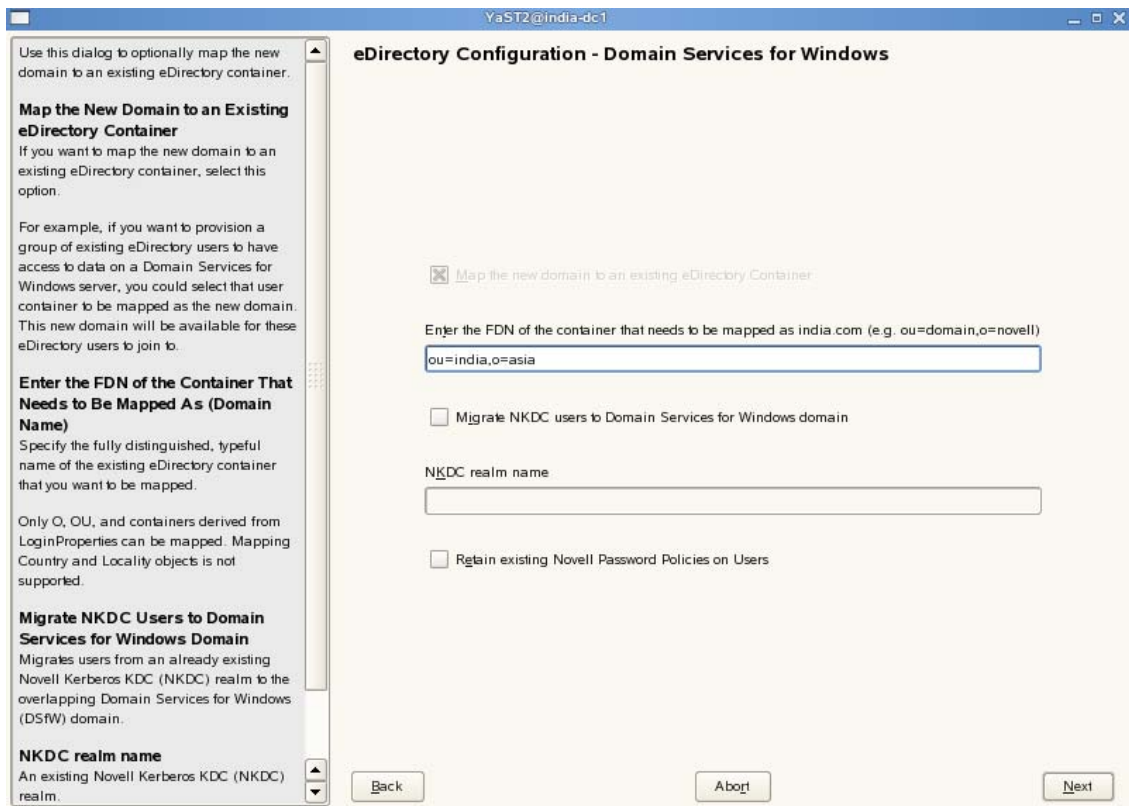
9a Enter the Fully Qualified Domain Name of the existing eDirectory container that you want to be mapped to the new domain.

NOTE: The container that is being mapped should be partitioned.

9b Select th*e Migrate NKDC users to Domain Services for Windows domain* option if you want to migrate the users from existing Novell KDC realm to DSfW domain. This facilitates the migration of existing eDirectory users who are using Novell KDC to the DSfW domain users keeping Novell KDC security identities (security principals and policies) intact. After the migration, the existing eDirectory users continue to use their own security settings in DSfW kerberos environment.

9c Specify the name of the *NKDC realm* from where you want to migrate the users to DSfW domain.

9d If you select the *Retain existing Novell Password Policies on Users* option the password policies assigned to the users within the container that is mapped to the new domain does not change. However the password policies outside the partition boundary is not carried forward. You need to create a fresh password policy assigned to the partition root. For details on creating a fresh password policy, see Creating Password Policies (http://www.novell.com/documentation/password_management/pwm_administration/data/an4bun5.html)

10 Specify common proxy details.
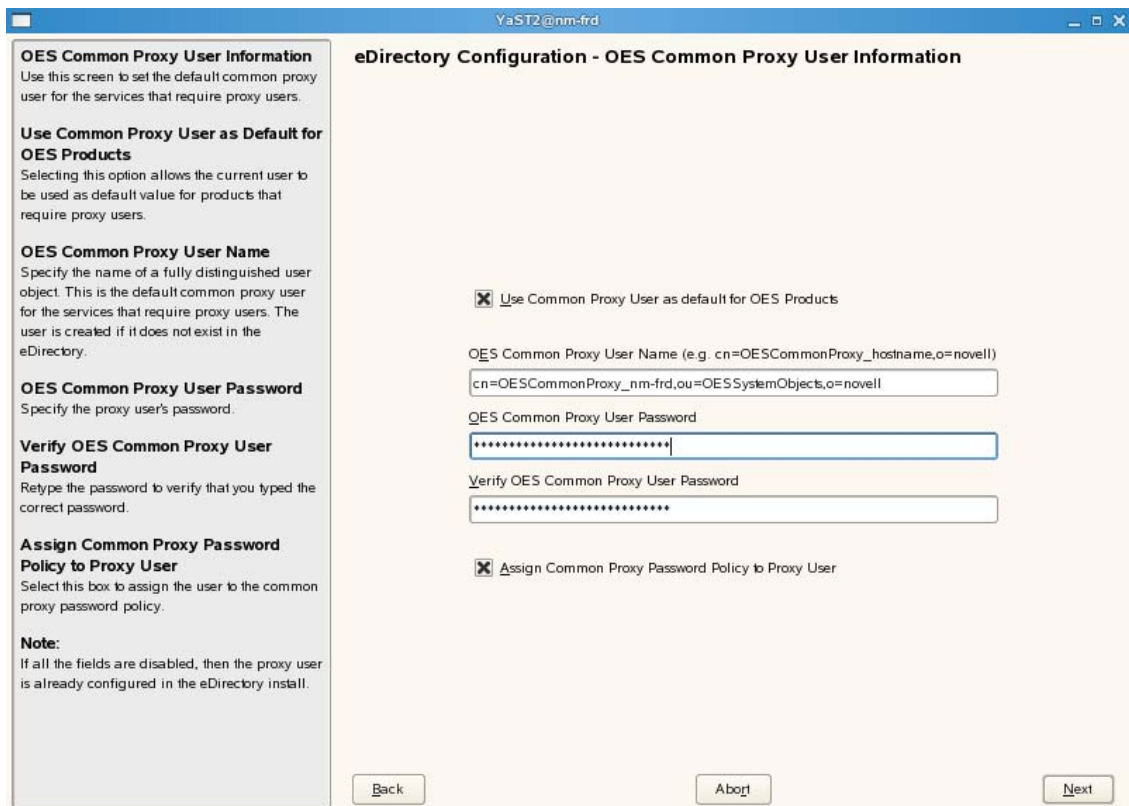
10a To use common proxy for DSfW, select the *Use Common Proxy User as default for OES Products* check box. When this check box is selected, the OES Common Proxy User Name and Password fields get enabled. These fields are populated with system generated user name and password. However, you can change these values. To change these values see Step 10b.

or

If you do not want to use common proxy, clear the check box and click *Next*. Then continue with Step 11.

10b Specify the following information:

- ◆ Common proxy user name in *OES Common Proxy User Name* field. You must specify a fully distinguished name.
- ◆ Proxy user password in *OES Common Proxy User Password* field.
- ◆ Retype the password in the *Verify OES Common Proxy User Password* field.

10c To assign common proxy password policy to proxy user, select the *Assign Common Proxy Password Policy to Proxy User* check box.

10d Click *Next* to continue.

11 Specify details to configure the DNS server.
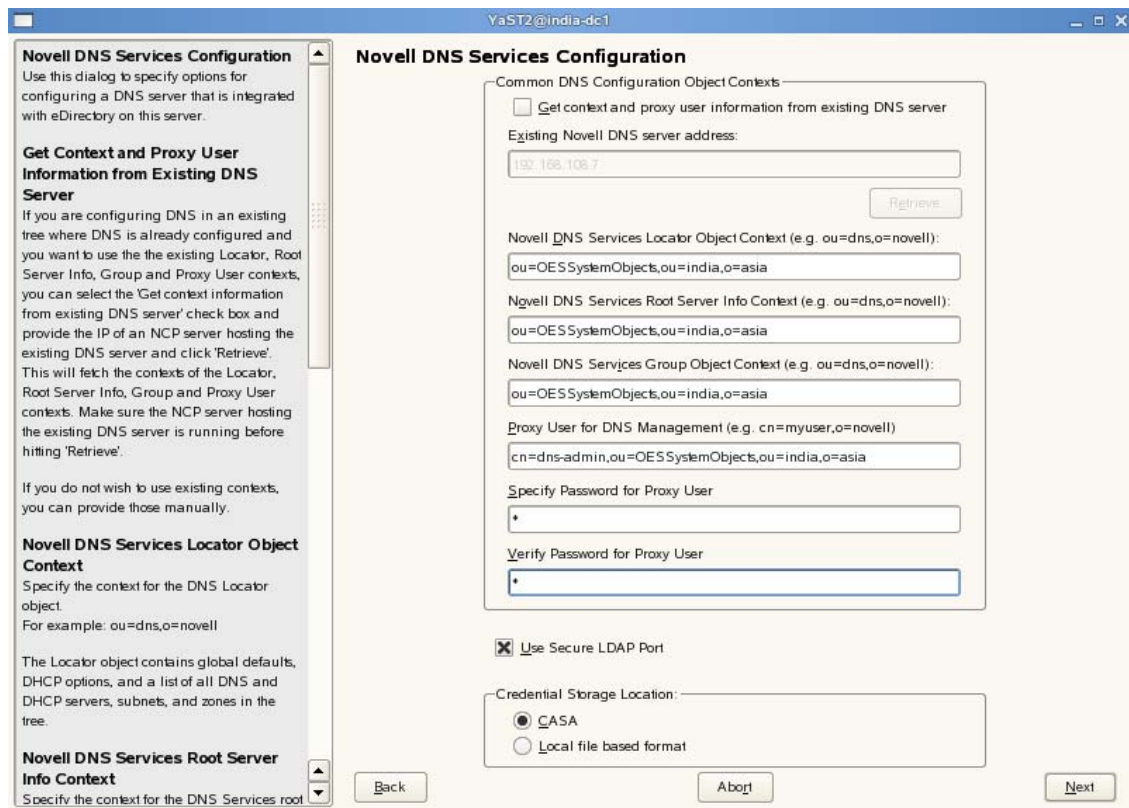
11a Specify the following information:

- Specify the context of the DNS service locator object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).
- Specify the context of the DNS Root ServerInfo object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).
- Specify the context of the DNS group object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

11b Specify the fully distinguished, typeful name of the proxy user that will be used for DNS Management. For example: `cn=dns-admin,dc=dsfw,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.

11c Specify the password of the eDirectory user that you specified for accessing DNS.

NOTE: If you have selected the *Use Common Proxy User as default for OES Products* check box in Step 10a, then the proxy user and password fields are populated with common proxy user name and password.

11d *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.

11e Specify the *Credential Storage Location* as CASA.

11f Click *Next* to continue.

12 After the installation is completed, the OES Configuration Summary page is displayed. Review the settings made earlier. Click *Next*.

13 This starts the DSfW installation.When the installation is complete, click *Finish*.

This completes the process of DSfW installation. But the server is not ready for use till you complete configure DSfW and the supporting services through the process of provisioning.

14 To start provisioning, do one of the following:

 ◆ From the terminal, run the `/opt/novell/xad/sbin/provision_dsfw.sh` script.

 ◆ Launch YaST. The DSfW Provisioning Wizard is listed as an option.

To authenticate, enter the password of the current domain and the tree admin.

For more details on Provisioning, see

15 The DSfW server is now ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by executing the instructions in .

Installing a Child Domain

Prerequisites: Before proceeding with this name-mapped installation, review Installation Prerequisites for a Name-Mapped Setup

1 In the YaST install for OES from *Software Selections* page, select *Novell Domain Services for Windows* pattern. Click *Accept*.

Ensure that *Novell DNS* is selected along with *Novell Domain Services for Windows*.

Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

For information about the entire OES 2 Linux installation process, see the *OES 2 SP3: Installation Guide*.

2 On the first eDirectory configuration page in YaST, select the *Existing Tree* option. This indicates that you are installing the server into an existing eDirectory tree:

2a Select Existing Tree and specify the name of the tree. For example, DSfW-TREE.

2b 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.

2c Select the *Require TLS for Simple Binds with Password* option if you want to disallow clear passwords and other data.

2d Select *Install SecretStore* if you want to eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications.

2e Click *Next* to continue.

3 Specify the existing eDirectory configuration details.

3a Specify the IP address of the Forest Root domain.

3b Do not change the NCP Port, LDAP Port and Secure LDAP Port information.

3c Specify the existing tree admin credentials.

3d Click *Next*.

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

4a Leave the location of the Directory Information Base (DIB) at the default setting.

4b Leave the *iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4c Leave the *Secure iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4d Click *Next* to continue.

5 Specify details for NTP and SLP.

5a 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.

5b Specify details to configure SLP:

5b1 If you do not want to configure the Service Location Protocol, select the *Do not configure SLP* option.

5b2 Select the *Use multicast to access SLP* option to request SLP information using multicast packet.

5b3 If you have more than three servers in your eDirectory tree, and you already have a Directory Agent running, select the *Configure SLP to use an existing Directory Agent* option.
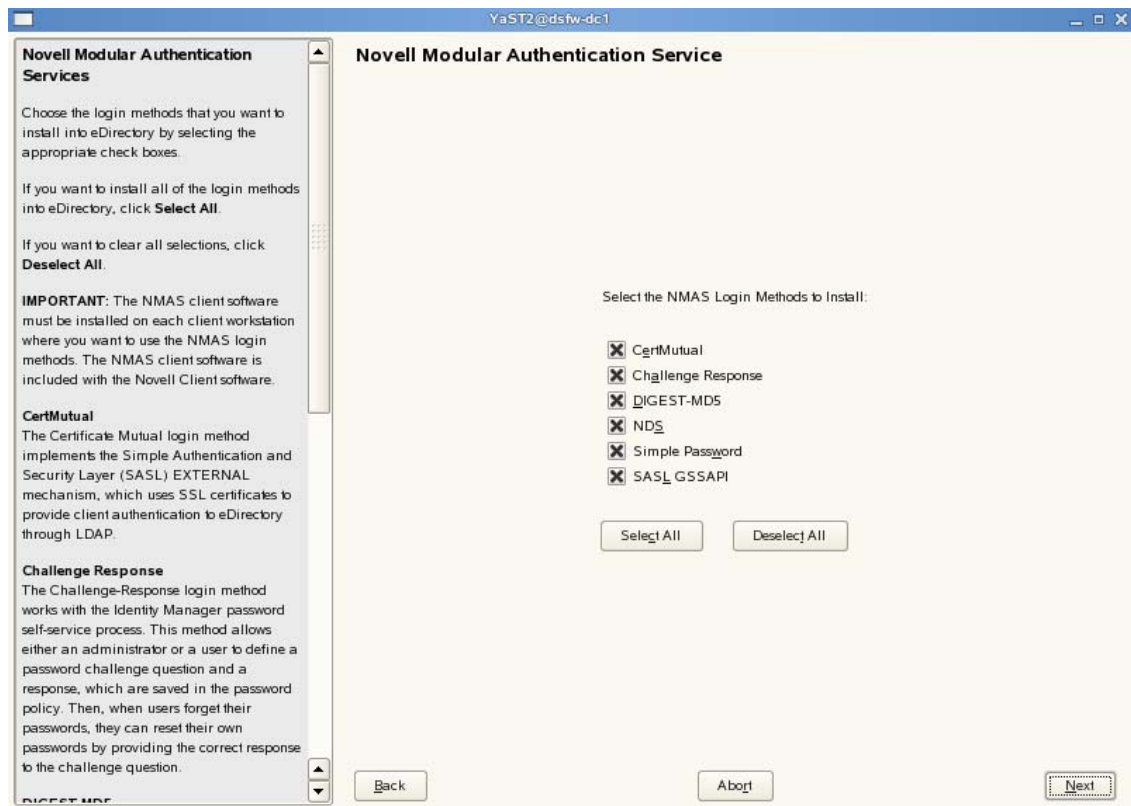
5b4 Select the *Configure as Directory Agent* option if you want the local server to act as a directory agent.

◆ Select the *DASyncReg* check box to enable SLP to query statically configured directory agents for registrations.

◆ Select the Backup SLP Registrations check box to enable periodical backup of all registrations. In the *Backup Interval in Seconds* field, specify the time interval (seconds) to perform the backup.
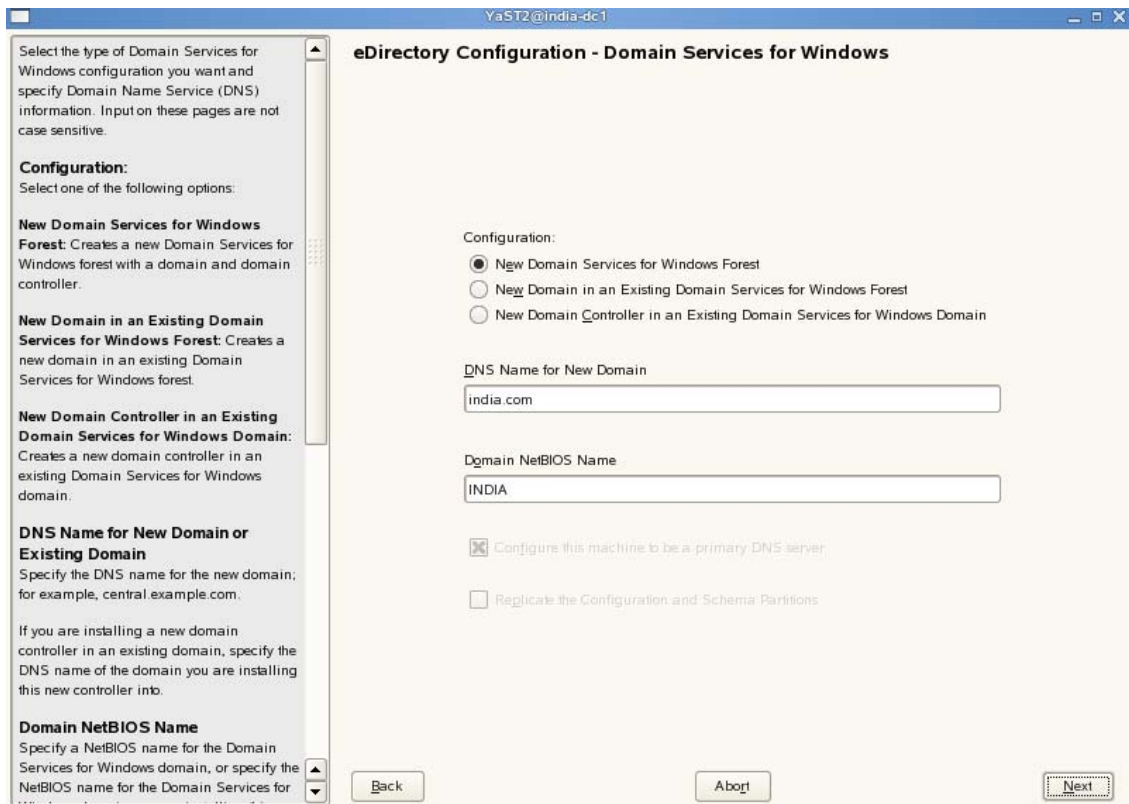
5c Click *Next.*

6 Select the authentication service you want to install.

6a Click *Next*.

7 Specify details to configure DSfW on eDirectory.

7a Select the *New Domain in an Existing Domain Services for Windows forest* option. This indicates that you setting up a new domain in an existing DSfW forest.

7b The *DNS Name for the New Domain* is by default taken from the entry in the `/etc/hosts` file. In case you need to change the domain name, make sure you follow the instructions in "Domain Name and Name Server Configuration is Correct" on page 38.

7c We recommend you to leave the NetBIOS name setting at the default, then click *Next* to continue.

For more information, see Section 5.11, "Limitations," on page 46

7d Select *Configure this machine to be a primary DNS server* if you want the machine being configured to function as a DNS server.

> **IMPORTANT:** If you want to configure the child domain controller to act as a primary DNS server, ensure the DNS servers of the forest root domain and the child domain controller act as passive primary DNS servers of each other's zones, else the installation of an subsequent domain controller to the child domain controller fails.
>
> Also make sure you configure the forward lookup zone and the reverse lookup zone for this DNS server. For more information, see "Zone Management" in the *OES 2 SP3: Novell DNS/ DHCP Administration Guide*.

7e Click *Next* to continue.

8 Specify details to configure the DSfW server.
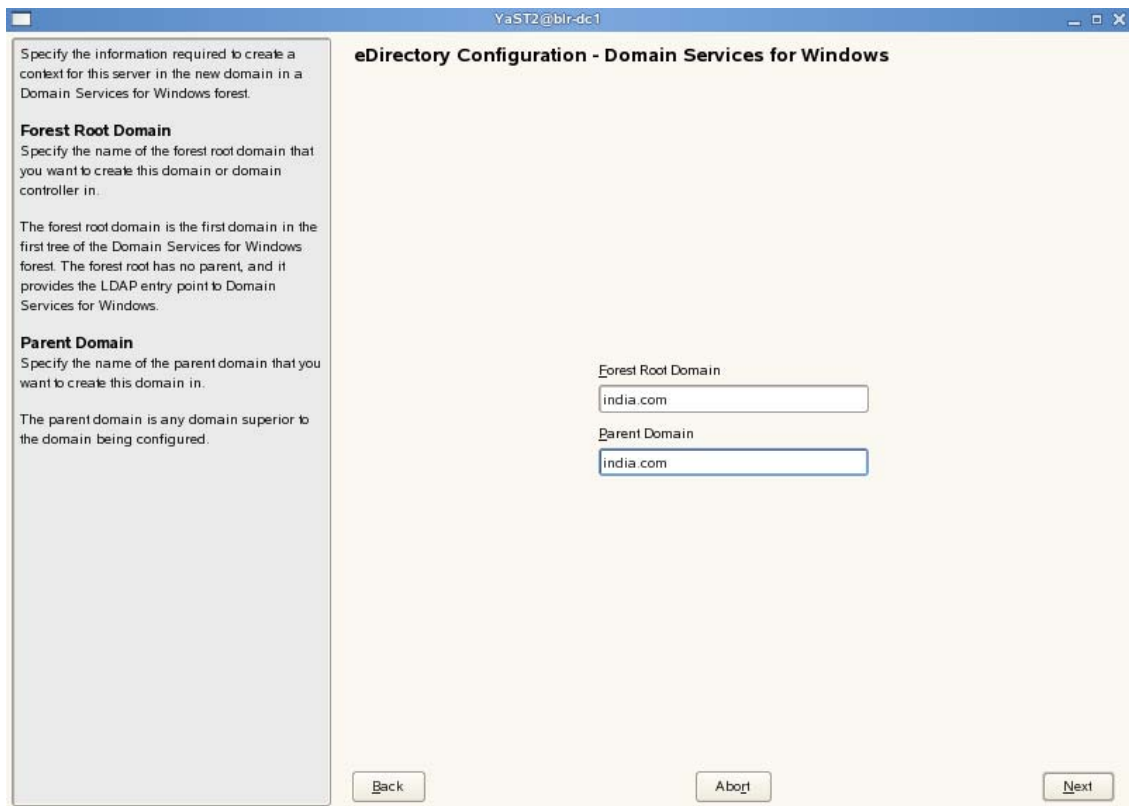
8a Specify the name of the Forest Root Domain in which you want to create the child domain.

8b Specify the parent domain in which you want to create the child domain.

8c Click *Next*.

9 Specify the information needed to identify the child domain you are creating.

NOTE: The *New Domain Administrator Name* is hard-coded. However, after completing DSfW installation and configuration (post provisioning), you can modify administrator details such as the administrator name. For more information, see Section 8.2, "Renaming Administrator Details Using MMC," on page 146.

9a Specify the IP Address, name and context for the administrator of the parent domain.

9b Specify the password for the administrator of the new child domain. Retype the password to verify it.

9c Click *Next*.

**10** Specify the information to map the new domain to an existing eDirectory container

---

IMPORTANT: 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.
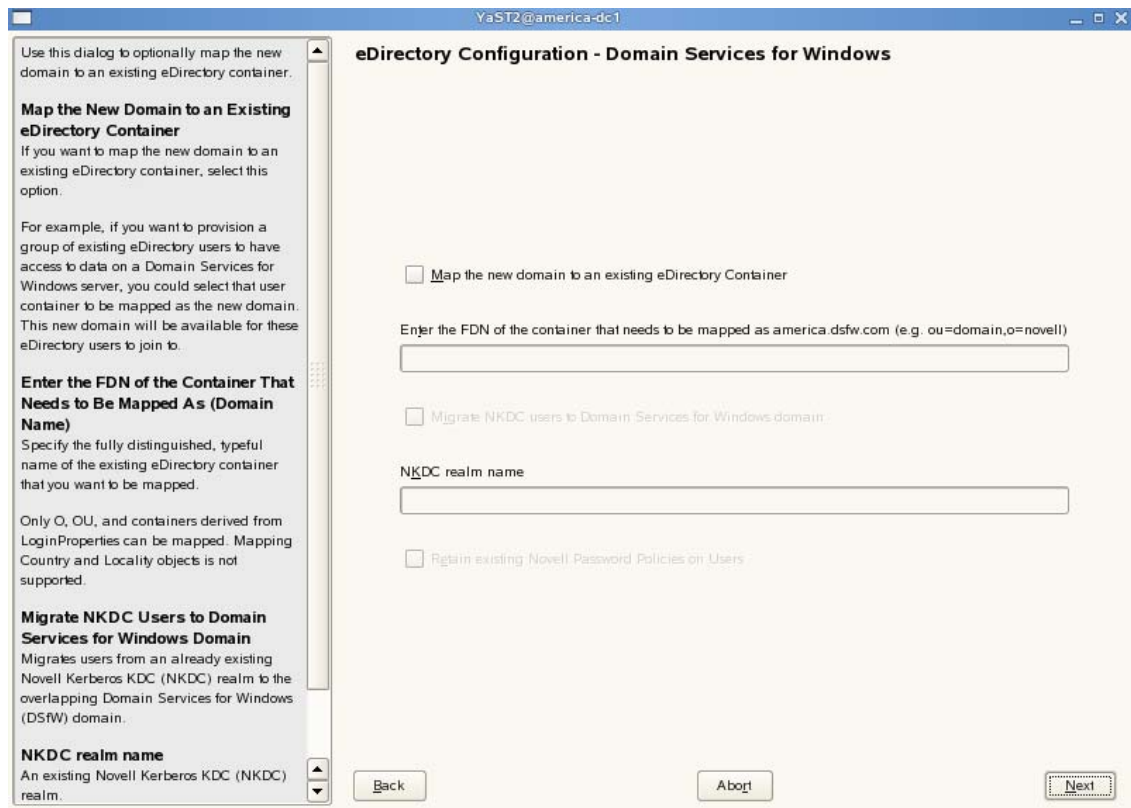
10a Select *Map the New Domain to an Existing eDirectory Container* option.

10b Specify the fully distinguished typeful name of the existing eDirectory container

10c Specify the name of the realm where you have existing Kerberos users.

10d If you select the *Retain existing Novell Password Policies on Users* option the password policies assigned to the users within the container that is mapped to the new domain does not change. However the password policies outside the partition boundary is not carried forward. You need to create a fresh password policy assigned to the partition root. For details, see Creating Password Policies (http://www.novell.com/documentation/ password_management/pwm_administration/data/an4bun5.html)

10e Click *Next*.

11 Specify common proxy details.

11a To use common proxy for DSfW, select the *Use Common Proxy User as default for OES Products* check box. When this check box is selected, the OES Common Proxy User Name and Password fields get enabled. These fields are populated with system generated user name and password. However, you can change these values. To change these values see Step 11b.

or

If you do not want to use common proxy, clear the check box and click *Next*. Then continue with Step 13.

11b Specify the following information:

- Common proxy user name in *OES Common Proxy User Name* field. You must specify a fully distinguished name.
- Proxy user password in *OES Common Proxy User Password* field.
- Retype the password in the *Verify OES Common Proxy User Password* field.

11c To assign common proxy password policy to proxy user, select the *Assign Common Proxy Password Policy to Proxy User* check box.

11d Click *Next* to continue.

12 This screen is displayed if you have not selected the *Configure this machine to be a primary DNS server* check box in Step 7d. If you have selected this check box, continue with step Step 13.

12a If you already have an DNS server configured in your tree, select the *Get context information from existing DNS Server* option and provide the IP address of an existing DNS server and select *Retrieve*.

This will fetch the contexts of the existing Locator and Group objects. If you do not wish to use the existing contexts, you can manually enter the details.

12b Specify the context of the DNS Locator object.

12c Specify the context of the DNS Group object.

Click *Next* and proceed with .

13 Specify details to configure the DNS server.

13a If you are configuring DNS in an existing tree where DNS is already configured, select the *Get context and proxy user information from existing DNS server* check box. Specify the IP address 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. However, the proxy user password is not retrieved. Therefore, you must first retrieve the proxy user password and then specify the password manually in the proxy user password field. To retrieve the proxy user password, run the following command from the existing novell DNS server:

`/opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred password`

13b Specify the following information:

 ◆ Specify the context of the DNS service locator object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

 ◆ Specify the context of the DNS Root ServerInfo object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

 ◆ Specify the context of the DNS Services Group object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

13c Specify the fully distinguished, typeful name of the proxy user that will be used for DNS Management. For example: `cn=dns-admin,dc=dsfw,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.

13d Specify the password of the proxy user that you specified for accessing DNS.

NOTE: If you have selected the *Use Common Proxy User as default for OES Products* check box in Step 11a, then the proxy user and password fields are populated with common proxy user name and password.

13e *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.
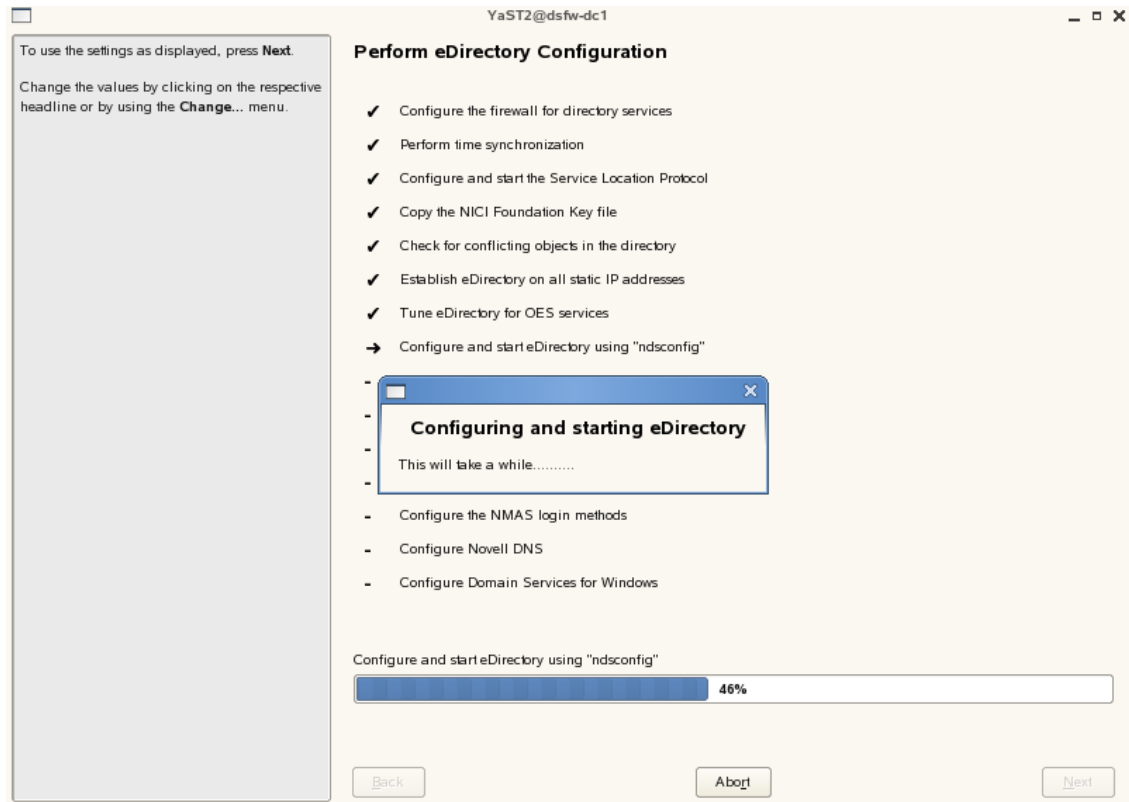
13f Specify the *Credential Storage Location* as CASA.
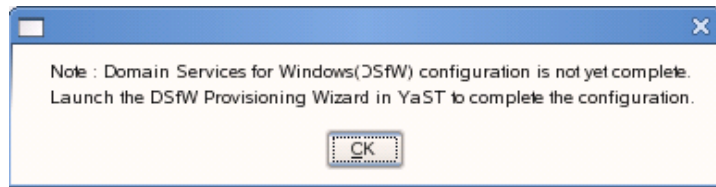
13g Click *Next* to continue.

14 After the installation is completed, the OES Configuration Summary page is displayed. Review the settings made earlier. Click *Next*.

15 This starts the DSfW installation.When the installation is complete, click *Finish*.

This completes the process of DSfW installation. But the server is not ready for use till you complete configure DSfW and the supporting services through the process of provisioning.

16 To start provisioning, do one of the following:

- From the terminal, run the `/opt/novell/xad/sbin/provision_dsfw.sh` script.
- Launch YaST. The DSfW Provisioning Wizard is listed as an option.

To authenticate, enter the password of the current domain, the parent domain, and the tree/container admin.

For more details on Provisioning, see "Provisioning Domain Services for Windows" on page 123

17 The DSfW server is now ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by executing the instructions in Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145.

Installing DSfW as a Subsequent Domain Controller in a Domain

Prerequisites: Before proceeding with this name-mapped installation, review Section 5.5.2, "Installation Prerequisites for a Name-Mapped Setup," on page 40.

1 In the YaST install for OES from *Software Selections* page, select *Novell Domain Services for Windows* pattern. Click *Accept*.

Ensure that *Novell DNS* is selected along with *Novell Domain Services for Windows*.

Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

For information about the entire OES 2 Linux installation process, see the *OES 2 SP3: Installation Guide*.

2 On the first eDirectory configuration page in YaST, select the *Existing Tree* option. This indicates that you are installing the server into an existing eDirectory tree:

2a Select *Existing Tree* and specify the name of the tree. For example, DSfW-TREE.

2b 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.

2c Select the *Require TLS for Simple Binds with Password* option if you want to disallow clear passwords and other data.

2d Select *Install SecretStore* if you want to eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications.

2e Click *Next* to continue.

3 Specify information to access the existing eDirectory Tree.

3a Specify the IP Address of the Forest Root domain.

3b Do not change the NCP Port, LDAP Port and Secure LDAP Port information.

3c Specify the tree admin credentials for the administrator to log into the eDirectory tree.

3d Click *Next*.

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

4a Leave the location of the *Directory Information Base (DIB)* at the default setting.

4b Leave the *iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4c Leave the *Secure iMonitor Port* settings at the defaults unless you need to change them to avoid port conflicts with other services.

4d Click *Next* to continue.

5 Specify details for NTP and SLP.

5a 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.

5b Specify details to configure SLP:

5b1 If you do not want to configure the Service Location Protocol, select the *Do not configure SLP* option.

5b2 Select the *Use multicast to access SLP* option to request SLP information using multicast packet.

5b3 If you have more than three servers in your eDirectory tree, and you already have a Directory Agent running, select the *Configure SLP to use an existing Directory Agent* option.

5b4 Select the *Configure as Directory Agent* option if you want the local server to act as a directory agent.

◆ Select the *DASyncReg* check box to enable SLP to query statically configured directory agents for registrations.

◆ Select the Backup SLP Registrations check box to enable periodical backup of all registrations. In the *Backup Interval in Seconds* field, specify the time interval (seconds) to perform the backup.

5c Click *Next.*

6 Select the authentication service you want to install.

6a Click *Next*.

7 Specify details to configure DSfW on eDirectory

    7a Select the *New Domain Controller in an Existing Domain Services for Windows Domain* option. This indicates that you are installing DSfW in an existing eDirectory tree.

7b Select *Configure this machine to be a primary DNS server* if you want the machine being configured to function as a DNS server.

IMPORTANT: If you want to configure DNS on an additional domain controller in a domain that already has a parent or a child domain, you must ensure that the additional domain controller's DNS server and the parent or child domain's DNS server act as passive primary DNS server for each other's zones. This ensures that the additional domain controller is resolved from a parent or child domain's DNS server and the parent or child domain is resolved from the additional domain controller.

Also, make sure you configure the forward lookup zone and the reverse lookup zone for this DNS server. For more information, see "Zone Management" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

7c The configuration partition is forest-specific and by default the first domain controller of every domain gets a replica. The subsequent domain gets the replica of this partition if you select the *Replicate schema and configuration Partitions* option.

NOTE: We recommend that you select this option to replicate the schema and configuration partition to the subsequent domain controller

8 Specify administrator name and forest root domain details

When 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.

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.

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 the Administrator account shown in the previous field.

eDirectory Configuration - Domain Services for Windows

Forest Root Domain

dsfw.com

Existing domain administrator name

cn=Administrator,cn=Users,dc=dsfw,dc=com

Specify Administrator Password

•••

Back   Abort   Next

    8a Specify the name of the domain in which you want to create the domain controller.

    8b Specify the password for the domain administrator.

    8c Click *Next*.

9 Specify common proxy details.

9a To use common proxy for DSfW, select the *Use Common Proxy User as default for OES Products* check box. When this check box is selected, the OES Common Proxy User Name and Password fields get enabled. These fields are populated with system generated user name and password. However, you can change these values. To change these values see Step 9b.

or

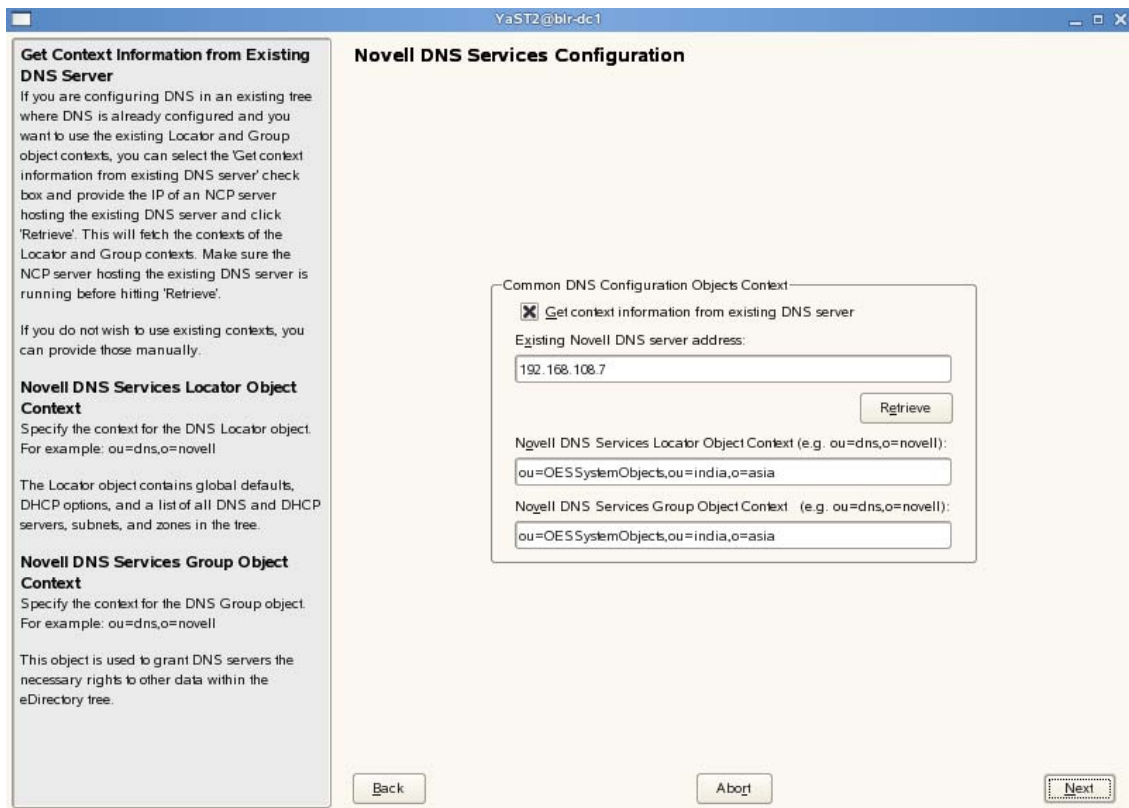If you do not want to use common proxy, clear the check box and click *Next*. Then continue with Step 11.

9b Specify the following information:

- Common proxy user name in *OES Common Proxy User Name* field. You must specify a fully distinguished name.

- Proxy user password in *OES Common Proxy User Password* field.

- Retype the password in the *Verify OES Common Proxy User Password* field.

9c To assign common proxy password policy to proxy user, select the *Assign Common Proxy Password Policy to Proxy User* check box.

9d Click *Next* to continue.

10 This screen is displayed if you have not selected the *Configure this machine to be a primary DNS server* check box in Step 7b. If you have selected this check box, continue with step Step 11.
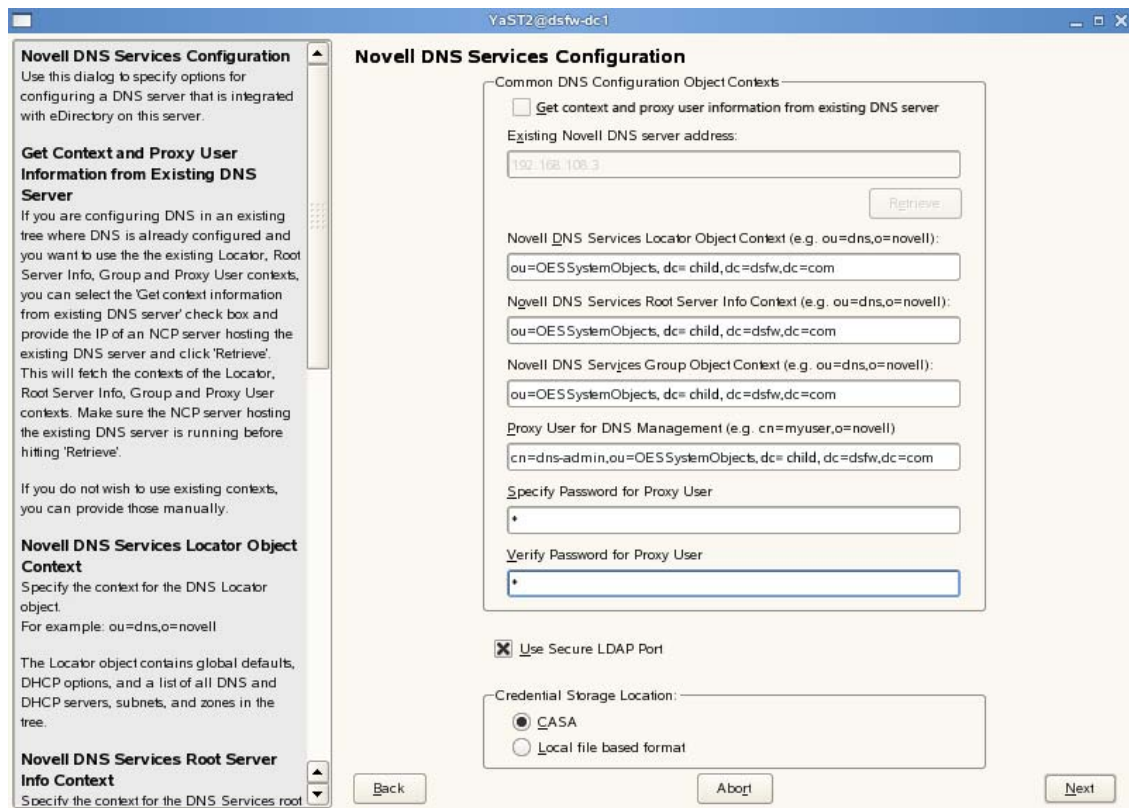
10a If you already have an DNS server configured in your tree, select the *Get context information from existing DNS Server* option and provide the IP address of an existing DNS server and select *Retrieve*.

This will fetch the contexts of the existing Locator and Group objects. If you do not wish to use the existing contexts, you can manually enter the details.

10b Specify the context of the DNS Locator object.

10c Specify the context of the DNS Group object.

Click *Next* and proceed with Step 12.

11 Specify details to configure the DNS server.

11a If you are configuring DNS in an existing tree where DNS is already configured, select the *Get context and proxy user information from existing DNS server* check box. Specify the IP address 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. However, the proxy user password is not retrieved. Therefore, you must first retrieve the proxy user password and then specify the password manually in the proxy user password field. To retrieve the proxy user password, run the following command from the existing novell DNS server:

```
/opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred password
```
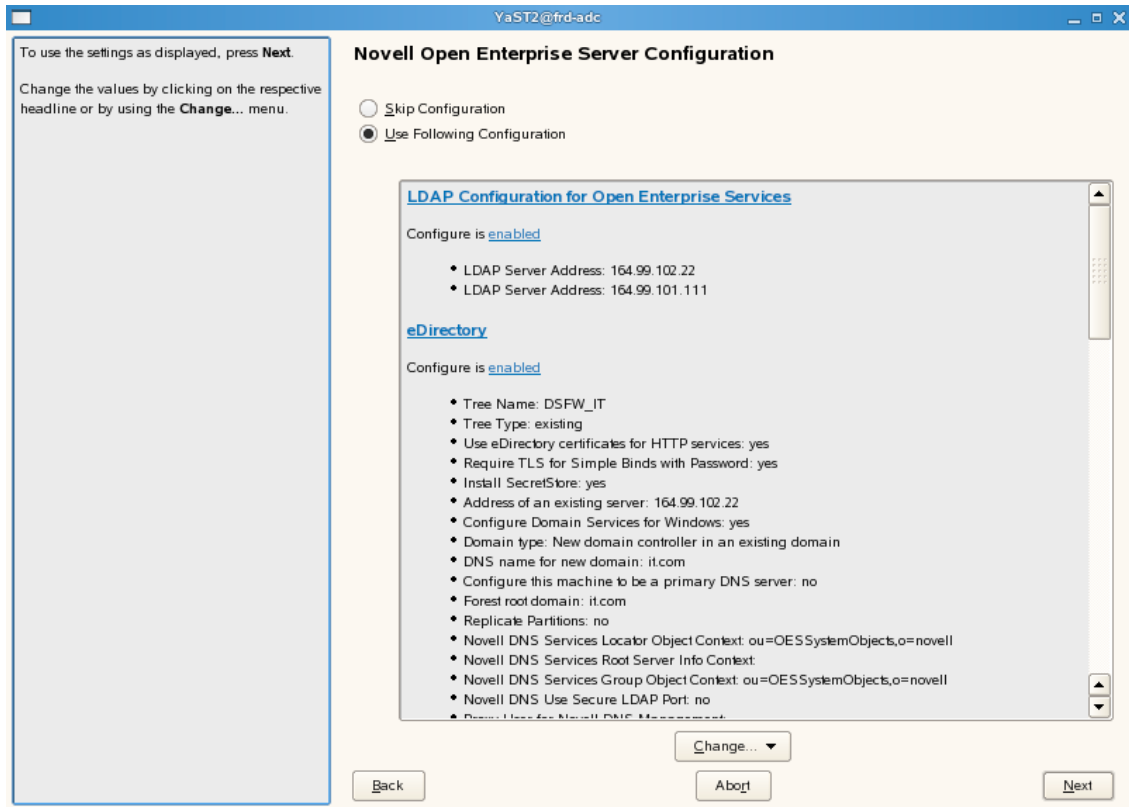
11b Specify the following information:

- Specify the context of the DNS service locator object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

- Specify the context of the DNS Root ServerInfo object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

- Specify the context of the DNS Services Group object (for example, `ou=OESSystemObjects,dc=dsfw,dc=com`).

11c Specify the fully distinguished, typeful name of the proxy user that will be used for DNS Management. For example: `cn=dns-admin,dc=dsfw,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.
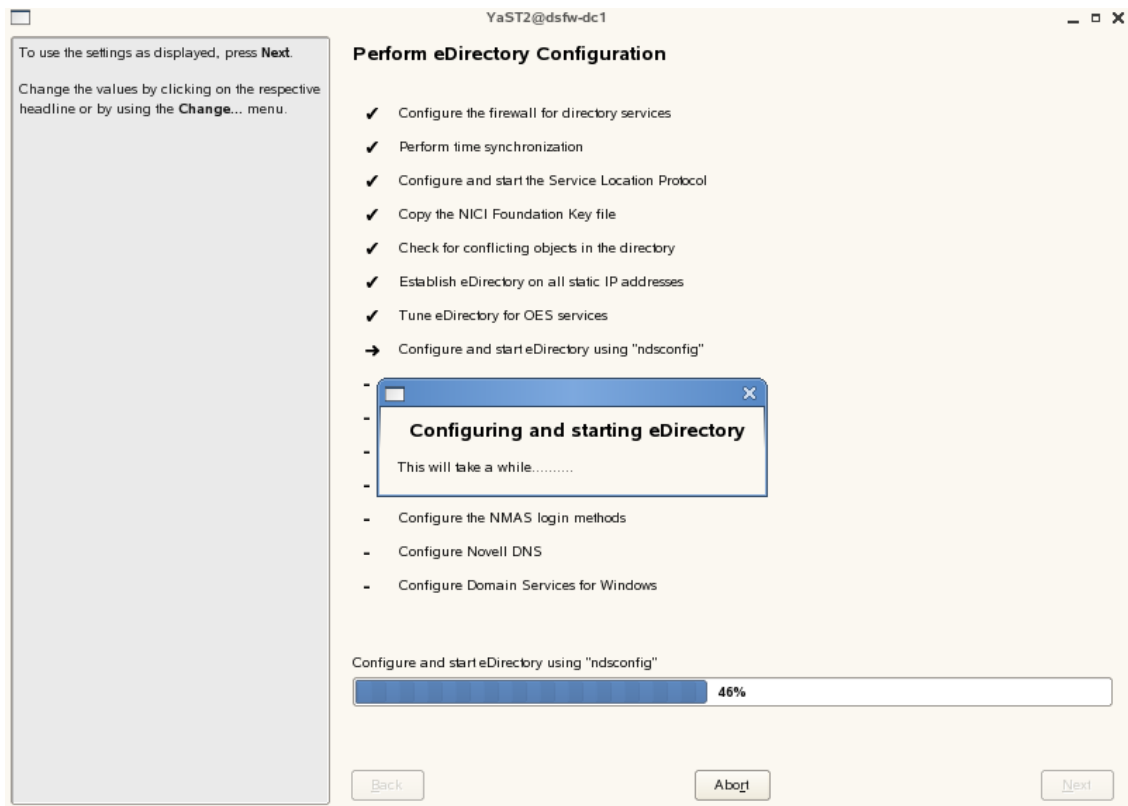
11d Specify the password of the proxy user that you specified for accessing DNS.

NOTE: If you have selected the *Use Common Proxy User as default for OES Products* check box in Step 9a, then the proxy user and password fields are populated with common proxy user name and password.
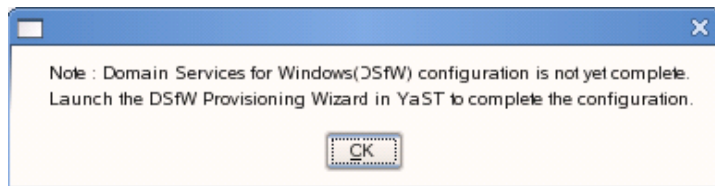
11e *Use Secure LDAP Port* option is selected by default to ensure that the data transferred by this service is secure and private. If you deselect this option, the data transferred is in clear text format.

11f Specify the *Credential Storage Location* as CASA.

11g Click *Next* to continue.

12 After the installation is completed, the OES Configuration Summary page is displayed. Review the settings made earlier. Click *Next*.

13 This starts the DSfW installation.When the installation is complete, click *Finish*.

This completes the process of DSfW installation. But the server is not ready for use till you complete configure DSfW and the supporting services through the process of provisioning.

14 To start provisioning, do one of the following:

- From the terminal, run the `/opt/novell/xad/sbin/provision_dsfw.sh` script.
- Launch YaST. The DSfW Provisioning Wizard is listed as an option.

To authenticate, enter the password of the current domain.

For more details on Provisioning, see "Provisioning Domain Services for Windows" on page 123

15 The DSfW server is now ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by executing the instructions in Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145.

6.3   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.

Prerequisite:

You must have at least one eDirectory 8.8 SP2 and above 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 during DSfW configuration.

To configure a container admin:

1 Create a container in an already existing tree.

```
eg:ou=india.o=novell
```

2 Create a user `cn=localadmin` under the container `eg:ou=india.o=novell`,and ensure the following prerequisite is met:

The container must be partitioned (before installing the server) by using the admin for the tree.

3 Assign the following rights to the container admin:

❒ Supervisor rights on this partition.

❒ Supervisor rights (inherited) for the entry rights to the security container.

❒ Read and Write permission for the DNS locator and DNS group object.

❒ Read and Write permission for the DNS server object if the DNS server is located in other domain.

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

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

❒ The container admin needs supervisor rights on the configuration partition and schema partition to create a subsequent domain or a subsequent domain controller.

For information on rights that must be assigned before doing a container admin installation, see "Rights Required for Subcontainer Administrators" in the *OES 2 SP3: Installation Guide*.

For more information on installing a secondary server into an existing tree as a non-administrator user, refer to the eDirectory 8.8 Installation Guide (http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a7ivcnh.html).

4 Use the tree admin to extend the schema for DSfW:

4a 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 SP5 server with a writable replica of the root.

4b Specify the tree admin's password and click *Next*.

4c Select *Novell Linux User Management (LUM), Novell DNS, Novell Domain Services for Windows, Novell Directory Services, Novell iPrint Services, Novell Storage Services (NSS), Novell NCP Server, Novell SMS,* 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.

5 Configure Novell DSfW using YaST with the container admin credentials.

For information on installing and configuring Novell DNS service, refer to "Installing the DNS Server" and "eDirectory Permissions " in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

NOTE: Apart from the tree administrator installation, container administrator installation is the only supported installation scenario. DSfW installation as a DSfW Domain Administrator is not supported.

---

7 Provisioning Domain Services for Windows

This section describes the process of provisioning and describes how you can use the Domain Services for Windows (DSfW) Provisioning Wizard to configure DSfW and the supporting services on top of eDirectory.

7.1 What Is Provisioning?

After you have installed DSfW, you need to configure DSfW and the supporting services to make the DSfW server ready for use. Provisioning is the process of configuring the services on a DSfW server. It is made up of a series of logical steps that execute in a predetermined order to complete the DSfW installation.

The configuration details provided during DSfW installation serve as input for the Provisioning Wizard. The tasks to be executed for provisioning vary with the scenario in which DSfW has been installed.

7.2 Features and Capabilities of the Provisioning Wizard

The Provisioning Wizard makes it easy to configure services on DSfW.

- **Dynamic Task list** : As explained in What Is Provisioning?, the tasks displayed during the provisioning process vary with the scenario in which DSfW has been installed. When you launch the Provisioning Wizard, you see only those tasks that are essential to provision the DSfW server in a specific scenario.

- **Resuming Tasks** : The Provisioning Wizard stores the status and details of the tasks being performed in the `/etc/opt/novell/xad/provisioning.xml` file. If you close the wizard window or cancel a task during provisioning, the next time you launch provisioning, the task resumes from the point it was stopped.

- **Precheck and Post check** : The Provisioning Wizard is made up of pluggable scripts that contain set of instructions to validate the state of the system after a provisioning task is completed and before the start of the next provisioning task.

  Each task has a corresponding script located in the `/opt/novell/xad/lib/perl/Install` folder. These scripts contain pre-operation and post-operation pluggable subroutines that take care of the validation process. The precheck ensures that all the prerequisites are met for execution of the task and the post-check ensures that the task is finished before moving on to the next task.

  NOTE: For 64-bit systems, the scripts are located in the `/opt/novell/xad/lib/perl/Install` folder.

- **Skipping Tasks:** If you choose not to execute a particular task from the Provisioning Wizard, you can choose to skip that task and later execute the task manually from the console. The logging feature is available only for tasks performed through the Provisioning Wizard. If you execute tasks manually by using the process in Executing Provisioning Tasks Manually, the task execution details are logged in the `/var/opt/novell/xad/log/ndsdcinit.log` file.

  IMPORTANT: When you decide to skip a task from the Provisioning Wizard, the task has to be executed from the console. As part of pre-check process, checks are done to ensure that all the prerequisites are met for execution of the next task.

- **Error Handling and Logging** : During execution of each provisioning task, any errors or warnings are logged in the `/var/opt/novell/xad/log/provisioning.log` file. The log file records details and error codes that help you when you need to debug errors. For more information about logging, see Section 7.7, "Logging," on page 134.

7.3 Provisioning Wizard Interface

The Provisioning Wizard provides a single interface to configure services on DSfW and is divided into the following panes:

- Task List
- Task Description
- Log Messages

Figure 7-1   *Snapshot of the Provisioning Wizard*
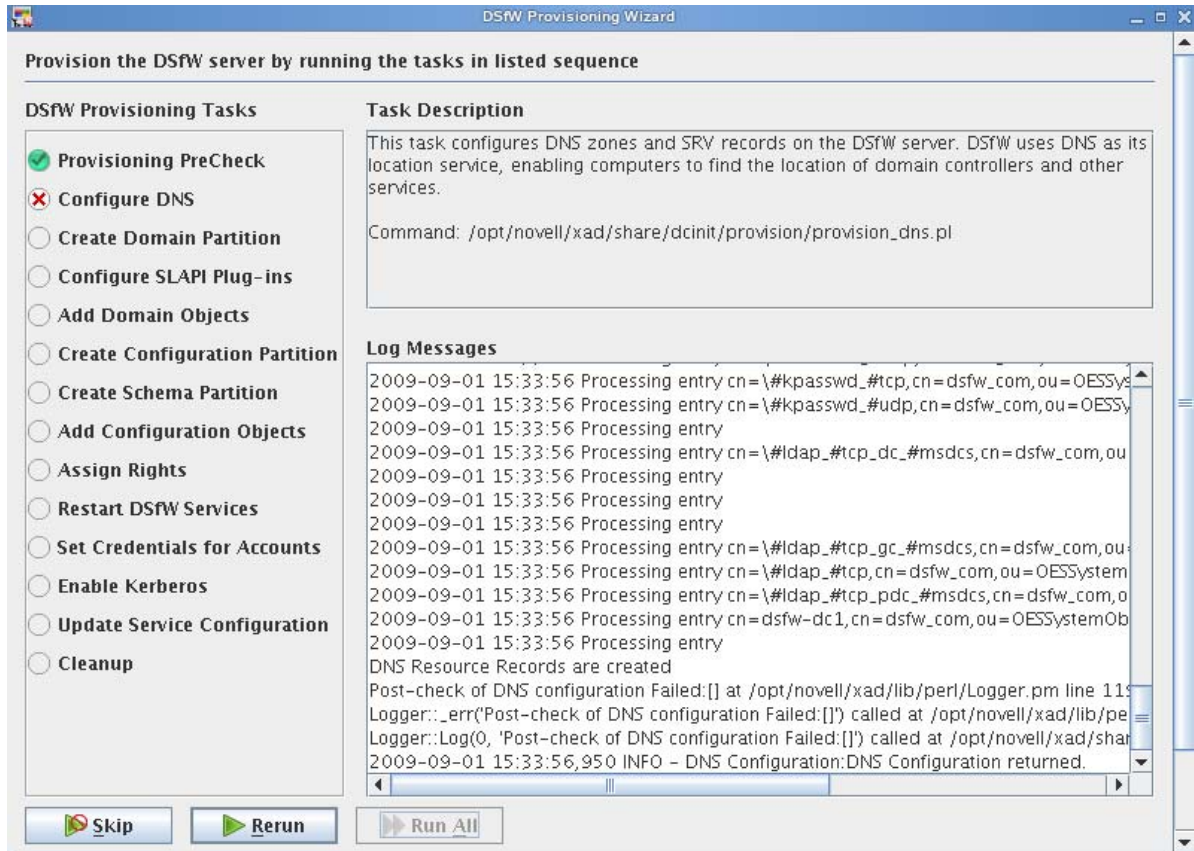
Task List : The task list displayed on the left pane of the wizard varies with the installation scenario. The configuration information provided during DSfW installation serves as input for the Provisioning Wizard to compute the list of tasks to be displayed.

For example: If you selected a non-name-mapped scenario for DSfW installation, the tasks to be performed for provisioning are different from the tasks to be performed if you selected a name-mapped scenario for installation. For details on the tasks for each provisioning scenario, see Section 7.6, "Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios," on page 131.

Task Description : The Task Description pane displays a short description of the task currently being performed. If you need more information on the task, select the *Help* option. This displays detailed help for the wizard.

Log Messages : The Log Messages pane displays details of events happening in the background and the status of each operation. To read more about logs, see Section 7.7, "Logging," on page 134.

The following table describes the functionality of the buttons in the Provisioning Wizard:

Table 7-1 *Provisioning Screen Buttons*

Option	Description
Skip	This option can be used in cases where you have already executed a task manually and then decide to execute rest of the tasks by using the Provisioning Wizard.
	When you click the *Skip* option, the next task is selected.
Run All	Select this option if you want all the tasks to be executed sequentially without manual intervention.
Run	Executes the current task.
Rerun	This option is displayed when a task fails to complete because of an error. Select this option to execute the task again.
Abort	Cancels the current task.
Help	Displays descriptive help for each task.

7.4 Using the Wizard to Provision the DSfW Server

1 After DSfW installation is done, you must run the Provisioning Wizard to complete the DSfW configuration process. To launch the wizard, do one of the following:

 ◆ From the terminal, run the /opt/novell/xad/sbin/provision_dsfw.sh script.

 ◆ Launch YaST. The DSfW Provisioning Wizard is listed as an option.

This opens the login dialog box.

NOTE: If you do not provision the DSfW server every time you login, a dialog box indicating that DSfW configuration is not complete is displayed. The DSfW server will not be functional till the provisioning is completed.

2 Enter the password in the login dialog box, depending on the scenario in which you are provisioning.

Table 7-2 *Authentication Details for Provisioning*

Provisioning Scenario	Password Details Required
Non-name-mapped, forest root domain	The current domain password.
Name-mapped, forest root domain	The current domain password and the tree admin password.
Non-name-mapped child	The current domain password, the parent domain password, and the tree/container admin password.
Name-mapped child	The current domain password, the parent domain password, and the tree/container admin password.
Subsequent Domain Controller	The current domain and tree admin password.

After the password details are verified, the Provisioning Wizard is launched.

IMPORTANT: If you are installing the first child domain in a non-name-mapped scenario, the tree admin and the parent domain password is the same.

For name mapped installation scenarios, the *Enable Custom Provisioning* check box is enabled. This check box remains disabled for all non-name mapped and ADC installation scenarios. To enable custom provisioning, continue with .

or

If you don't want to customize provisioning, leave the *Enable Custom Provisioning* check box deselected. Click *OK*, then follow the on-screen prompts to configure DSfW and the supporting services to complete the installation process and make the DSfW server ready for use.

3 Select the *Enable Custom Provisioning* check box and click *OK*. Custom provisioning enables you to add multiple eDirectory partitions to a DSfW domain.

4 Select the partitions that you want to map to the domain. When you select a partition, validation checks are performed on the partition before mapping it to the domain.

IMPORTANT: If the replica is not local, you cannot select the partition. To map a partition to the domain, you must first ensure that the replica is present on the local server and then click *Refresh* to reload the tree view. You can then select the partitions from the tree view.

5 Click *Next* to continue with the DSfW provisioning process.

7.5 Provisioning Tasks

The Provisioning Wizard lets you perform the following tasks:

7.5.1 Provisioning Precheck

This task verifies the state of the servers to ensure that they are ready for provisioning.

As part of the provisioning precheck activity, a health check is performed in the background to validate the state of the system to avoid a stale state. Not validating the system state can lead to irrecoverable failures in the system. This makes the health check very important.

The health check performs the following actions:

- Verifies that the services important for the installation, such as Kerberos, Samba, and NMB services, are running on the remote server.
- Verifies that the DNS service is active on the server configured as the DNS server.
- Verifies that all the servers that are part of the replica ring are active and that time is synchronized among the servers.
- Verifies that the version of eDirectory on the server where installation is done is 8.8 SP2 or later.
- In a name-mapped installation scenario, it checks the server to see if it contains any existing DSfW-specific objects.
- Triggers a purge on the remote server to clear deleted objects.

7.5.2 Configure DNS

This task configures DNS on the DSfW server. DSfW uses DNS as its location service, enabling computers to find the location of domain controllers.

As part of this task, the following actions are performed:

- Forward Lookup zones are configured for the domain to resolve queries on domain name lookup.
- Reverse Zones are configured for the domain to resolve requests that need to associate a DNS name with an IP address.
- Resource records of type NS, SRV, A, PTR are created.
- The zone references are added to the DNS Server, DNS Group object, and the DNS Locator object.

   Currently, DSfW is tightly coupled with Novell DNS and needs at least one DNS server to run on a domain controller.

NOTE: As part of DSfW installation, the DNS server is configured in the first domain in the forest. For subsequent child domains, you can either link to the DNS server in the first domain or install a DNS server for the child domain.

7.5.3 Create Domain Partition

This task creates a partition for the domain.

This partition has complete information about all the domain objects. Information about the domain objects is replicated to domain controllers in the same domain.

7.5.4 Add Domain Replica

This task adds the replica to the local server.

NOTE: This task is executed for all provisioning scenarios except for non-name-mapped and forest root domain installation.

7.5.5 Configure SLAPI Plug-Ins

This task loads the SLAPI plug-ins. The SLAPI plug-ins take care of maintaining the Active Directory information model. This ensures that the SLAPI framework is ready before any domain-specific data is added.

During the configuration process, the following tasks are performed:

 ◆ Attributes and Classes are mapped between Active Directory and eDirectory schema objects.
 ◆ The NLDAP server is refreshed and the SLAPI plug-ins are loaded.
 ◆ The NAD plug-in is checked to see if it is loaded.

7.5.6 Add Domain Objects

This task adds the domain objects that represent the domain-specific information under the domain partition.

The domain partition replicates data only to the domain controllers within its domain. In addition to this, it also creates containers for configuration and schema partitions that are later partitioned.

7.5.7 Create Configuration Partition

This task partitions the configuration container (cn=configuration) created as part of the Domain Objects Addition task. This configuration partition contains information on the physical structure and configuration of the forest (such as the site topology).

In case of a child domain installation, the replica of the configuration container is added to the local server.

The configuration partition is forest specific and by default the first domain controller of every domain gets a replica. The Additional Domain gets the replica of this partition if you select the *Replicate schema and configuration partitions* option in YaST during installation.

7.5.8 Create Schema Partition

This task partitions the schema container (cn=schema) created during the Domain Objects Addition task.

The schema partition contains the definition of object classes and attributes within the forest. If there is a child domain or an additional domain controller, replica of the schema container is added to the local server.

The schema partition is forest-specific and by default the first domain controller of every domain gets a replica. The Additional Domain gets the replica of this partition if you select the *Replicate schema and configuration partitions* option in YaST during installation.

7.5.9 Add Configuration Objects

This task adds the configuration and schema partition objects.

It helps maintain integrity with the Active Directory information model.

7.5.10 Add Domain Controller

This task adds the domain controller to the domain.

This task creates additional objects that make your server act as a domain controller. The task is only executed if you have installed DSfW as an subsequent domain controller in the domain.

7.5.11 Assign Rights

This task configures directory-specific access rights for the domain and the domain administrator being provisioned.

 The task performs the following activities:

- Computes effective ACLs.
- Imports NDS Super rights ACLs and sets rights for the administrator at the container level.
- Imports NDS Admin ACLs.

7.5.12 Restart DSfW Services

This task restarts services in order of dependence.

The restart is essential for the changes to be committed. The services that are restarted, as part of this task are:

1. ndsd (eDirectory)
2. novell-named (DNS)
3. nscd (Name Server cache daemon)
4. rpcd (RPC server)
5. xad-krb5kdc (Kerberos)
6. xad-kpasswdd (Kpassword)
7. xadsd (XAD daemon)
8. nmb (NMB server, NETBIOS lookup)
9. winbind
10. smb (Samba)
11. sshd (SSH)
12. rsyncd (rsync)

After the services are restarted, your domain is up. However, before it is ready for use, you need to perform the remaining tasks in the provisioning wizard.

7.5.13 Set Credentials for Accounts

This task sets the password and kerberizes the administrator, krbgt, and guest accounts.

7.5.14   Enable Kerberos

In DSfW, Kerberos is the primary security protocol for authentication within a domain. The Kerberos authentication mechanism issues tickets for accessing network services.

As part of this task, the `krb5.conf` file is updated and a ticket is sent to the administrator principal.

These changes trigger a change in the Kerberos Policy files that are stored in `sysvol`. This change requires a synchronization update to eDirectory, which is done by using the `gpo2nmas` utility.

7.5.15   Samify Objects

This task is specific to a name-mapped installation. The existing user and group objects are extended to receive Active Directory attributes that allow them to be part of the domain being provisioned. Some of the extended attributes are supplementary Credentials, objectSid, and samAccountName.

7.5.16   Establish Trust

A trust is a relationship established between domains that enables users in one domain to be authenticated by a domain controller in the other domain. Authentication between domains occurs through trusts.

This task establishes two-way transitive trust relationships between the domain being provisioned and the parent domain. In a transitive trust, all the domains belonging to the same forest trust each other. If any more new domains are added, an automatic trust relationship is established between the root domain and the new domain.

For example: If domain A trusts domain B and domain B trusts domain C, then users from domain C can access resources in domain A.

7.5.17   Update Service Configuration

This task modifies the configuration of services such as sshd, rsync and krb5. It configures the `sysvol` policies, synchronizes the group policies with NMAS, and adds a crontab entry for subsequent synchronization of policies.

7.5.18   Cleanup

This task removes files from a partial or failed installation. It also removes the temp directories and checkpoint files created during provisioning.

7.6   Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios

The following table lists the provisioning tasks corresponding to each installation scenario.

Table 7-3 *Provisioning Tasks for Different Installation Scenarios*

Installation Scenario	Provisioning Tasks
Installing DSfW in a Non-Name-Mapped Setup (Forest Root Domain)	◆ Provisioning Precheck ◆ Configure DNS ◆ Create Domain Partition ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Update Service Configuration ◆ Cleanup
Installing DSfW in a Name-Mapped Setup (Forest Root Domain)	◆ Provisioning Precheck ◆ Configure DNS ◆ Add Domain Replica ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Samify Objects ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Update Service Configuration ◆ Cleanup

Installation Scenario	Provisioning Tasks
Installing DSfW in a Name-Mapped Setup(Child domain)	◆ Provisioning Precheck ◆ Configure DNS ◆ Add Domain Replica ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Samify Objects ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Establish Trust ◆ Update Service Configuration ◆ Cleanup
Installing DSfW in a Non-Name-Mapped Setup (Child domain)	◆ Provisioning Precheck ◆ Configure DNS ◆ Create Domain Partition ◆ Add Domain Replica ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Establish Trust ◆ Update Service Configuration ◆ Cleanup

Installation Scenario	Provisioning Tasks
Installing DSfW as a Subsequent Domain Controller in a Domain	◆ Provisioning Precheck
	◆ Add Domain Replica
	◆ Configure SLAPI Plug-Ins
	◆ Create Configuration Partition
	◆ Create Schema Partition
	◆ Add Domain Controller
	◆ Assign Rights
	◆ Restart DSfW Services
	◆ Update Service Configuration
	◆ Configure DNS
	◆ Cleanup

7.7 Logging

The Log Messages pane in the Provisioning Wizard displays the details and status of events happening in the background during the execution of each task.

The log details are displayed on the GUI and also logged in the `/var/opt/novell/xad/log/provisioning.log` file.

The details that are recorded in the log file are:

- ◆ The status of each task.
- ◆ The status of health check operations
- ◆ The output, error messages, and warnings printed by utilities such as `ldapsearch`, and `ldapconfig`.

Tasks return a zero value on success and specific error codes on failure. These error codes provide useful information for debugging purposes.

Table 7-4 *Error Code Identifiers*

Error Codes	Module
101-110	Remote Server Health Check
111-120	DNS Server Status
121-130	Bad Address Cache
131-140	Purger Execution
141-150	Top Level Container Check
151-160	eDirectory Server Status

In addition to the `provisioning.log` file that contains information on tasks executed through the Provisioning Wizard, you can use the following log files for debugging purposes:

Table 7-5 *Additional Log Files*

Log file	What it Contains
`/var/opt/novell/xad/log/healthcheck.log`	Contains details about health check process
`/var/opt/novell/xad/log/ndsdcinit.log`	Contains log messages from the install framework. Details recorded include: ◆ Commands executed ◆ Success or failure of each operation ◆ Pre and post check operation details.

7.8   Troubleshooting

This section describes some issues you might experience with Novell Domain Services for Windows(DSfW) while provisioning and provides suggestions for resolving or avoiding them.

◆ Section 7.8.1, "Troubleshooting Provisioning Tasks," on page 135

7.8.1   Troubleshooting Provisioning Tasks

This section describes the errors that you might experience while executing the Provisioning tasks and provides details for resolving them.

◆ "Provisioning Precheck" on page 135
◆ "Configure DNS" on page 136
◆ "Configure SLAPI Plug-in" on page 137
◆ "Create Domain Partition" on page 138
◆ "Add Domain Replica" on page 138
◆ "Add Domain Objects" on page 139
◆ "Create Configuration Partition" on page 140
◆ "Create Schema Partition" on page 140
◆ "Add Configuration Objects" on page 141
◆ "Assign Rights" on page 142
◆ "Establish Trust" on page 142
◆ "Update Service Configuration" on page 142
◆ "Cleanup" on page 143

Provisioning Precheck

All details related to task execution and state of the task are recorded in the `provisioning.log` file

Error: Provisioning Pre-check Failed

Cause: The provisioning pre-check scripts check for existence of schema and configuration partition in the first domain controller. If the first domain controller does not have a schema and configuration partition, it fails to locate the partitions, an error is thrown.

Solution: It is recommended that you select the Replicate schema and configuration Partitions option during installation. If you have failed to do that, replicate the partitions using iManager. For more information, see Administering Replicas (http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html)

Configure DNS

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- ◆ "Error: Insufficient Access" on page 136
- ◆ "Entry already Exists" on page 136
- ◆ "ldapmodify Failed" on page 136
- ◆ "No such Entry" on page 136

Error: Insufficient Access

Cause: The administrator being used to execute the `ldapmodify` command does not have privileges to complete the operation.

Solution 1: In the `provisioning.log` file, search for the `ldapmodify` command. Make sure the administrator used to execute that command has adequate privileges to execute this command.

Solution 2: If the DNS Locator and Group objects are outside the domain partition, make sure the administrator has privileges to access the objects.

Entry already Exists

Cause: You see this error when you retry executing a task and the task fails during execution.

Solution: For any task that has failed, delete the associated objects from the server and then retry the task.

Depending on the task that failed, different objects are created. For instance, if the DNS Configuration task failed, you need to delete the Locator object and the Group object

ldapmodify Failed

Cause: Replica synchronization fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

No such Entry

Cause:

This error is seen in cases where the version of the forest root domain is OES 2 SP1 and you are attempting to install a subsequent domain controller of version OES 2 SP2.

Solution:

   1 To resolve this issue, run the provisioning script with the get-domain-guid option. For example:

```
/opt/novell/xad/share/dcinit/provisionTools.sh get-domain-guid -p 192.168.3.11 -c
ou=domain,o=novell
```

Here *-p* represents the IP address of the domain and *-c* represents the distinguished name of the mapped domain.

This command returns the GUID value of the domain.

2 Using iManager, search and select the zone object of the domain.

For more details about using iManager see, Browsing Objects (http://www.novell.com/documentation/imanager27/imanager_admin_273/data/bob1yft.html)

3 In the zone, search for the DNS record with the following entry:

```
_ldap._tcp.DOMAIN-GUID.domains._msdcs.DOMAIN.COM
```

4 If the entry does not have a valid GUID, replace the incorrect GUID value with the correct GUID value obtained from Step 1.

5 Check the value of the domain GUID in the dnipdnsdomainname attribute. If found to be incorrect, replace the replace the incorrect GUID value with the correct GUID value obtained from Step 1.

Configure SLAPI Plug-in

- ◆ "Error: Insufficient Access" on page 137
- ◆ "Entry already Exists" on page 137
- ◆ "ldapmodify Failed" on page 137

Cause:

The NAD Plug-in is not loaded

Solution:

Execute ldapsearch on the LDAP server object to find out adman NAD plug-in is configured.

Perform LDAP server refresh using iManager or using the ldapconfig -R -a *<admin>* -w *<passwd>* command.

Error: Insufficient Access

Cause: The administrator being used to execute the ldapmodify command does not have privileges to complete the operation.

Solution : In the provisioning.log file, search for the ldapmodify command. Make sure the administrator used to execute that command has adequate privileges to execute this command.

Entry already Exists

Cause: You see this error when you retry executing a task and the task fails during execution.

Solution: For any task that has failed, delete the associated objects from the server and then retry the task.

Depending on the task that failed, different objects are created. For instance, if the DNS Configuration task failed, you need to delete the Locator object and the Group object

ldapmodify Failed

Cause: Replica synchronization fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Create Domain Partition

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- "Error: 626 All Referrals Failed" on page 138
- "Error: 625 Transport Failure/ Unknown Error" on page 138
- "Error: 30 Retry Entries to Get the Replica Status in the Log File" on page 138

Error: 626 All Referrals Failed

Cause: The synchronization process between the replicas fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Error: 625 Transport Failure/ Unknown Error

Cause: The DSfW server could not reach the master server. For example, installing a child server requires the parent server to be reachable, or installing a DSfW server in the name-mapped forest root domain scenario requires the server holding the tree replica to be reachable.

Solution 1: Ensure that the servers are reachable. Remove the bad address cache from the servers by using the following command:

```
set ndstrace=*UP
```

Try executing the task again.

Solution 2: Try executing the provisioning task manually. For details see, Executing Provisioning Tasks Manually.

Error: 30 Retry Entries to Get the Replica Status in the Log File

Cause: A very slow network link can cause incomplete operations and multiple retries.

Solution: Check the speed of your network link. Try executing the task again.

Add Domain Replica

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- "Error: 626 All Referrals Failed" on page 138
- "Error: 625 Transport Failure/ Unknown Error" on page 139
- "Error: 30 Retry Entries to Get the Replica Status in the Log File" on page 139

Error: 626 All Referrals Failed

Cause: The synchronization process between the replicas fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Error: 625 Transport Failure/ Unknown Error

Cause: The DSfW server could not reach the master server. For example, installing a child server requires the parent server to be reachable, or installing a DSfW server in the name-mapped forest root domain scenario requires the server holding the tree replica to be reachable.

Solution 1: Ensure that the servers are reachable. Remove the bad address cache from the current server by using the following command:.

```
set ndstrace=*UP
```

Try executing the task again.

Solution 2: Try executing the provisioning task manually. For details see, Executing Provisioning Tasks Manually.

Error: 30 Retry Entries to Get the Replica Status in the Log File

Cause: A very slow network link can cause incomplete operations and multiple retries.

Solution: Check the speed of your network link. Try executing the task again.

Add Domain Objects

All details related to task execution and state of the task are recorded in the `provisioning.log` file.

- "Error: Insufficient Access" on page 139
- "Entry already Exists" on page 139
- "ldapmodify Failed" on page 139

Error: Insufficient Access

Cause: The administrator being used to execute the `ldapmodify` command does not have privileges to complete the operation.

Solution: In the `provisioning.log` file, search for the `ldapmodify` command. Make sure the administrator used to execute that command has adequate privileges to execute this command.

Entry already Exists

Cause: You see this error when you retry executing a task and the task fails during execution.

Solution: For any task that has failed, delete the associated objects from the server and then retry the task.

Depending on the task that failed, different objects are created. For instance, if the DNS Configuration task failed, you need to delete the Locator object and the Group object

ldapmodify Failed

Cause: Replica synchronization fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Create Configuration Partition

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- "Error: 626 All Referrals Failed" on page 140
- "Error: 625 Transport Failure/ Unknown Error" on page 140
- "Error: 30 Retry Entries to Get the Replica Status in the Log File" on page 140

Error: 626 All Referrals Failed

Cause: The synchronization process between the replicas fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Error: 625 Transport Failure/ Unknown Error

Cause: The DSfW server could not reach the master server. For example, installing a child server requires the parent server to be reachable, or installing a DSfW server in the name-mapped forest root domain scenario requires the server holding the tree replica to be reachable.

Solution 1: Ensure that the servers are reachable. Remove the bad address cache from the current server by using the following command:.

```
set ndstrace=*UP
```

Try executing the task again.

Solution 2: Try executing the provisioning task manually. For details see, Executing Provisioning Tasks Manually.

Error: 30 Retry Entries to Get the Replica Status in the Log File

Cause: A very slow network link can cause incomplete operations and multiple retries.

Solution: Check the speed of your network link. Try executing the task again.

Create Schema Partition

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- "Error: 626 All Referrals Failed" on page 140
- "Error: 625 Transport Failure/ Unknown Error" on page 141
- "Error: 30 Retry Entries to Get the Replica Status in the Log File" on page 141

Error: 626 All Referrals Failed

Cause: The synchronization process between the replicas fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Error: 625 Transport Failure/ Unknown Error

Cause: The DSfW server could not reach the master server. For example, installing a child server requires the parent server to be reachable, or installing a DSfW server in the name-mapped forest root domain scenario requires the server holding the tree replica to be reachable.

Solution 1: Ensure that the servers are reachable. Remove the bad address cache from the current server by using the following command:.

```
set ndstrace=*UP
```

Try executing the task again.

Solution 2: Try executing the provisioning task manually. For details see, Executing Provisioning Tasks Manually.

Error: 30 Retry Entries to Get the Replica Status in the Log File

Cause: A very slow network link can cause incomplete operations and multiple retries.

Solution: Check the speed of your network link. Try executing the task again.

Add Configuration Objects

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- "Error: Insufficient Access" on page 141
- "Entry already Exists" on page 141
- "ldapmodify Failed" on page 141

All details related to task execution and state of the task are recorded in the `provisioning.log` file

Error: Insufficient Access

Cause: The administrator being used to execute the `ldapmodify` command does not have privileges to complete the operation.

Solution: In the `provisioning.log` file, search for the `ldapmodify` command. Make sure the administrator used to execute that command has adequate privileges to execute this command.

Entry already Exists

Cause: You see this error when you retry executing a task and the task fails during execution.

Solution: For any task that has failed, delete the associated objects from the server and then retry the task.

Depending on the task that failed, different objects are created. For instance, if the DNS Configuration task failed, you need to delete the Locator object and the Group object

ldapmodify Failed

Cause: Replica synchronization fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Assign Rights

All details related to task execution and state of the task are recorded in the `provisioning.log` file

- "Error: Insufficient Access" on page 142
- "Entry already Exists" on page 142
- "ldapmodify Failed" on page 142

All details related to task execution and state of the task are recorded in the `provisioning.log` file

Error: Insufficient Access

Cause: The administrator being used to execute the `ldapmodify` command does not have privileges to complete the operation.

Solution 1: In the `provisioning.log` file, search for the `ldapmodify` command. Make sure the administrator used to execute that command has adequate privileges to execute this command.

Solution 2: If the DNS Locator and Group objects are outside the domain partition, make sure the administrator has privileges to access the objects.

Entry already Exists

Cause: You see this error when you retry executing a task and the task fails during execution.

Solution: For any task that has failed, delete the associated objects from the server and then retry the task.

Depending on the task that failed, different objects are created. For instance, if the DNS Configuration task failed, you need to delete the Locator object and the Group object

ldapmodify Failed

Cause: Replica synchronization fails.

Solution: To resolve this issue, refer Novell Error Codes Reference Guide (http://www.novell.com/documentation/nwec/?page=/documentation/nwec/nwec/data/al39nky.html)

Establish Trust

Cause

This error occurs in cases where the parent realm could not be resolved

Solution

Use the `provision -q -q --locate-dc parent.domain` command to resolve the parent domain. Retry executing the task.

Update Service Configuration

Cause

This error occurs in cases where the parent realm could not be resolved

Solution

Use the `provision -q -q --locate-dc parent.domain` command to resolve the parent domain. Retry executing the task.

Cleanup

Cause

This error occurs in cases where the parent realm could not be resolved

Solution

Use the `provision -q -q --locate-dc parent.domain` command to resolve the parent domain. Retry executing the task.

7.9 Executing Provisioning Tasks Manually

For details on executing Provisioning tasks manually, see Executing Provisioning Tasks Manually

8 Activities After DSfW Installation or Provisioning

This section discusses details about activities that can be performed after DSfW installation or provisioning.

8.1 Verifying the Installation

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

NOTE: After you have installed a child domain or an subsequent 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:

```
rcnovell-named restart
```

☐ 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.dsfw.com oesdc
```

☐ Check the `/etc/resolv.conf` file to ensure that it contains a name server and domain search entry for server on which DNS is hosted. For example:

```
nameserver 192.168.1.1
search dsfw.com
```

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

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

This command returns information similar to the following:

```
Tree Name: DSFW_TREE

Server Name:.CN=OESDC.OU=OESSystemObjects.dc=dsfw.dc=com.T=DSFW_TREE

Binary Version: 20217.06

Root Most Entry Depth: 0

Product Version: eDirectory for Linux v8.8 SP5 [DS]
```

☐ Execute `xadcntrl validate` at the terminal prompt.

If the services are configured correctly, the result of the command will be similar to the following output:

```
Tree Name: DSFW-TREE
Server Name: .CN=testfrd.OU=OESSystemObjects.dc=dsfw.dc=com.T=DSFW-TREE.
Binary Version: 20501.00
Root Most Entry Depth: 0
Product Version: eDirectory for Linux v8.8 SP5 [DS]

Checking for nameserver BIND
number of zones: 2
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/1000
tcp clients: 0/100
server is up and running
zone details are dumped at /var/opt/novell/log/named/named_zones.info


Checking for Name Service Cache Daemon:                           running
Checking for RPC Endpoint Mapper Service                          running
Checking for Kerberos KDC Service                                 running
Checking for Kerberos Password Change Server                      running
Checking for Domain Services Daemon                               running
Checking for Samba NMB daemon                                     running
Checking for Samba  WINBIND daemon                                running
Checking for Samba SMB daemon                                     running
Checking for service sshd                                         running
Checking for rsync daemon:                                        running
```

❐ Execute the following commands:

kinit administrator@domainname

rpcclient -k localhost –c dsroledominfo

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.
```

8.2 Renaming Administrator Details Using MMC

If you rename the administrator account using MMC, only AD-specific attributes like sAMAccountName are modified. You may be required to update the uniqueID attribute if you want to use the renamed administrator account for iManager administration. For more information, see Section 19.1.9, "iManager Fails to Create Samba Shares if the Administrator Name is Changed using MMC," on page 238.

NOTE: You must not use special characters such as $ ` ! ' while renaming a domain administrator, because if the domain administrator name contains any of these special characters, any ADC or child domain installations to the domain will not succeed.

---

1 On 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 *Users*.

4 In the details pane, right-click the user account that you want to rename, and then click *Rename*.

5 Type the new full name of the user account, then press ENTER to display the Rename User dialog box.

6 Fill in the following fields:

First name: Specify the first name of the user.

Last name: Specify the last name of the user.

Display name: Specify the user name to be displayed in Active Directory.

User logon name: Specify the user logon name and select the user principal name (UPN) suffix in the drop-down list. This field represents the userPrincipleName attribute.

User logon name (pre-Windows 2000): Specify a name for the user that is unique to the Active Directory forest. This field represents the sAMAccountName attribute.

7 Click *OK*.

8.3 Extending the Domain Post Provisioning

DSfW enables you to map multiple partitions to the domain post provisioning by using the domain partition management tool. The domain partition management tool manages partitions in the domain name space by adding or removing partitions. The tool can be used to manage local as well as remote domains, and it must be executed only from a DSfW server. The tool uses the following syntax:

```
domaincntrl <Operation> [arguments]
```

NOTE: To perform `add` and `remove` operations, you must ensure that all the domain controllers of a domain are up and reachable.

Operation	Description
--list	Lists the current domain partition list.

--add	Adds a partition to the domain name space. You can use this operation to specify the partition to be added to the domain name space from the list of partitions that are displayed. When you specify a partition, the tool runs validation checks on the partition before adding it to the domain name space. When the partition is added to the domain name space, the partition is samified.
	
	The add operation cannot be performed for the following:
	
	    ◆ Domain root partition
	    ◆ Configuration partition
	    ◆ Schema partition
	
	NOTE: To add a partition to the domain, all the domain controllers must have either read/write or master replica of the partition that is being added.

Operation	Description
--remove	Removes the specified partition from the domain name space. When you specify a partition, the tool runs validation checks on the partition before removing it from the domain name space. When the partition is removed from the domain name space, the partition is desamified.
	The remove operation cannot be performed for the following:
	♦ Domain root partition
	♦ Configuration partition
	♦ Schema partition
--samify	Samifies the specified partition. Samification can be done only for domain partitions. The add operation calls this operation internally. However, if samification is not successful when you use the add operation, you can perform samification explicitly by using this operation. If the specified partition contains several users or groups, the samification process can be time-consuming.
--desamify	Desamifies the specified partition. This operation can be run only on local domains and not on remote domains. The remove operation calls this operation internally. However, if desamification is not successful when you use the remove operation, you can perform desamification explicitly by using this operation.
--help	Displays usage of the command.

Arguments	Description
-a	Specifies the remote domain name. This argument cannot be used with the desamify operation.
-d	Enables debugging.
-F	Lists the partition mapping forest-wide. This argument is used only with the list operation.
-o	Sends debug logs to the specified file.

8.3.1 Examples

domaincntrl --list

Lists the current local domain partition list.

domaincntrl --list -F

Lists the partition list of each domain in the forest.

domaincntrl --list -a example.com

Lists the partition list of the example.com remote domain.

domaincntrl --add -d

Adds a partition to the local domain name space with debugging enabled.

domaincntrl --add -a example.com

> Adds a partition to the remote domain name space.

domaincntrl --remove -d -o /tmp/out.txt

> Removes a partition from the local domain name space with debugging enabled and saves the logs to the `out.txt` file.

domaincntrl --samify

> Samifies the specified domain partition.

domaincntrl --samify -a example.com

> Samifies the example.com remote domain partition.

domaincntrl --desamify

> Desamifies the specified partition.

9 Upgrading DSfW

This section provides information and links for upgrading DSfW to OES 2 SP3.

9.1 Upgrading DSfW to OES 2 SP3

This section helps you understand the types of upgrade, prerequisites for upgrading, and the upgrade process.

9.1.1 Upgrade Scenario

If a DSfW domain has multiple domain controllers, it is recommended to upgrade the primary domain controller first, followed by the upgrade of the remaining domain controllers. If all the domain controllers are not upgraded to the same patch level, the OES 2 SP3 features will not be available.

To determine the IP address of the server that is the primary domain controller, use the following command:

```
dig -t SRV _ldap._tcp.pdc._msdcs._DOMAIN_NAME_ +short
```

Here, _DOMAIN_NAME_ is the domain name of the current domain, for example dsfw.com. In a DSfW setup that has multiple domains like FRD or child domain, the upgrade can be commenced from any domain.

9.1.2 Supported Mixed Mode configurations

Mixed mode DSfW domains in a DSfW forest is supported. However, it is recommended to have all the domain controllers of a domain run the same version of OES. You can have DSfW domains run different versions of OES (SP1,SP2,and SP3) in the same DSfW forest. However, SP2-specific features will only work in domains that run OES 2 SP2 and above. Similarly, SP3-specific features will only work in domains that run OES 2 SP3.

9.1.3 Prerequisite

Before running the upgrade process, ensure that time is synchronized between all the servers in the replica ring.

9.1.4 Channel Upgrade

You can perform channel upgrade in silent or interactive mode.

- "Silent mode" on page 152
- "Interactive mode" on page 152

Silent mode

You can perform channel upgrade in silent mode by creating an answer file that contains the domain administrator password. For information on creating an answer file, refer to "Creating a Password Answer File" in the *OES 2 SP3: Installation Guide* .

Interactive mode

Upgrade process in interactive mode requires user intervention. To run the upgrade process in this mode, refer to "Performing the Upgrade" in the *OES 2 SP3: Installation Guide*.

9.1.5 Media Upgrade

Media upgrade involves upgrading in an offline mode from a physical media such as CD or DVD. For step-by-step instructions, refer to "Using Physical Media to Upgrade (Offline)" in the *OES 2 SP3: Installation Guide*.

9.1.6 Troubleshooting

- "Channel Upgrade from OES 2 SP2 to OES 2 SP3 Fails" on page 153
- "Samba cache File Corruption" on page 153
- "Upgrade Fails" on page 153

Channel Upgrade from OES 2 SP2 to OES 2 SP3 Fails

A channel upgrade from OES 2 SP2 to OES 2 SP3 fails after the RPMs are installed and the server is rebooted. The failure is observed while updating the domain with the ACL of the uniqueDomainID attribute.

To prevent this failure, after the RPMs are updated, you must extend the DSfW schema and reboot the server. For more information, refer to the TID 7007505 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7007505&sliceId=2&docTypeID=DT_TID_1_1&dialogID=242581535&stateId=0 0 242579776).

Samba cache File Corruption

After upgrading, you may encounter a Samba cache file corruption issue. Follow the instruction documented in "Error Mapping SID to UID" on page 244 to resolve the error.

Upgrade Fails

If upgrade to OES 2 SP3 fails during the post-configuration phase, then the upgrade tool will not retry and upgrade of other OES components will continue. You must rerun the upgrade scripts based on the upgrade scenario.

OES 2 SP1 to OES 2 SP2 upgrade: Use the script `/opt/novell/xad/share/dcinit/upgrade_sysvol.pl`

OES 2 SP1 or OES 2 SP2 to OES 2 SP3 upgrade: Use the script `/opt/novell/xad/sbin/upgrade_dsfw.pl`

You must also ensure that the kerberos ticket is up-to-date. To obtain the domain administrator's ticket use kinit.

```
kinit <Adminstrator Name>
```

9.2   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 NetWare or Linux server.

9.3   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 SP3: Migration Tool Administration Guide*

9.4 Limitations

An error is seen in cases where the version of the forest root domain is OES 2 SP1 and you are attempting to install a subsequent domain controller of version OES 2 SP2. To resolve the error, see "No such Entry" on page 136.

10 Running Domain Services for Windows in a Virtualized Environment

Domain Services for Windows runs in a virtualized environment just as it does on a physical Open Enterprise Server (OES) 2 Linux server and requires no special configuration or other changes.

To get started with virtualization, see "Introduction to Xen Virtualization (http://www.novell.com/documentation/sles10/book_virtualization_xen/?page=/documentation/sles10/book_virtualization_xen/data/sec_xen_basics.html)" in the Virtualization with Xen (http://www.novell.com/documentation/sles10/book_virtualization_xen/?page=/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html) guide.

For information on setting up virtualized OES 2 Linux, see "Installing, Upgrading, or Updating OES on a Xen-based VM" in the *OES 2 SP3: Installation Guide*.

11 Logging In from a Windows Workstation

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.

- Section 11.1, "Joining a Windows Workstation to a DSfW Domain," on page 157
- Section 11.2, "Logging In to a DSfW Domain," on page 160
- Section 11.3, "Logging Out," on page 160
- Section 11.4, "Limitations," on page 160

11.1 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.

You must ensure that the workstations joined to a DSfW domain have a unique machine name. A duplicate machine name will lead to an unstable domain and slow workstation logins. If you attempt to join a machine with a duplicate name to a DSfW domain, no warning or error messages will be displayed.

In case you experience slow workstation logins because of duplicate machine names in your environment, you can enforce intruder lockout. For more information, refer to the TID (http://www.novell.com/support/viewContent.do?externalId=7006851).

NOTE: A duplicate machine name may get assigned due to reuse of the machine name or re imaging the machines in a virtualized environment.

Execute the following 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*.
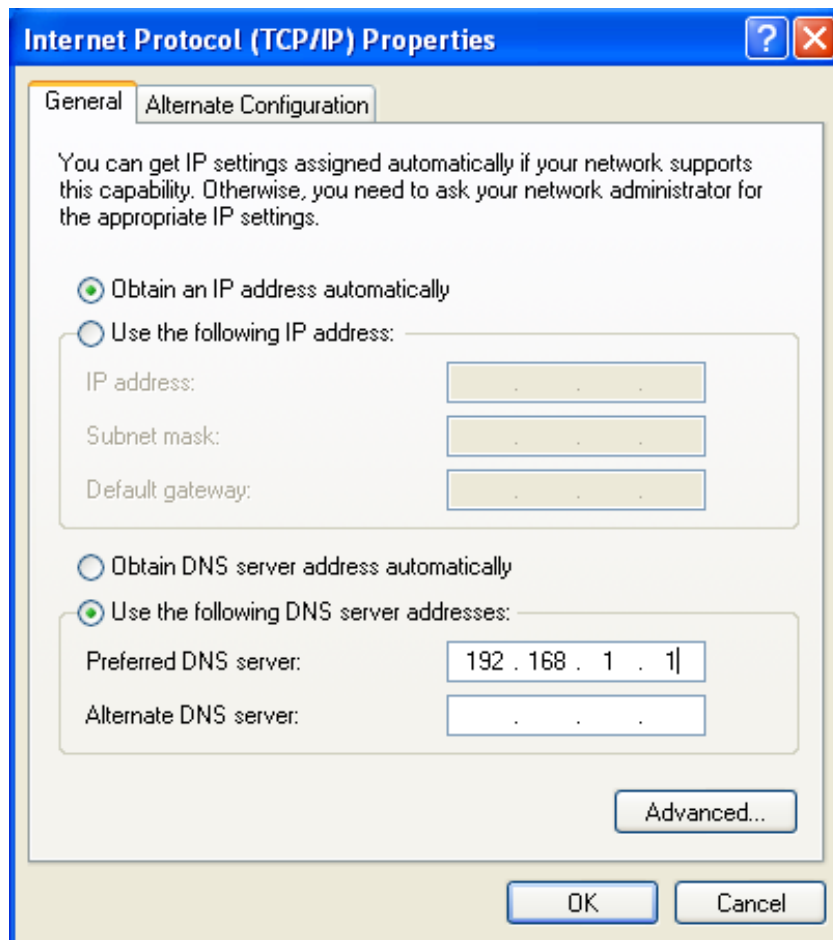
4 From the Start menu, right-click *My Computer* and select *Properties*.

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*.
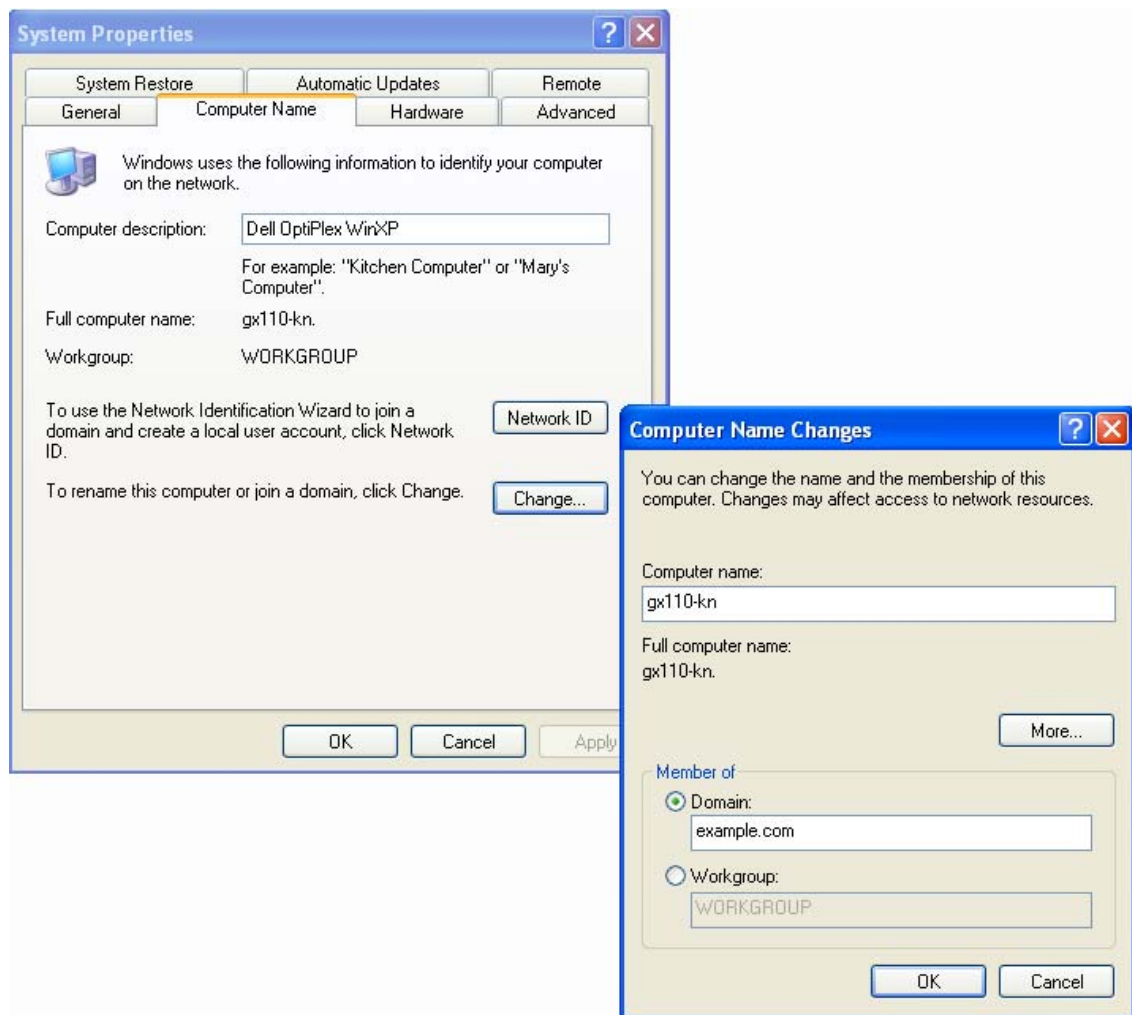
7 When prompted, provide the name and password for an account with permission to join the domain. This is the Administrator and password configured when you installed DSfW.

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.

11.2 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 11.1, "Joining a Windows Workstation to a DSfW Domain," on page 157), 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*.

11.3 Logging Out

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

11.4 Limitations

This section covers the limitations and known issues that you may encounter while joining a workstation to a domain and logging in.

11.4.1 Joining a Workstation that Has Novell Client Installed

While joining a workstation to a domain, you do not need to have Novell Client installed. But if you have Novell Client installed on your workstation, it will affect DSfW communication. We recommend that you add the IP address of the DSfW server to the Bad Address Cache of the Novell Client.

For more information see, AppNote: Novell Client 4.9 SP2: Initialization, Login and Settings (http://www.novell.com/coolsolutions/appnote/620.html)

11.4.2 Error while Joining a Workstation to a Domain

This error can occur due to the extra attributes that gets added in the Domain Password Policy after it has been opened using the iManager Passwords Plug-in and saved without making any changes.

To resolve this issue, see TID 7004481 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004481)

11.4.3 Error While Joining a Workstation to a Domain if Time is Not Synchronized

While joining a workstation to a domain, you must ensure that the system time is synchronized between the Windows workstation and the DSfW server. Otherwise, you will receive an error indicating incorrect username or password. An error message similar to the following is logged in the `/var/opt/novell/xad/log/kdc.log` file:

```
Dec 04 10:50:37 sles10sp3 krb5kdc[5048](info): preauth (timestamp) verify failure:
Clock skew too great
Dec 04 10:50:40 sles10sp3 krb5kdc[5048](info): AS_REQ (7 etypes {23 -133 -128 3 1
24 -135}) 192.168.100.129: PREAUTH_FAILED: Administrator@NTS.NOVELL.COM for
krbtgt/NTS.NOVELL.COM@NTS.NOVELL.COM, Clock skew too great
```

12 Creating Users

After Domain Services for Windows (DSfW) is properly installed and provisioned, 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 DSfW 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.

12.1 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 accidently attempt to log in as an administrator of an domain where you lack sufficient access.
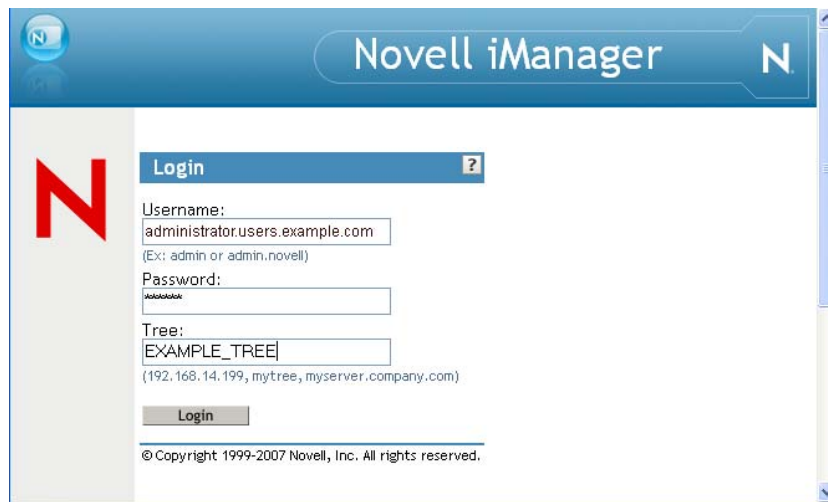
3 Under Roles and Tasks, select *Directory Administration > Create Object*.

4 Select the User object class and click *OK*.
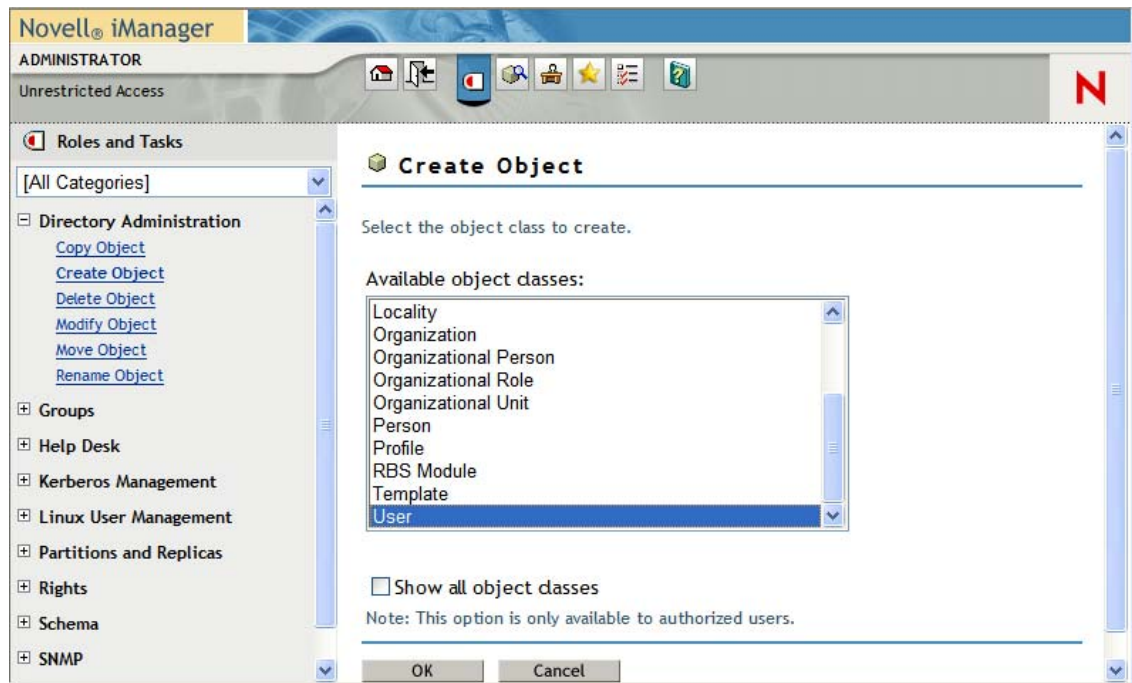
5 Specify the user account information, specify the context, and click *OK*.

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.

12.2 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).

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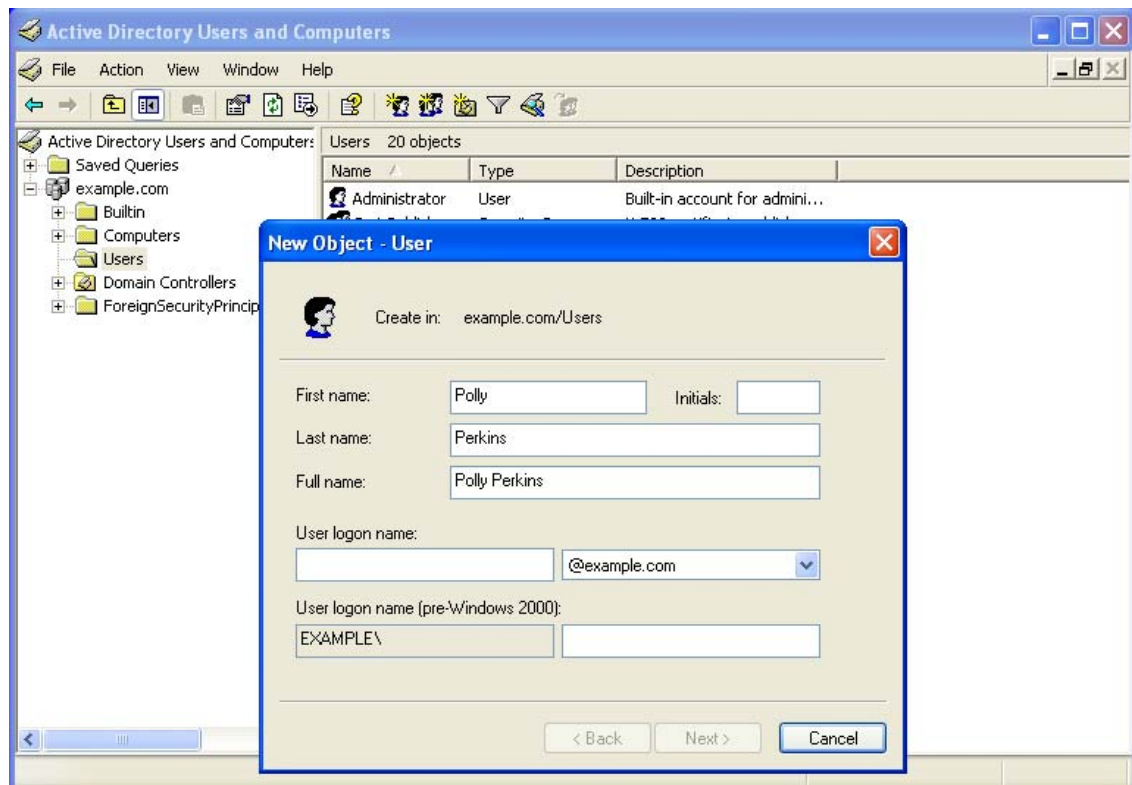
7 Follow the prompts to complete the user object creation.

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.

12.3 Moving Users Associated with Password Policies

When a user is moved into a DSfW domain and the associated password policy of the moved user does not fall under the domain boundary, the generation of the DSfW-specific authentication keys of the moved user might fail unless the associated password policy is in the security container. This is because the DSfW server (NCP server object) does not have permissions on the associated password policy object of the moved user, if the password policy object is not present either in the security container or the domain boundary.

You must ensure that all the DSfW servers (domain controllers) of a DSfW domain are granted read rights on the associated password policy. On the other hand, if the associated password policy of the moved user is located in the security container, the generation of DSfW-specific authentication keys is seamless as every server in the eDirectory Tree has preassigned rights on the security container.

It is recommended to have the password policies in the security container which allows moving users into the DSfW domain to work seamlessly. Alternatively, if the associated password policy is not under security container, you must grant Read and Compare permissions for *[All Attributes Rights]* on the password policy object for all the NCP server objects of the domain controllers of a DSfW domain.

12.4 Limitations

12.4.1 User Samification Fails On Moving Users into a DSfW Domain

When you move a user into a DSfW domain, the user samification fails. This means that AD attributes will not be generated for this user and hence the user will not be a part of the domain. This issue occurs when master replica of the domain partition is present on a non-DSfW server.

12.4.2 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.

12.4.3 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.

12.4.4 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.

12.4.5 Dynamic Groups Is Not Supported in DSfW

DSfW server does not support Dynamic Groups. However if applications are connected to plain eDirectory servers, dynamic groups will function as expected.

13 **Understanding DNS in Relation to DSfW**

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the network. DNS stores information in a distributed, coherent, reliable, autonomous, and hierarchical database.

DSfW uses the Novell DNS service as its location service, enabling users or computers to find the location of network resources. It maps hostnames to IP addresses and locates the services provided by the domain, such as LDAP, Kerberos and Global Catalog.

Novell DNS Services in Open Enterprise Server (OES) 2 Linux integrates the Domain Name System (DNS) service into eDirectory. Integrating this service into eDirectory provides centralized administration and enterprise-wide management of DNS by using either iManager or the Java Management Console. The Novell DNS configuration information is replicated just like any other data in eDirectory.

NOTE: A Novell DNS server can only be managed by using the iManager or Java Management Console utility. The DNS YaST plug-in or the DNS plug-in of Microsoft Management Console (MMC) do not support managing a Novell DNS server.

13.1 **DSfW and DNS**

DSfW uses the Novell DNS service that is included with OES. The DNS server that gets installed when you choose the DSfW pattern for installation is configured with DSfW-specific configuration.

While installing the first domain controller of a domain, you can configure a new DNS server or use an existing parent domain DNS server to host the new domain information. By default, the first domain controller in the forest root domain is automatically configured to be the DNS server. This is done for both name-mapped and non-name-mapped installations, if the *Configure this server as a Primary DNS server* option in YaST is selected while configuring the first domain controller of the forest root domain.

When a domain controller is added to a forest, the DNS zone hosted on a DNS server is updated with the DNS Locator object, the Address (A) record and the Service (SRV) record. To find domain controllers in a domain or forest, a client queries DNS for the SRV and A resource records of the domain controller. These records help in domain name resolution and service identification. For more information about A and SRV resource records, see "Types of Resource Records" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*.

While provisioning the DSfW server, secure dynamic updates are enabled as part of the *Update Service Configuration* task. Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

An existing DSfW DNS server can be migrated to Active Directory DNS in order to facilitate management of DNS data from the MMC DNS plug-in. However, migration of DNS does not provide Active Directory's inherent storage and replication benefits. For information about how to migrate DSfW DNS to Active Directory DNS, see Setting Up a Windows DNS Server for DSfW.

It is also possible to migrate an existing DSfW DNS server to any other domain controller of the same domain or to a domain that has a read/write replica of the partition where the zone records are located. For details, see Section 13.4, "Migrating DNS to Another Domain Controller," on page 172

13.1.1 Limitations

- It is not possible to use an existing Novell DNS server configured on a local or remote server to work with DSfW.
- Third-party DNS servers are also not supported, with the exception of the Windows DNS, which can later be used by transferring the DNS data from an existing DSfW DNS to the Windows DNS. For more details, see Section 13.2.3, "Configuring a Domain Controller by Using an Existing DNS Server," on page 171.
- DSfW cannot be configured with an existing Windows DNS. However, an existing DSfW DNS server can be migrated to a Windows DNS server. For details, see Setting Up a Windows DNS Server for DSfW

13.2 Understanding DNS Settings in the DSfW Environment

This section explains the configuration changes that happen while DNS is configured for DSfW.

- Section 13.2.1, "General DNS Settings," on page 170
- Section 13.2.2, "Configuring a Domain Controller as a Primary DNS Server," on page 171
- Section 13.2.3, "Configuring a Domain Controller by Using an Existing DNS Server," on page 171

13.2.1 General DNS Settings

The DSfW installation page requires details on the following objects:

- Context of the DNS-DHCP Locator object
- Context of the DNS-DHCP Group object
- Context of the RootServerInfo object

DNS-DHCP Locator Object: The DNS-DHCP Locator object contains global defaults, DNS options, and a list of DNS servers and zones in the tree. The iManager and Java Management Console use the Locator object to locate the object instead of searching the entire tree to display these objects.

DNSDHCP Group Object: The DNSDHCP-Group object is a standard eDirectory group object. The DNS servers gain access to the DNS data within the tree through the DNSDHCP-Group object.

RootServerInfo Object: The RootServInfo object is a container object that contains resource records for the DNS root servers. The resource record sets contain Name Server(NS)records and Address (A) records of name servers that provide pointers for DNS queries to the root servers.

In addition to these objects, the following objects are required for DSfW:

- DNS Server Object
- DNS Zone Object
- DNS Resource Record Set Object
- DNS Resource Records

Only one copy of these objects exists in the DSfW tree. The DNS servers, DHCP servers, iManager, and the Microsoft Management Console must have access to these objects.

13.2.2 Configuring a Domain Controller as a Primary DNS Server

For a non-name-mapped setup, the contexts of the Locator object, RootServerInfo object, and the DNS-DHCP group object is automatically populated as the NCP server object location in the YaST page. By default, this context is `ou=OESSystemObjects,<DomainDN>`.

For a name-mapped setup, the fields are blank and the user can enter any context in the tree.

For an subsequent domain controller configuration, the Locator and Group contexts are retrieved from the existing DNS server. This is also useful for administrators who might not want to configure many DNS services in a network.

The default refresh interval of the DNS server is 15 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.

A DNS administrator object must be created for DNS server configuration. Provide the name and the location of the DNS administrator object. This information is required only if you configure this server as a primary DNS server. For a forest root domain installation, the DNS is configured by default in first domain controller, so this information is required for DNS configuration.

While configuring first domain controller in any subsequent domain (except a forest root domain), the `/etc/resolv.conf` file must point to the existing DNS server. This is required to perform lookups during configuration. Later if you choose this server to be configured as a primary DNS server, the DNS configured on this server and the `/etc/resolv.conf` file gets automatically updated during provisioning and points to the local DNS server.

For information on installing and configuring Novell DNS services, see "Installing and Configuring DNS" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide OES 2 SP3: Novell DNS/DHCP Administration Guide*

13.2.3 Configuring a Domain Controller by Using an Existing DNS Server

When the first domain controller in a domain is using an existing DNS server, YaST provides an option to retrieve these values from the existing DNS server. During installation through YaST, you can retrieve these values by selecting *Retrieve DNS entries*, and then selecting *Retrieve.*

NOTE: If you are configuring an subsequent domain controller for a domain that is already configured to host a DNS server, make sure your first entry in the `/etc/resolv.conf` file is pointing to the DNS server that the first domain controller is using.

13.3 Setting Up a Windows DNS Server for DSfW

Although it is possible to migrate DSfW DNS to a Windows DNS server, the migrated DNS records cannot be integrated with Active Directory. Use the following procedure to migrate DSfW DNS server to a Windows DNS server.

1 Using MMC, add secondary zones for all the existing forward and reverse lookup zones hosted in the DSfW DNS server.

   Windows DNS does a zone transfer of the newly created zones from the DSfW server.

2 Using iManager or the DNS/DHCP Management Console, configure the servers that were designated as primary servers to be secondary servers.

3 In the first domain controller, edit the `/etc/resolv.conf` file and change the IP address to the server where the Windows DNS Server is running

4 Restart Novell DNS server for the changes to take effect by using the `rc-novell-named restart` command.

13.4 Migrating DNS to Another Domain Controller

In a typical DSfW deployment, beginning OES2 SP3, any domain controller can be configured as a DNS server. If the domain controller serving as primary DNS server does not function due to a hardware or software fault, the other domain controllers need at least one DNS server to keep the domain services intact.

IMPORTANT: The DNS migration can happen even when the source DNS server is down. If the DNS server is down, make sure that any of the subsequent domain controllers in the forest have the replica of the Tree Root partition. This is necessary to perform Step 2.

When the first domain controller goes down, make sure that the configuration partition and schema partition replica is there on at least one domain controller in the domain. This is required to keep the functioning of DSfW intact.

To migrate the DNS server from the first domain controller, from the subsequent domain controller execute the following steps:

1 Using the `CASAcli` client utility, set the CASA credentials on the subsequent 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`

2 Using iManager, execute the following steps:

2a Click *DNS>DNS Server Management>Create Server* option.

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

2b Click *DNS>DNS Server Management>View/Modify Zone* option.

2b1 Select the DNS zone from the list. Click *OK*.

2b2 Associate the zone with the DNS server. For details on associating zone with a DNS server, see "Zone Management" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*

3 Restart novell-named on the subsequent domain controller using the following command:

`rcnovell-named restart`

After migrating the DNS server to the destination domain controller, the DNS entry referencing the first domain controller is still retained in the cache for some time. This does not affect the functionality in any way as when a name resolution request is issued, it gets resolved by the DNS server on the other domain controller, if the first domain controller has not responded.

IMPORTANT: If you have changed any DNS records or the configuration file, the changes are effected after the dynamic reconfiguration interval of DNS. The default value of this interval is 15 minutes. If the changes are not done, we recommend you to restart the DNS server using the `rcnovell-named restart` command.

13.5 Restarting DNS

If you have changed any DNS records or have changed the DNS configuration file, you need to restart the DNS server so that the changes take effect.

To restart the DNS server, use the following command:

```
rcnovell-named restart
```

For information on updating records, refer to "Understanding DNS and DHCP Services" in the *OES 2 SP3: Novell DNS/DHCP Administration Guide*

14 Managing Group Policy Settings

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 a DSfW domain is provisioned, a single group policy called 'Default Domain Policy' is created. Along with many workstation specific policies, the Group Policy Object also contains the Kerberos, Account Lockout and Password related policies under the 'Account Policies' section.

You must be a member of the Domain Admins group to edit an Active Directory Group Policy for a domain. For troubleshooting information pertaining to group policy management, see Section 19.5, "Group Policy Management Issues," on page 246.

- Section 14.1, "Configuring Group Policies," on page 175
- Section 14.2, "Group Policy Objects," on page 178
- Section 14.3, "Sysvol," on page 180

14.1 Configuring Group Policies

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.

To Configure a new Group Policy

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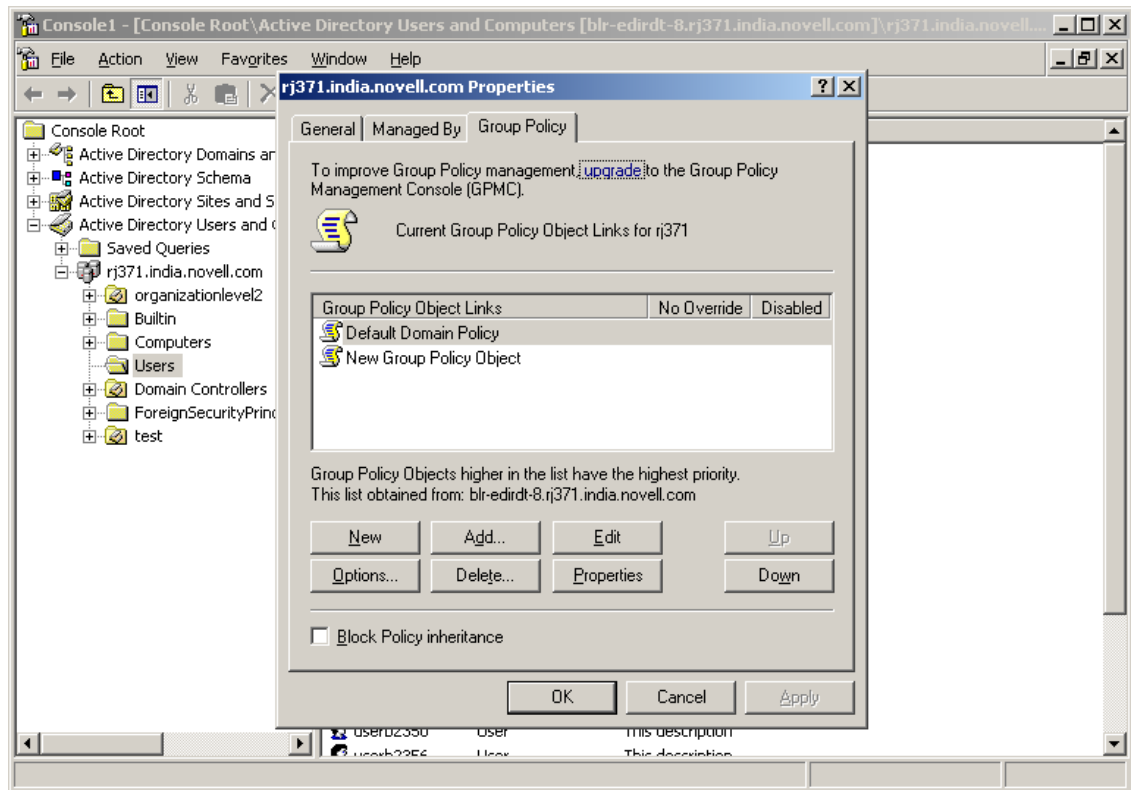
4 Specify a name for the new Group Policy, then click OK.

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.

These additional Group Policies can be associated to a Organization Unit under the domain.

Editing an Existing Group Policy

To modify Group Policy settings within Group Policy objects (GPOs), you can use the Group Policy Object Editor which is a Microsoft Management Console (MMC) snap-in used for configuring and modifying Group Policy settings. It operates as an extension to Group Policy Management Console (GPMC).

If GPMC is not available, you can use the Active Directory Users and Computers snap-in or the Active Directory Sites and Services snap-in.

To edit and existing group policy, follow the instructions in How To Use the Group Policy Editor to Manage Local Computer Policy (http://support.microsoft.com/kb/307882)

NOTE: If you are not able to edit the Group Policy, it is because the DFS cache is pointing to a server that is not holding the PDC Emulator role. To set the DFS link to point to the server holding the PDC Emulator role, execute the steps in Setting the DFS Referral of the Server Holding the PDC Emulator Role as Active on the Workstation.

Setting the DFS Referral of the Server Holding the PDC Emulator Role as Active on the Workstation

To set the DFS link of the server holding the PDC Emulator role as active, execute the following procedure:

1 Browse to the SYSVOL folder by typing \\domain.tld\sysvol\ or \\ *ipadress*\sysvol in the file explorer. Select the domain.tld folder.

2 Right click the domain.tld folder to view the properties. Click the *DFS* tab. It will list two referrals.

3 Select the link of the server holding the PDC Emulator role and set it as active.

This procedure of settings the DFS referral can be used even if there are multiple domain controllers in a domain. However, while setting the DFS referral, you must ensure that you do not specify the fully qualified domain name of the domain controller in the file explorer to browse the SYSVOL folder. For instance, for a domain named dsfw.com that has multiple domain controllers nmfadc.dsfw.com and nmfrd.dsfw.com, you must specify \\dsfw.com\sysvol in the file explorer for setting the DFS referral as shown in the figure below.
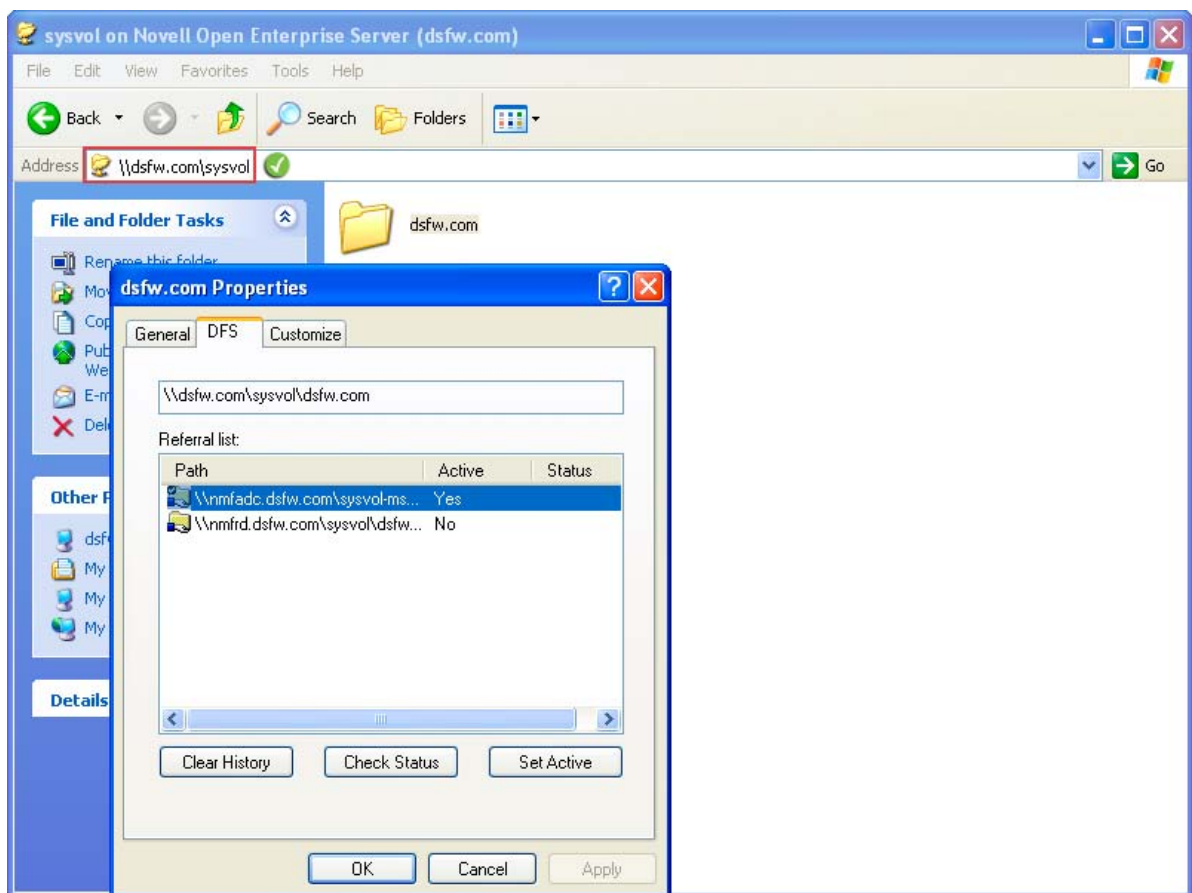
You must not specify the fully qualified domain name of the domain controller in the file explorer as shown in the following figure.
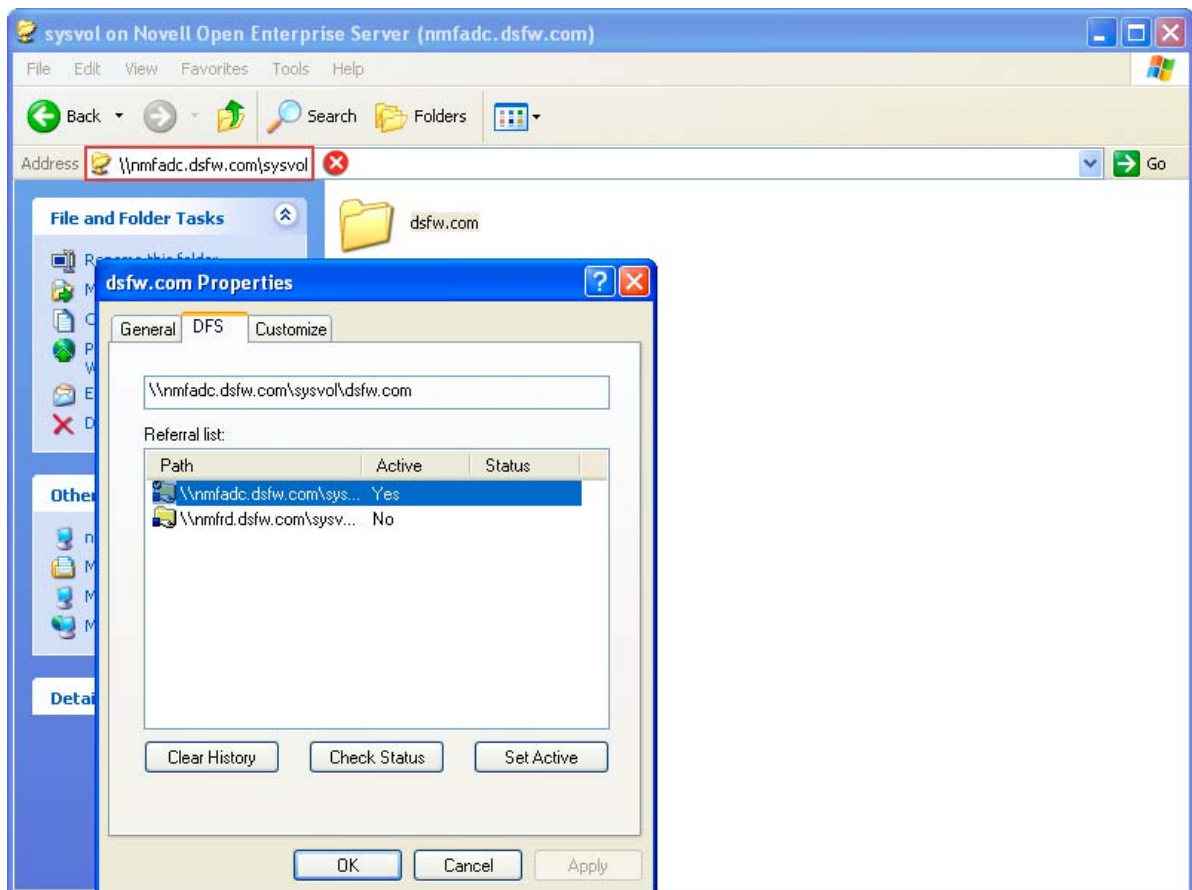
For more information about Group Policy Object settings, refer to Microsoft's online Group Policy documentation (http://technet2.microsoft.com/WindowsServer/en/library/abc2890d-f3f1-408c-bafc-ac9e4e5b0e831033.mspx?mfr=true). For more information about NMAS and Universal Password settings, refer to the Novell eDirectory documentation (http://www.novell.com/documentation/edir88/).

14.2 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.

14.2.1 GPO Account Policies

The group of security settings in the GPO is called Account Policies and 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 the Samba server.

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>.

The Password Policy and the Account Lockout Policy are enforced by eDirectory. The Account Policies settings are not read directly by eDirectory or KDC.

The Kerberos Policy is enforced by the Kerberos Key Distribution Center (KDC). The eDirectory server enforces only those policies that are stored in its Directory Information Base (DIB). The Kerberos KDC expects the Kerberos Policy to be stored in eDirectory.

The 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

14.2.2 gpo2nmas

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.

14.2.3 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.

14.2.4 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 returns the information for the local users and the domain users.

  If you are using the `getent` utility in the DSfW environment, substitute the *username* with the domain user name.

- Check the Samba log files in `/var/log/samba` for any errors.

14.3 Sysvol

The System Volume (Sysvol) is a shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain. The 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.

Beginning OES 2 SP2, the SYSVOL volume of a domain is now stored on each domain controller of the domain. This enhancement resolves the performance and scalability limitations arising from the initial design of having the SYSVOL volume only on the first domain controller.

Following are the benefits of having the SYSVOL volume on every domain controller:

- Reduces the load on each domain controller as now during user login or workstation bootup, policies can be read from any domain controller as each domain controller holds a copy of SYSVOL.
- Provides fault tolerance in form of backup domain controllers providing seamless transition from the first domain controller, in event of failure.

The synchronization of data between the domain controllers is handled by sysvolsync utility. During the DSfW installation a crontab entry is added for sysvolsync that synchronizes the changes on the domain controller playing the role of a PDC emulator with the other domain controllers in the domain. The synchronization by default happens every half an hour.For more details on the sysvolsync utility see, Section 14.3.1, "sysvolsync Utility," on page 181

14.3.1   sysvolsync Utility

The sysvolsync utility is introduced to provide synchronization of sysvol and the underlying policies between the domain controllers of a domain.

This utility when invoked finds the domain controllers for the domain and initiates the synchronization process with them, contacting one domain controller at a time.During the synchronization only the changes are transferred and not the entire data. This helps in faster synchronization between the domain controllers. All the POSIX file permissions and ACLs are retained during transfer.

For intermediate synchronization, you can invoke the utility using the following command:

/opt/novell/xad/sbin/sysvolsync

During the synchronization the changes are transferred from the first domain controller(holding the PDC Emulator role) to the other domain controllers.

The details of synchronization events are captured in /var/opt/novell/xad/log/sysvolsync.log file.

15 Managing Trust Relationships in Domain Services for Windows

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

15.1 What is a Trust?

A trust is used to allow users of one domain to access resources from another domain. By default, two-way, transitive trusts are automatically created when a new domain is 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 cross-forest trusts:

- **External Trusts:** These trusts are non-transitive 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 non-transitive 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) and New Trust Wizard Pages (http://technet.microsoft.com/en-us/library/cc784531.aspx) for more information on trusts.

15.2 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.

- Section 15.2.1, "Creating a Cross-forest Trust between Active Directory and Domain Services for Windows Forests," on page 184
- Section 15.2.2, "Shortcut Trusts," on page 215

15.2.1 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 185
- "Configuring the Reverse Lookup Zone Forwarder" on page 195
- "Configuring the DNS Forward Lookup Zone on the Active Directory Server" on page 205
- "Creating the Trust" on page 208
- "Verifying the Trust" on page 215

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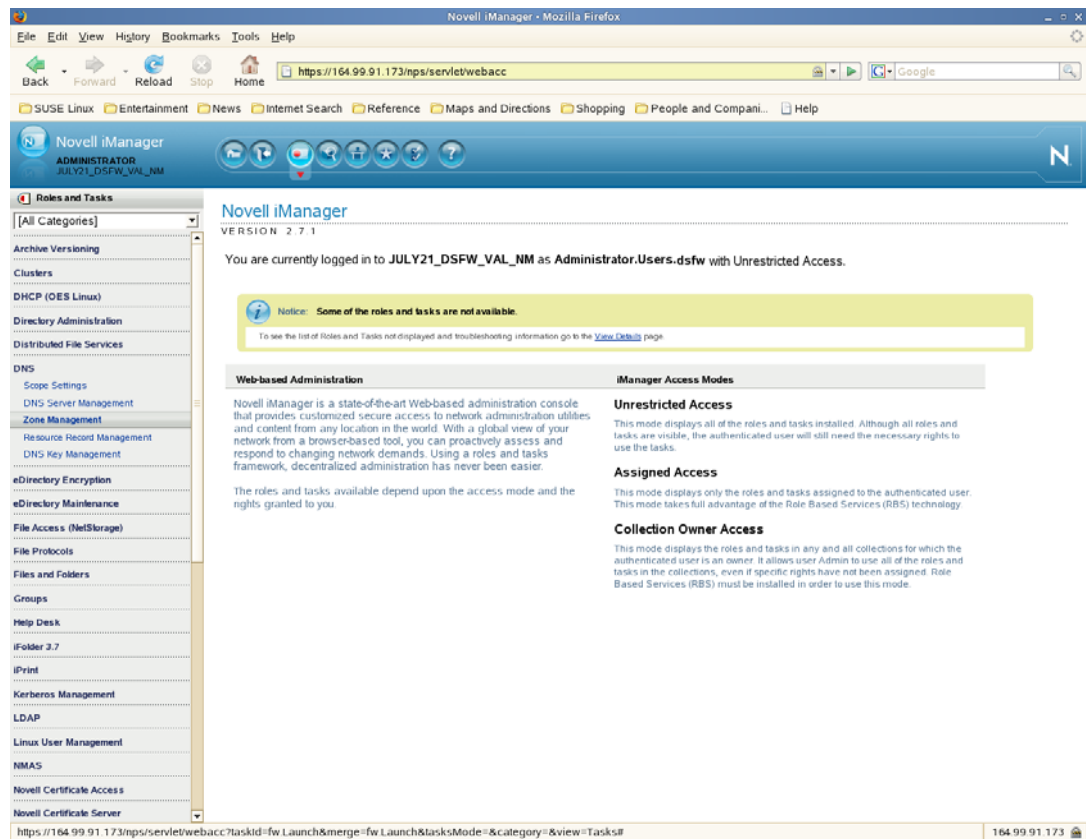
1b Click DNS > *Zone Management* to open the Zone Management window in the main panel.

2 From the drop-down list select *Create Zone,* then click *OK* to open the Create DNS Zone window.
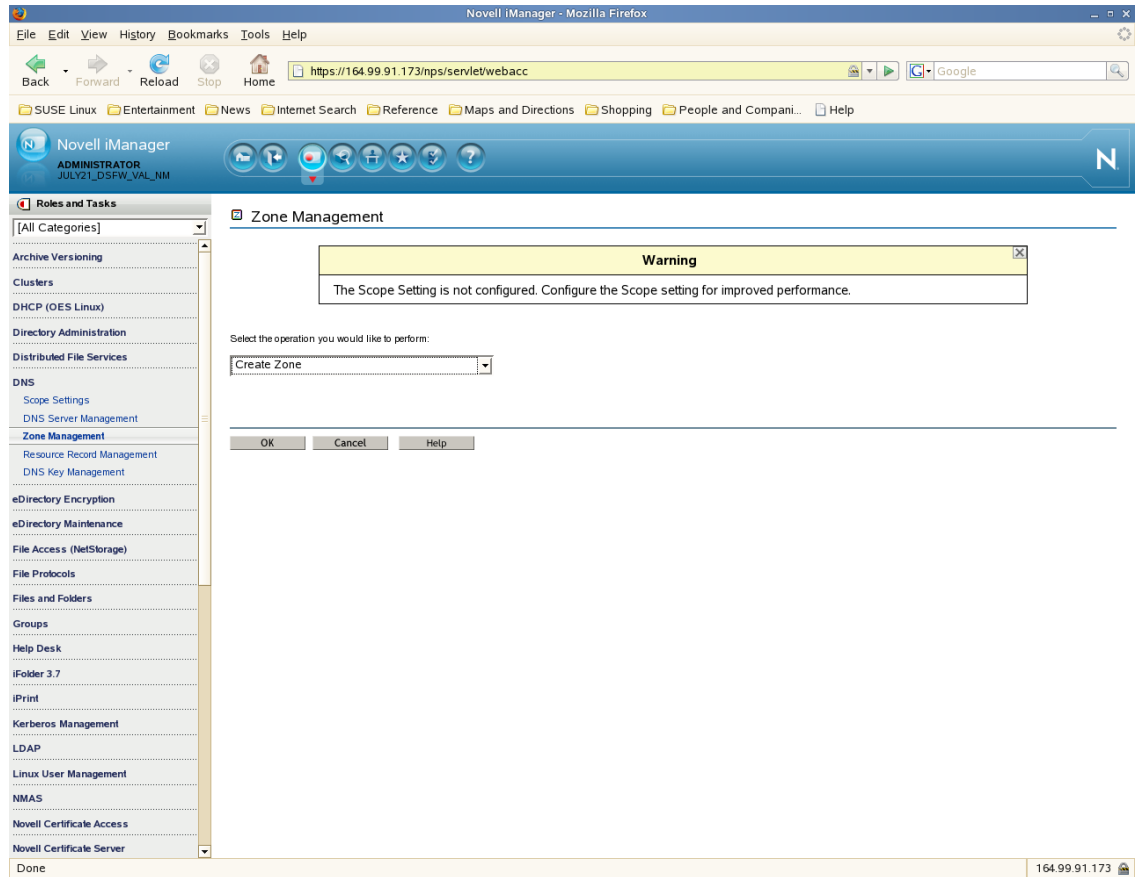
3 Select *Create New Zone* and specify the DNS configuration parameters as follows:
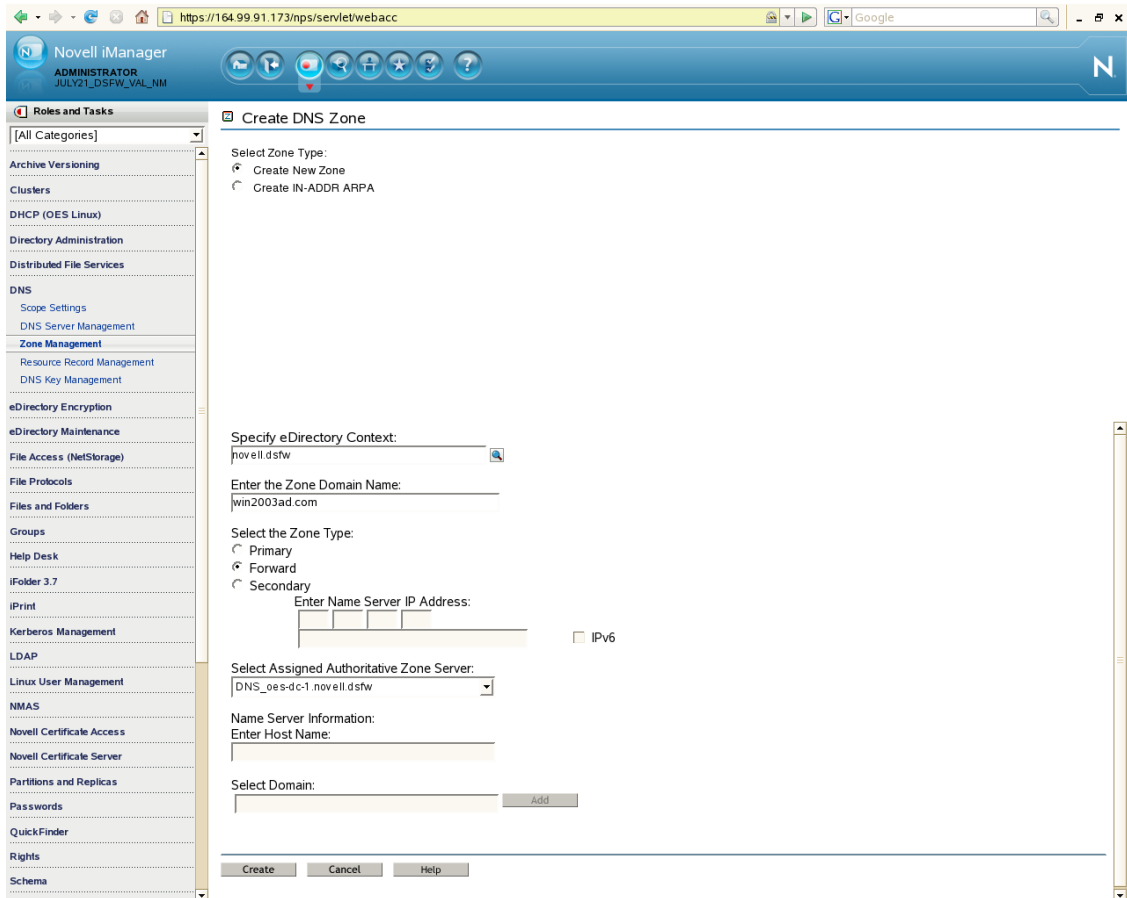
3a Specify the eDirectory context for the zone or browse to select it; that is, the container containing the DNS related objects (In this example, it is `OESSystemObjects.dsfw`).

3b Specify a name for the zone; that is, the domain name of the Active Directory forest (in this example, it is `win2003ad.com`).

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.OESSystemObjects.dsfw`. This parameter is optional.

3e Click *Create.* A message indicates that the new forward zone has been created.
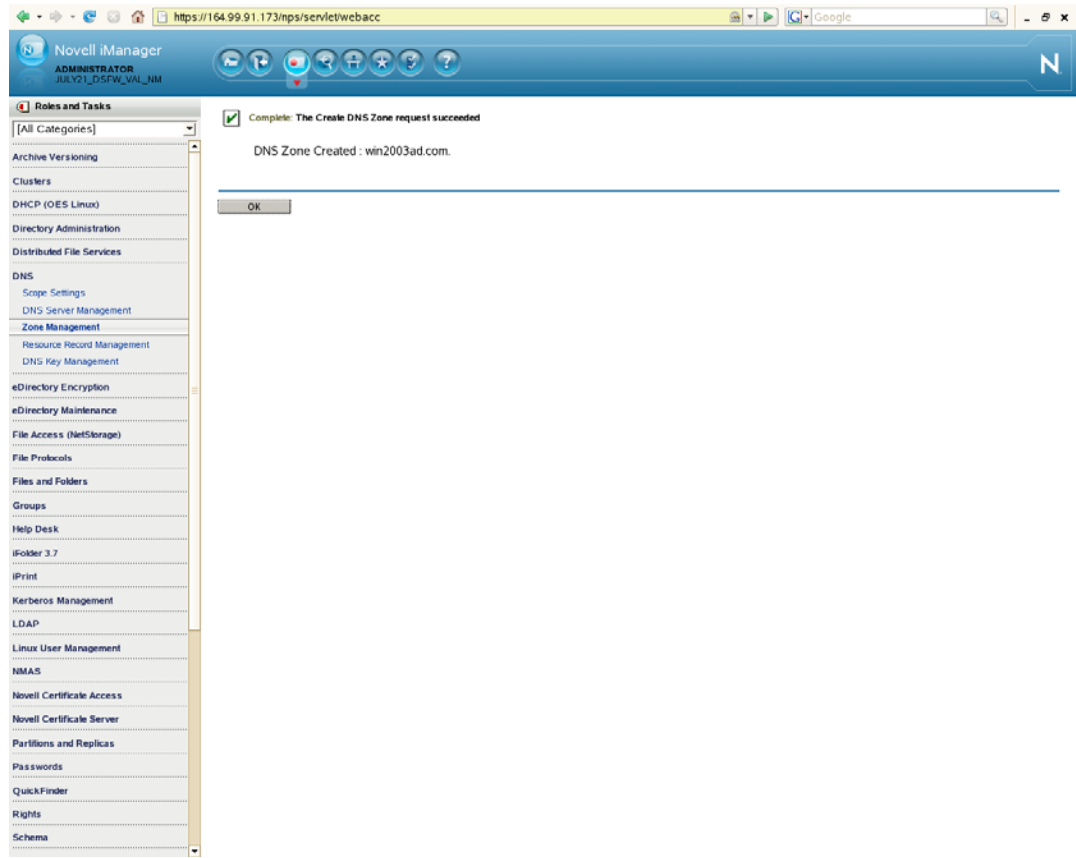
4 Select *Zone Management* from the iManager DNS plug-in, then select *View/Modify Zone* from the drop-down list and click *OK*.
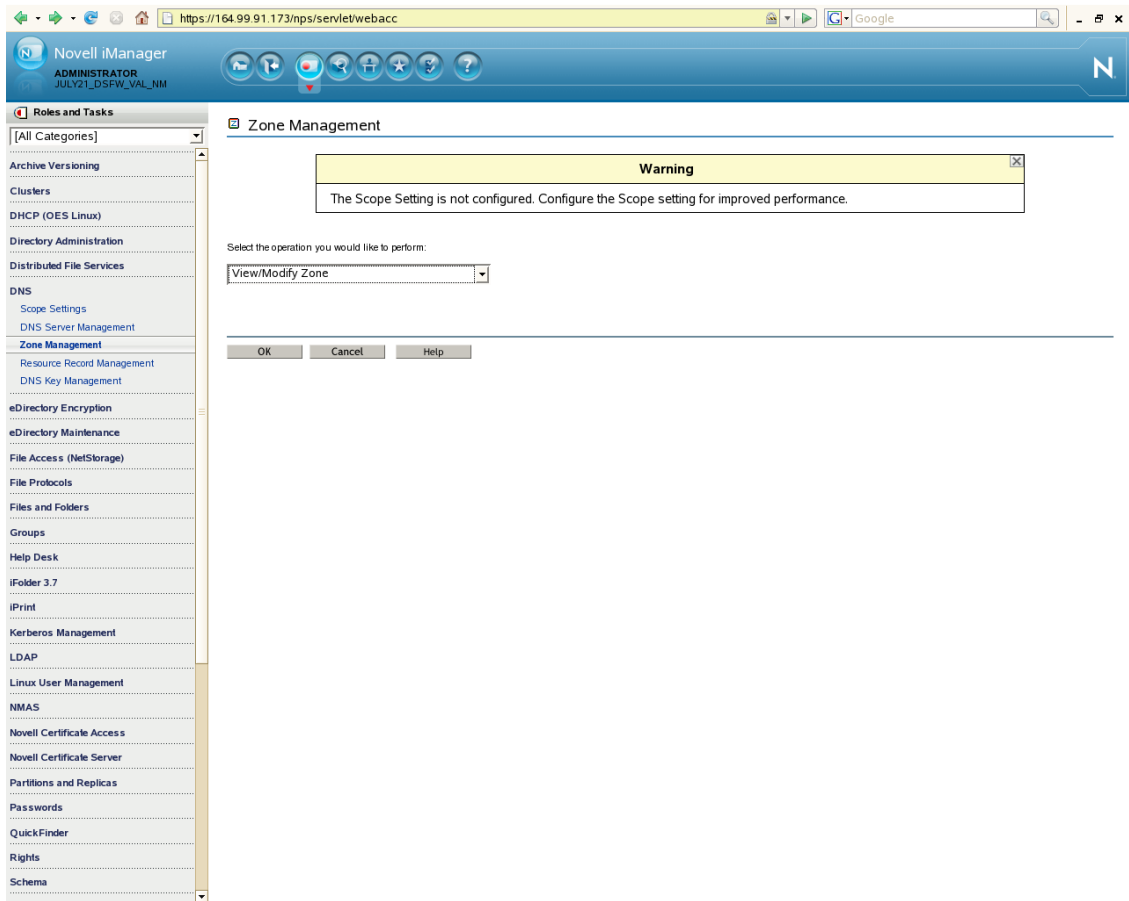
5 Select Active Directory forest's domain zone from the drop-down list, then click *OK*.

6 Click *Next*.

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*.
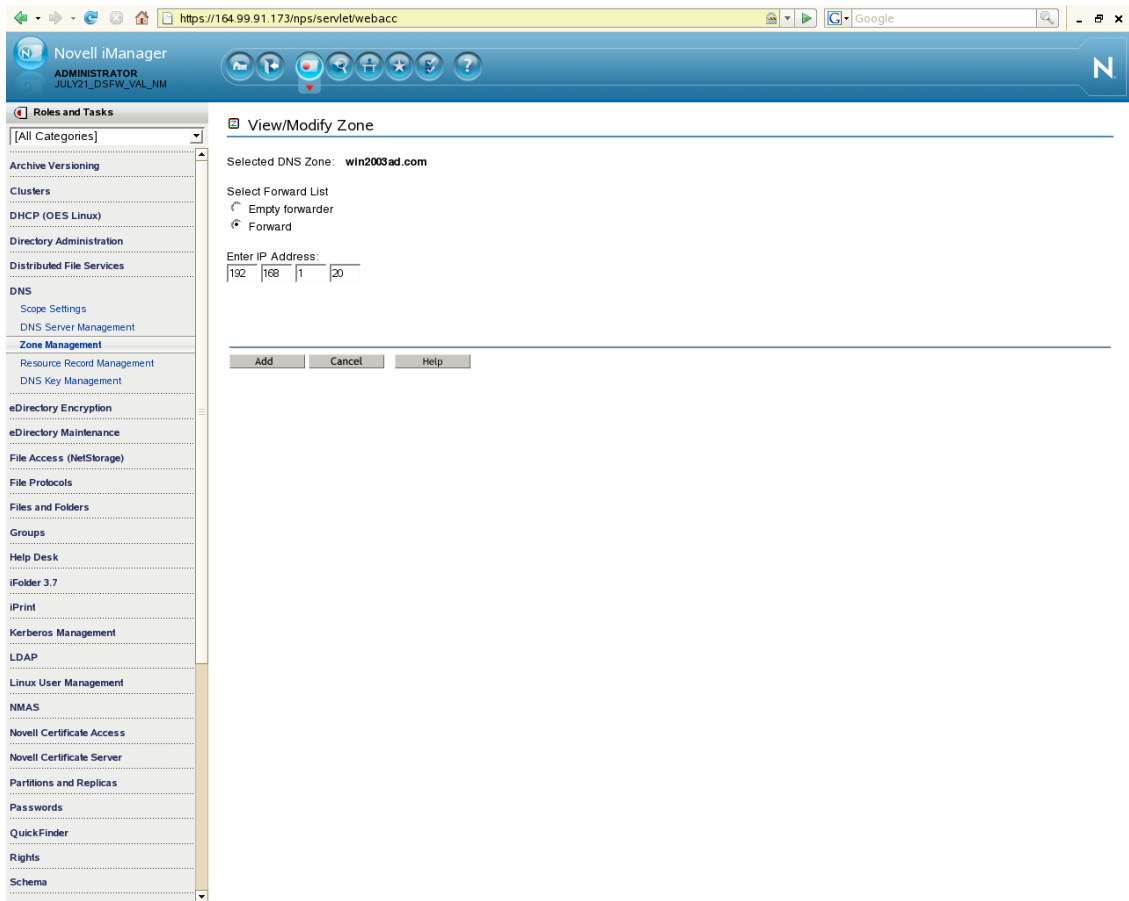
9 Click *Done*.
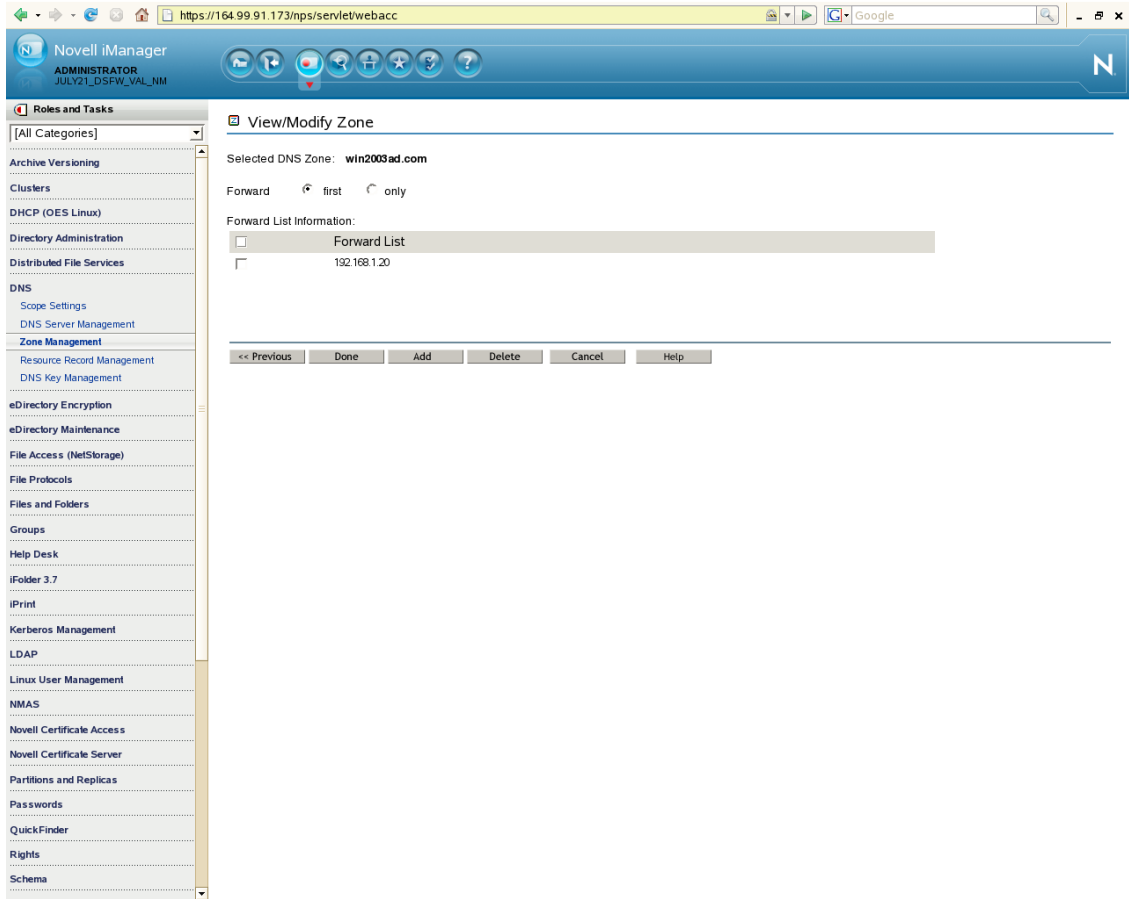
10 A message indicates that the new secondary zone has been created. Click *OK*.
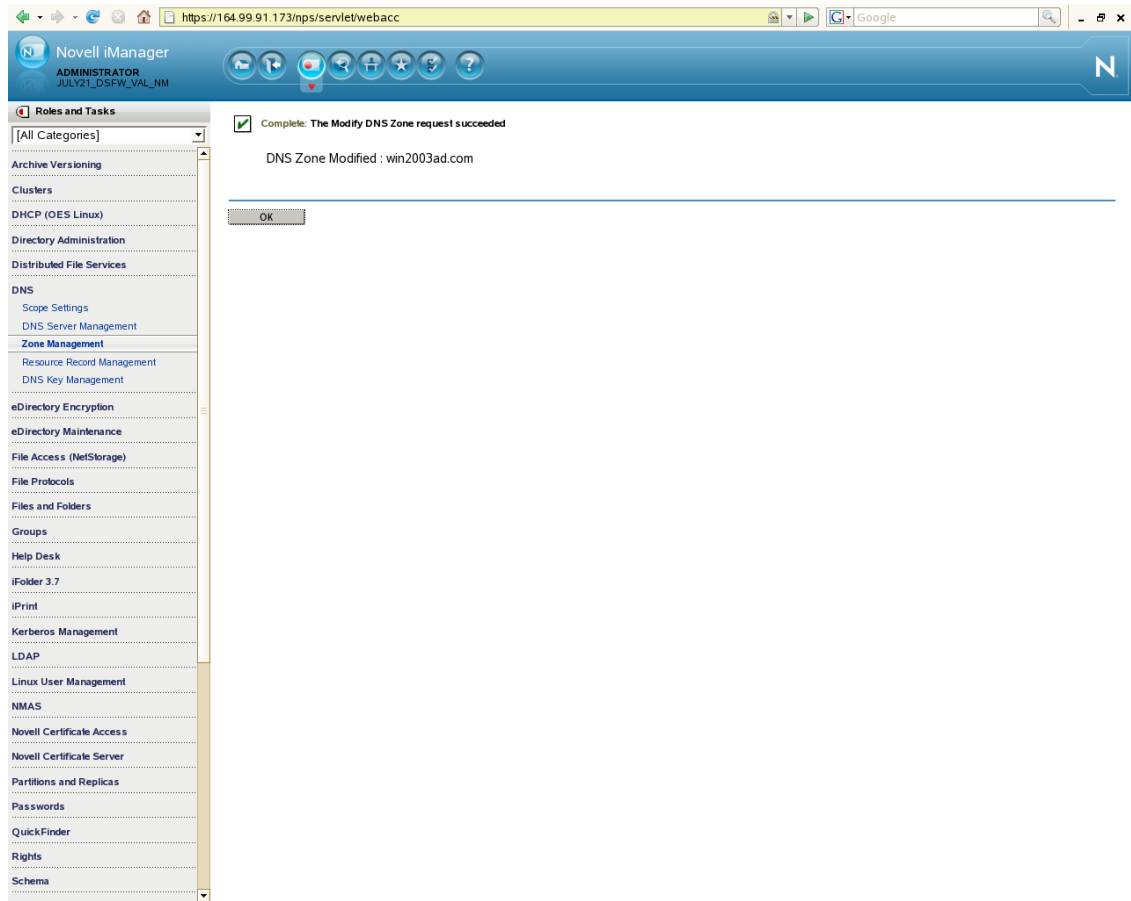
11 Restart DNS by using the `rcnovell-named start` command.

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.
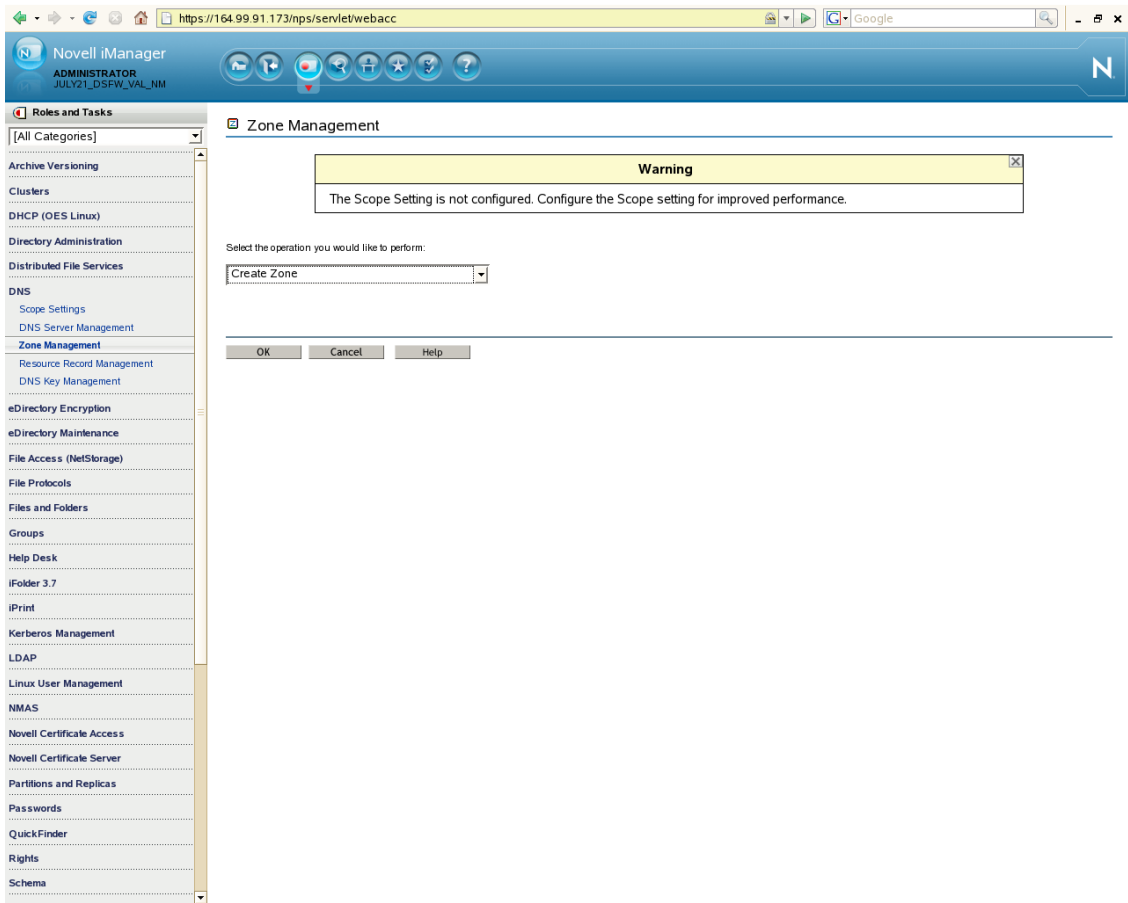
2 Specify the DNS configuration parameters as follows:
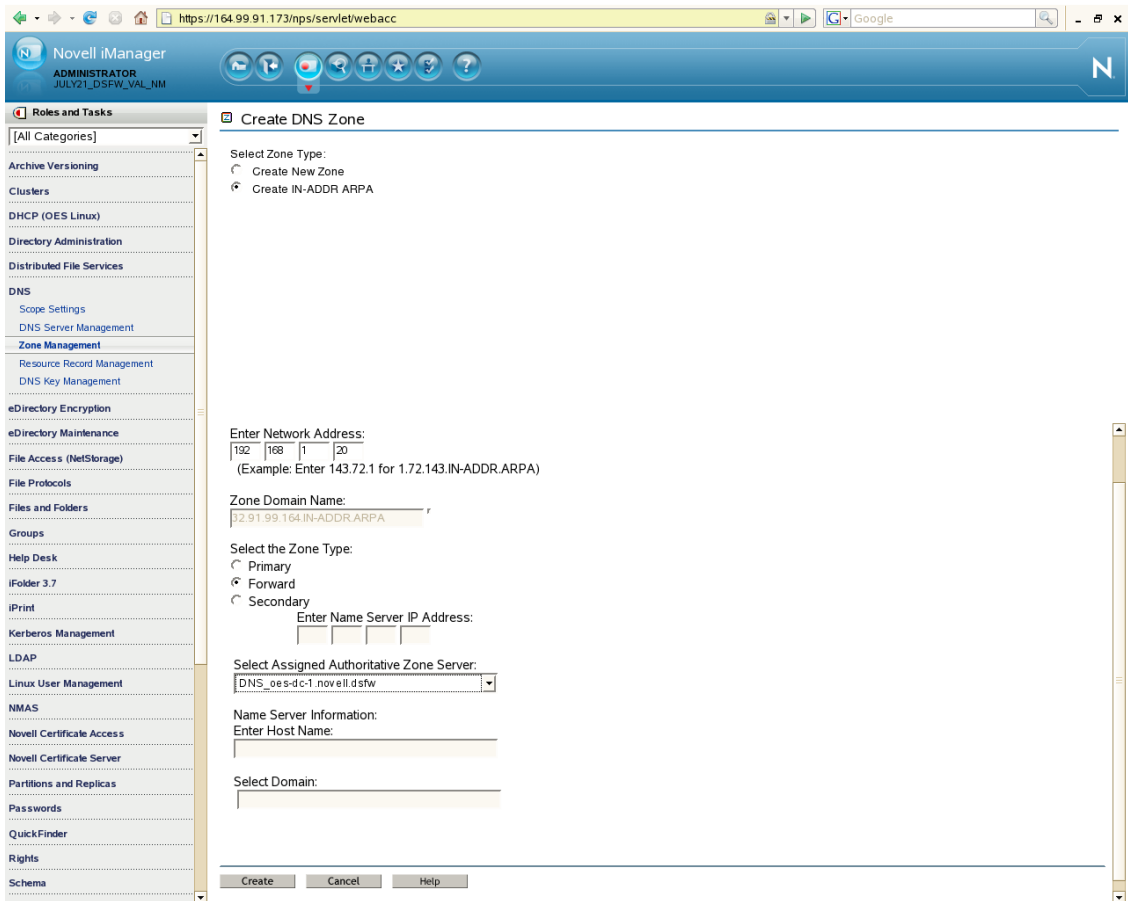
2a Select the Create IN-ADDR ARPA option as the *Zone Type*.

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.OESSystemObjects.dsfw`).

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*.
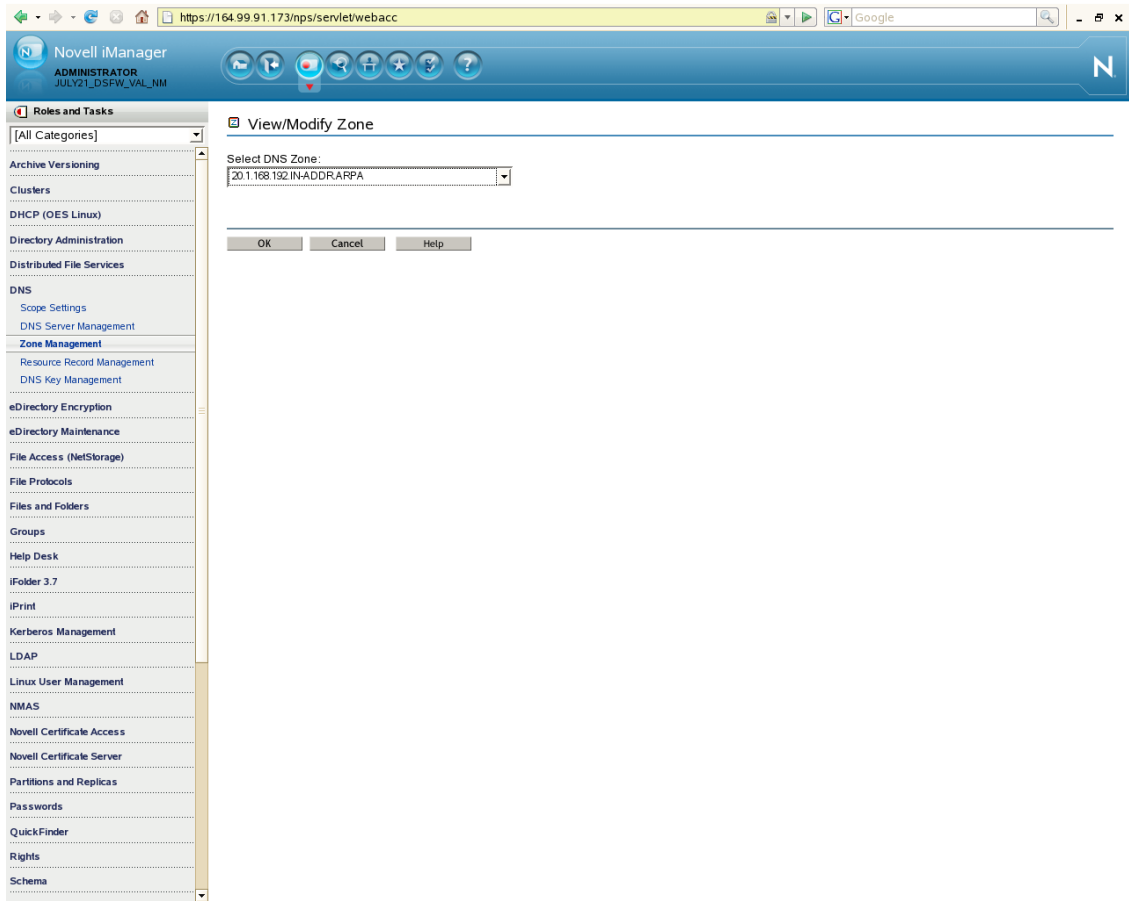
5 Click *Next*.
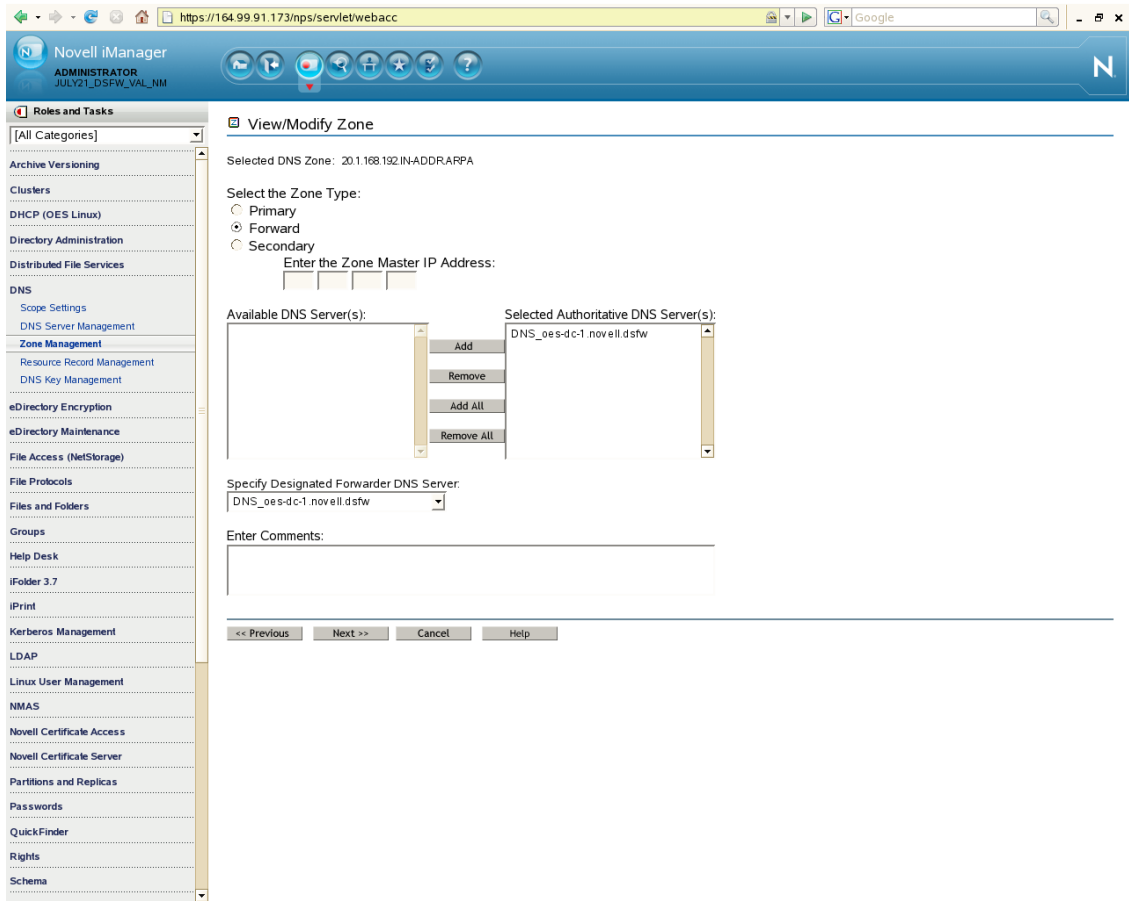
6 Click *Add* to add this DNS server object.
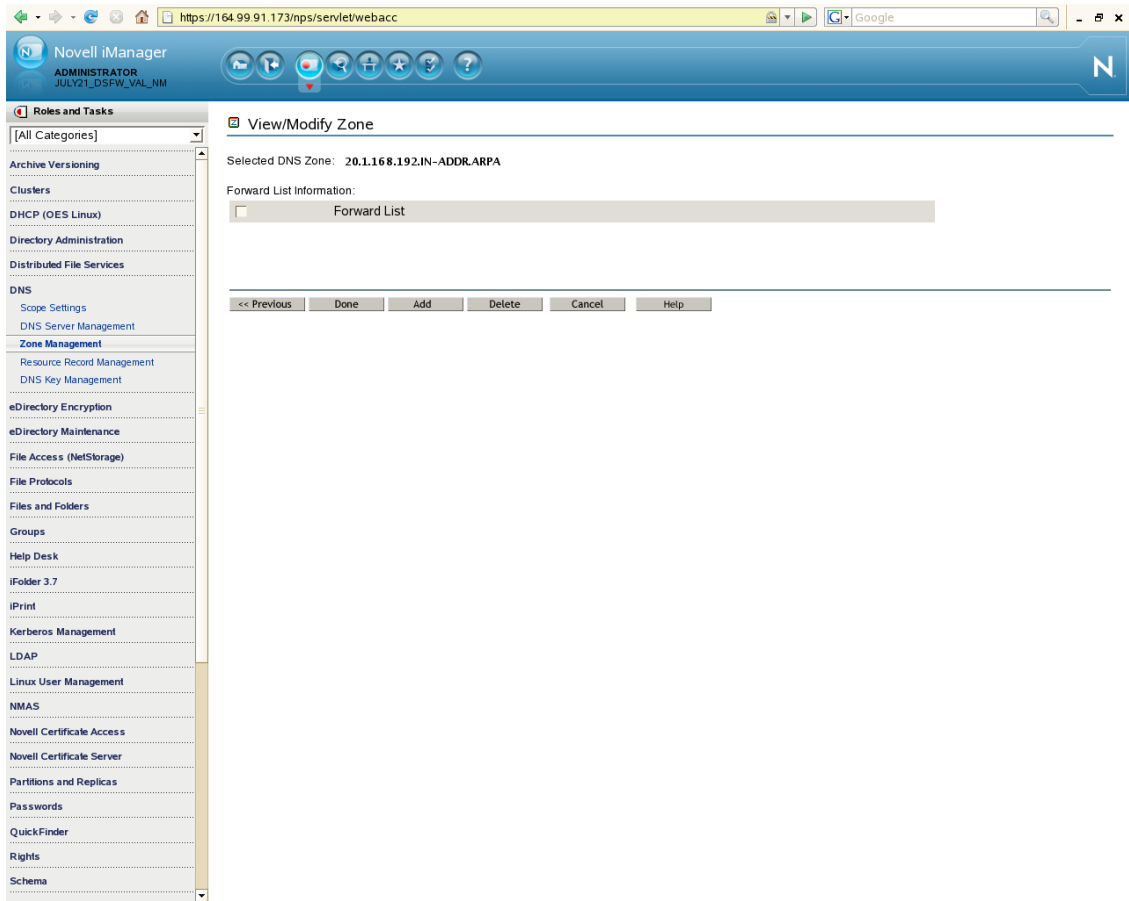
7 Select the *Forward* option and specify the IP address of Active Directory forest's DNS server (192.168.1.20 in this example). Click *Add*, then click *Done*.
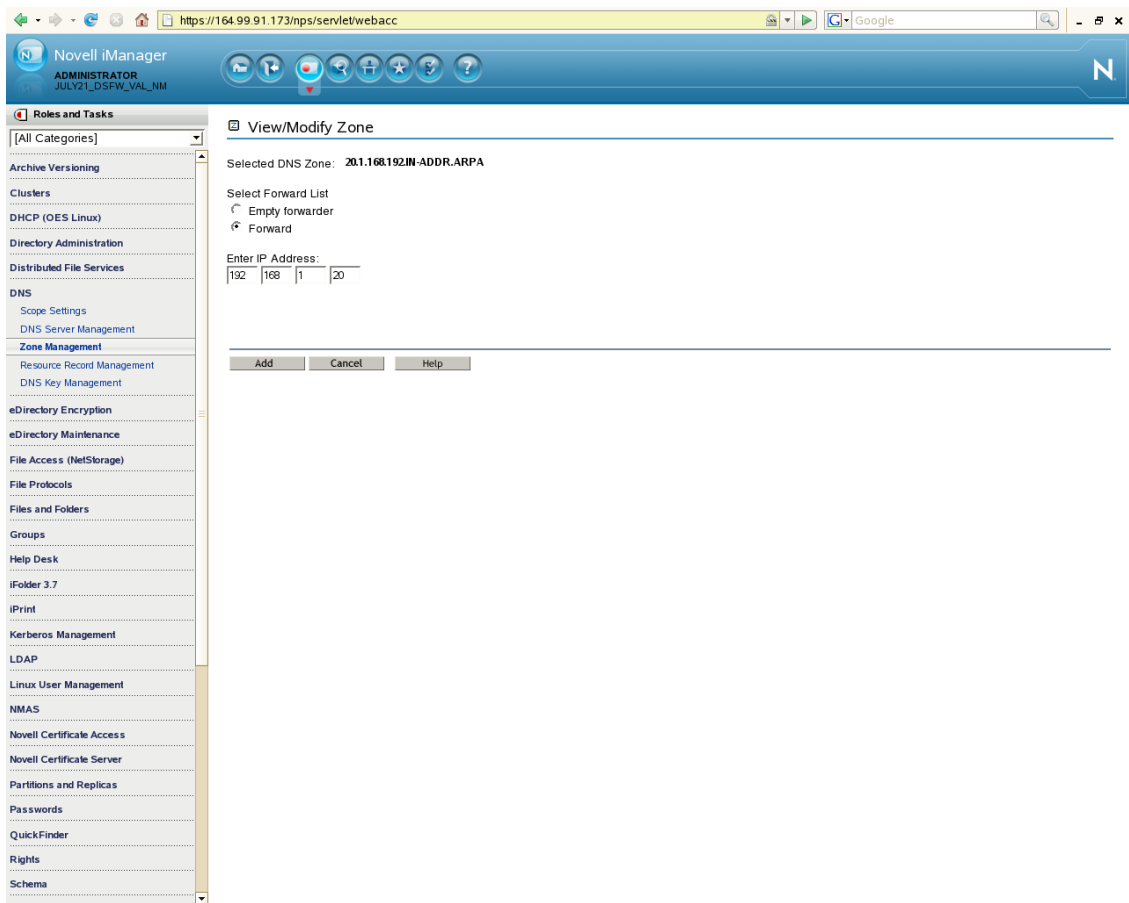
8 Select *Forward List* and click *Add.*
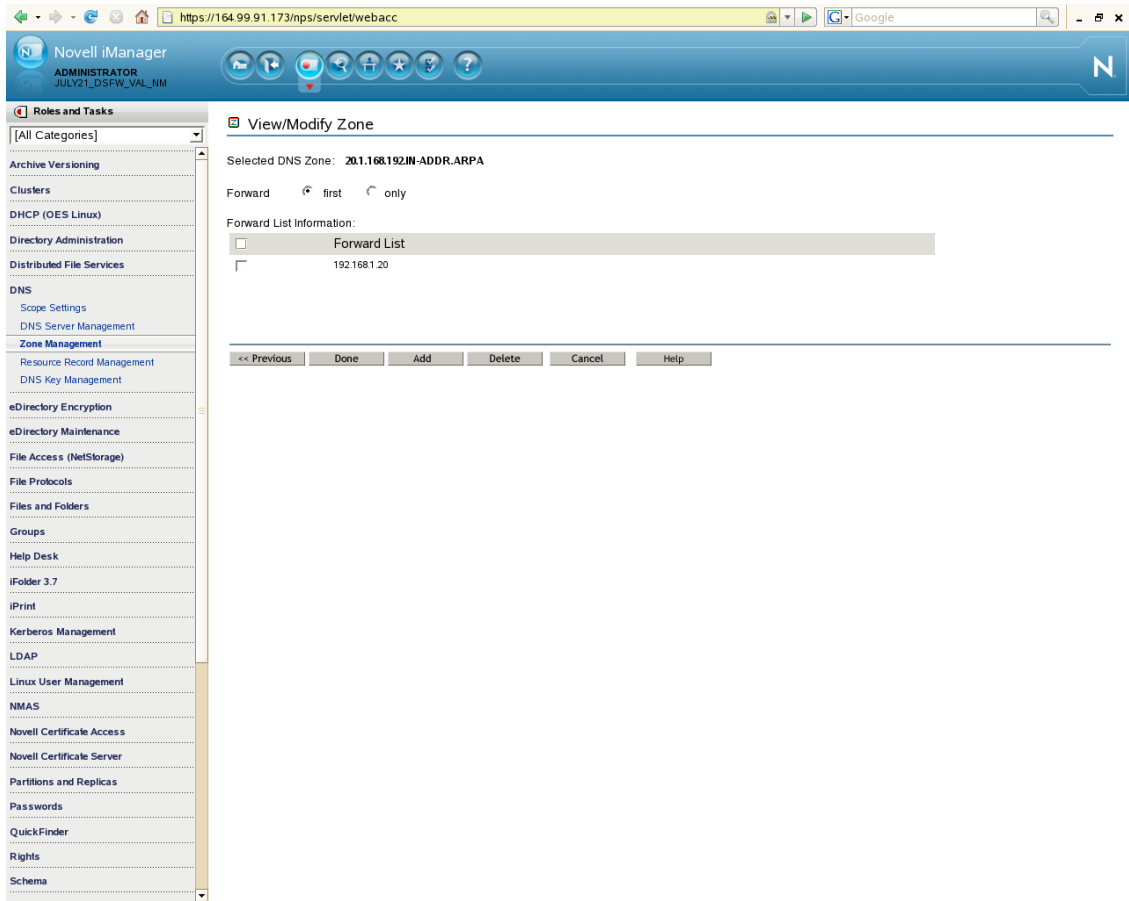
9 A message indicates that a zone has been created. Click *OK*.
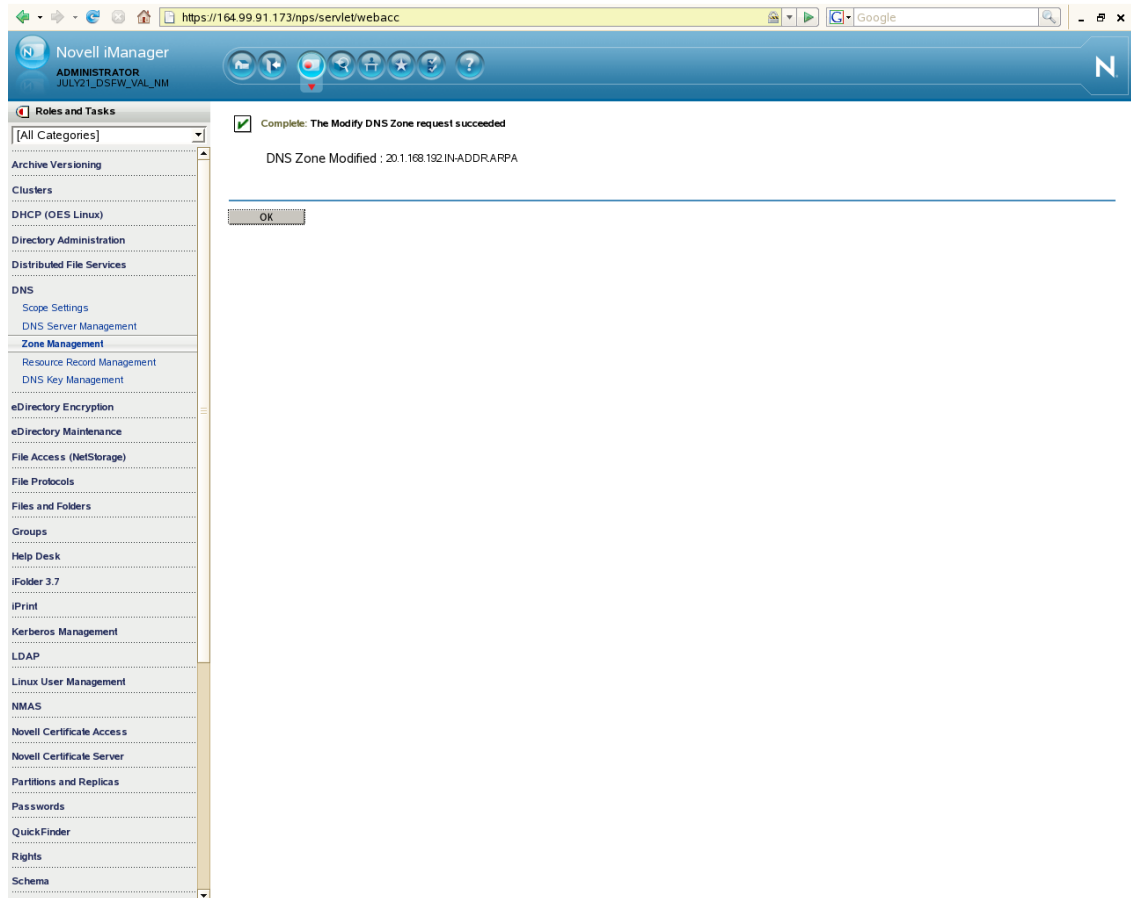
10 Verify the DNS configuration by trying to resolve the Active Directory domain and its DNS SRV records using `nslookup`, as follows:

`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.

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*.
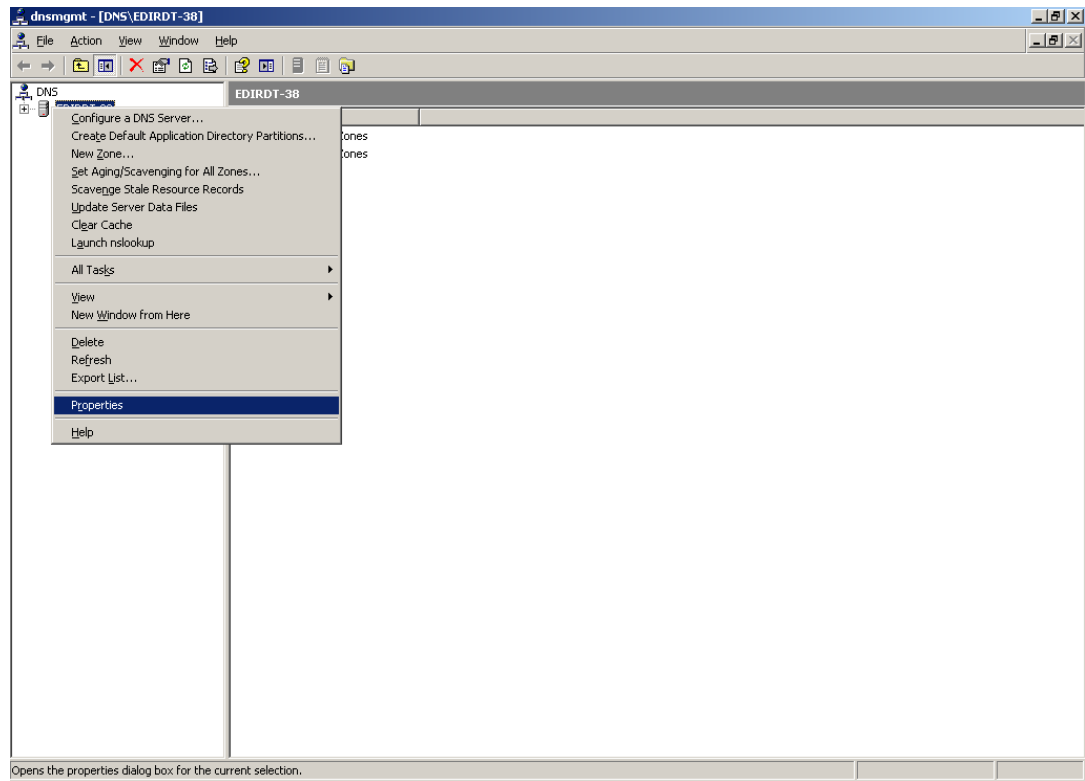
1b Select the *Forwarders* tab, then click *New* and add a new forwarder for the DSfW domain. Specify the DSfW domain name and click *OK*.
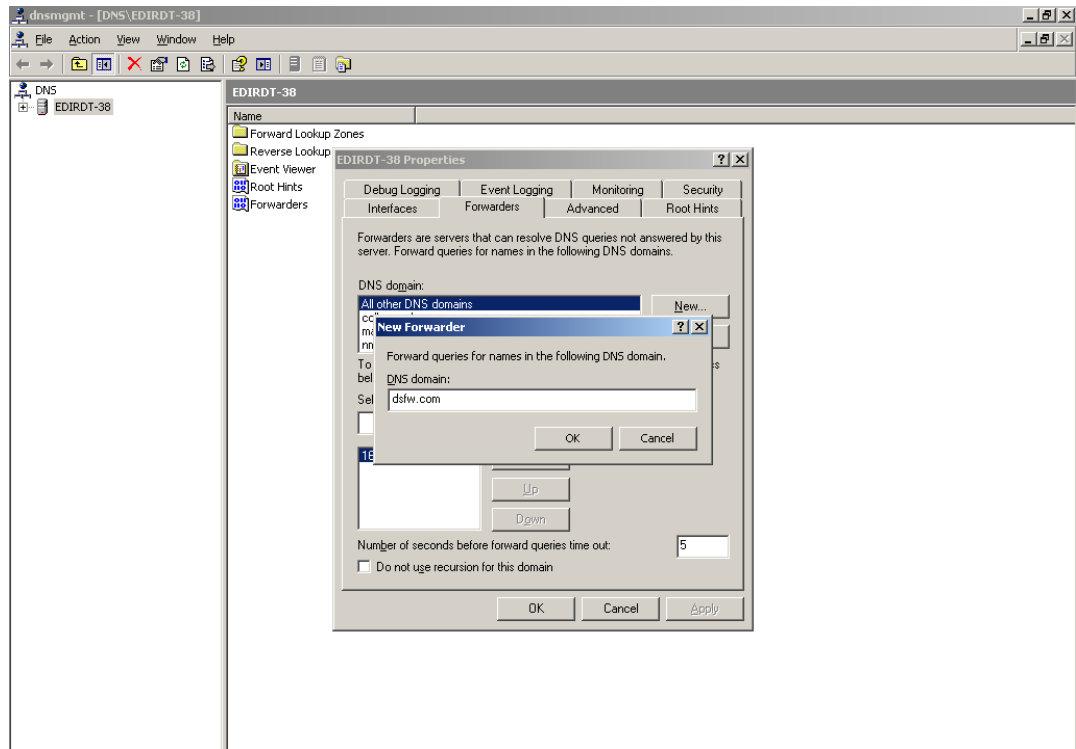
1c Select the new forwarder, specify the IP address of the DNS server of the DSfW domain, then click *Add*.
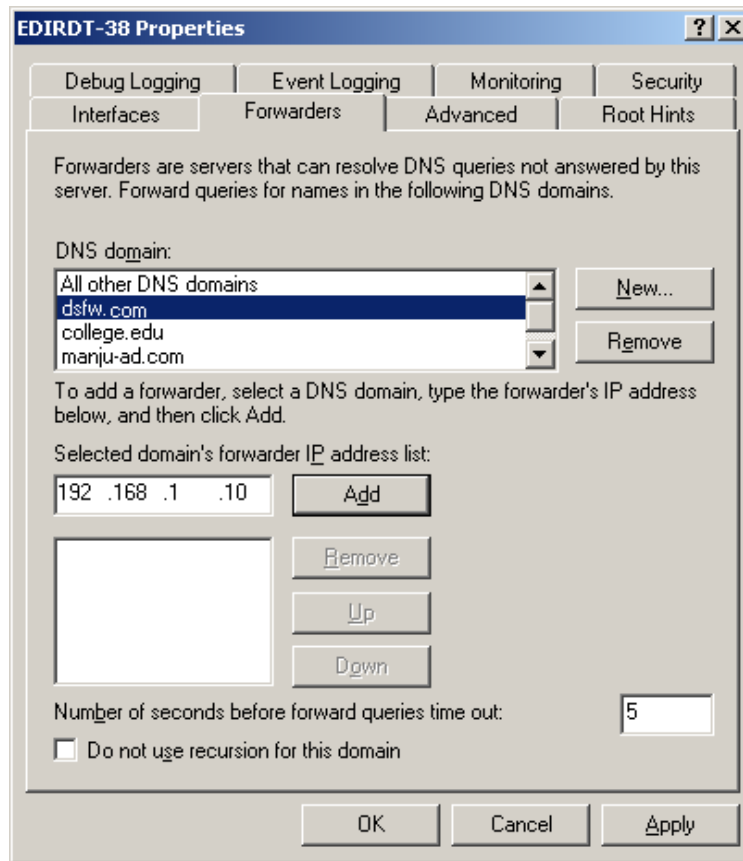
1d Verify the DNS configuration by using `nslookup` to resolve the Active Directory domain and its DNS SRV records, as follows:

```
nslookup -query=any _ldap._tcp.dc._msdcs.<DSfW domain name>
```
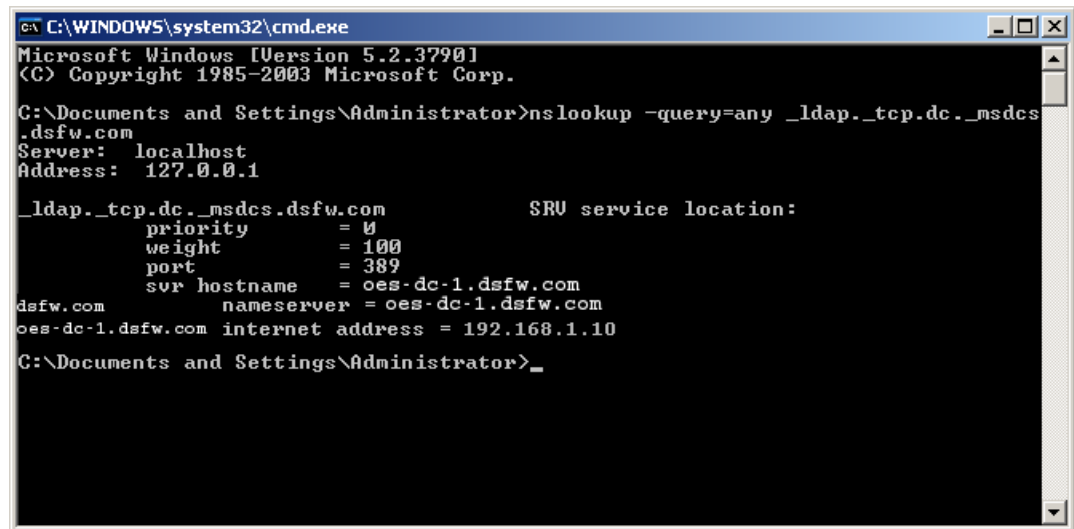
2 Right-click *Reverse Lookup Zones*, select *New Zone*.

    2a Select *Primary Zone*. Deselect the *Store the zone in Active Directory* option.

    2b Specify the Network IP and click *Finish*. The zone is now created.

    2c Right-click the newly created zone to create a PTR record and enter the required details.

3 If the Active Directory domain's Domain Functional Level is not Windows Server 2003, do the following to raise it:

    3a Open Active Directory Domains and Trusts snap-in from the MMC.

    3b Right-click the icon representing the Active Directory domain, select *Raise Domain Functional Leve*l from the menu, then set it to *Windows Server 2003*.

4 If the Active Directory forest's Forest Functional Level is not Windows Server 2003, do the following to raise it:

    4a Right-click the Active Directory Domains and Trusts snap-in from MMC.

    4b 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*.
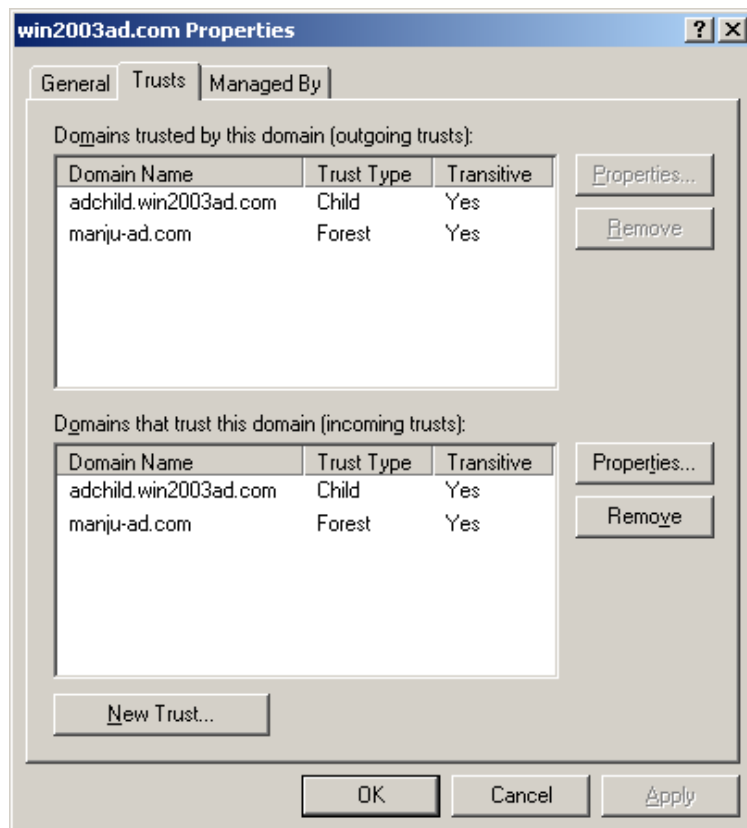
6 Click *Next* to start creating a new trust.

7 Specify the DNS name (or NetBIOS name) of the Active Directory forest, then click *Next*.
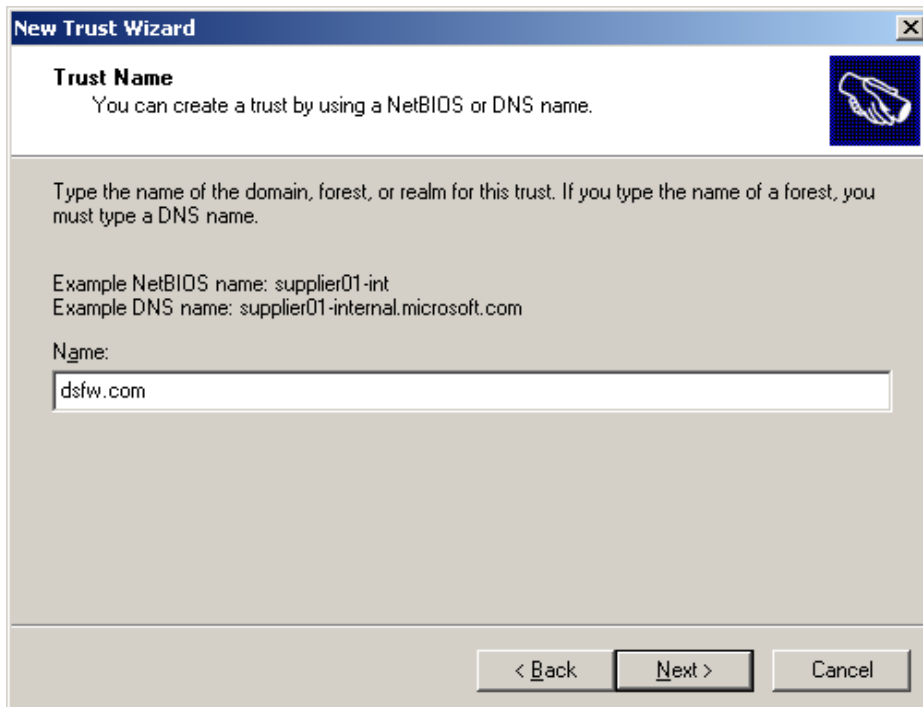
8 Select *Forest trust*, then click *Next*.
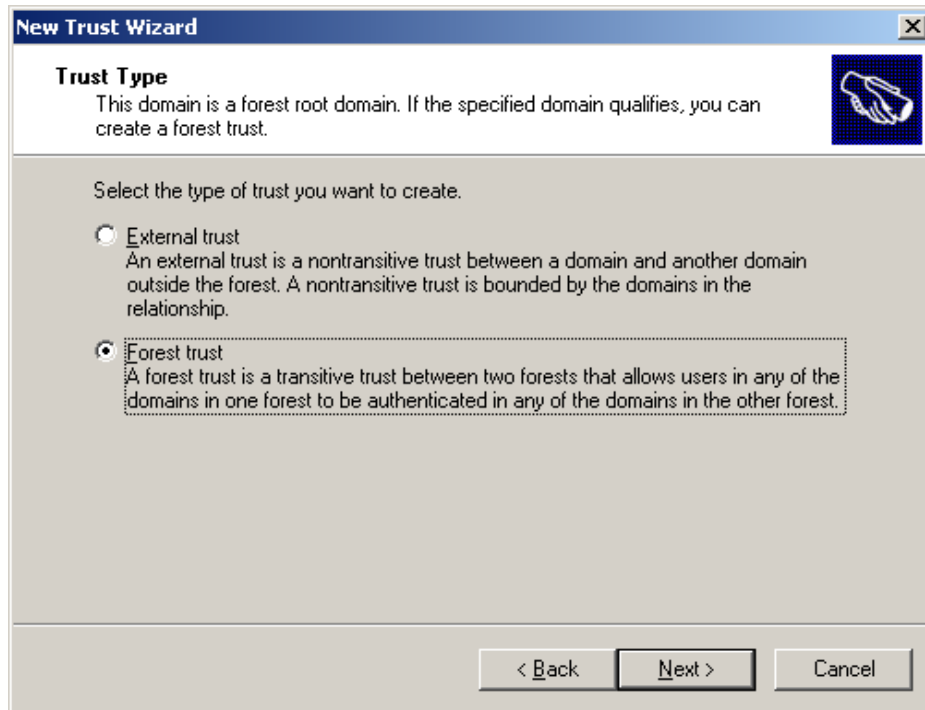
9 To select the direction of trust, do one of the following:

* 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.
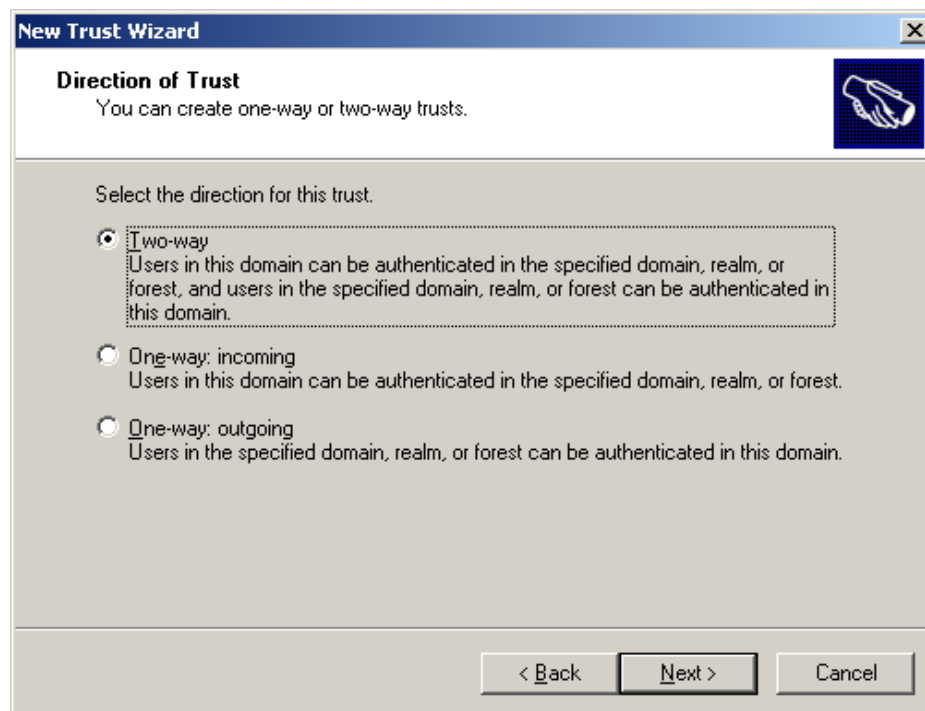
10 Click *Next.*

11 Select *Both this domain and the specified domain* and click *Next*.
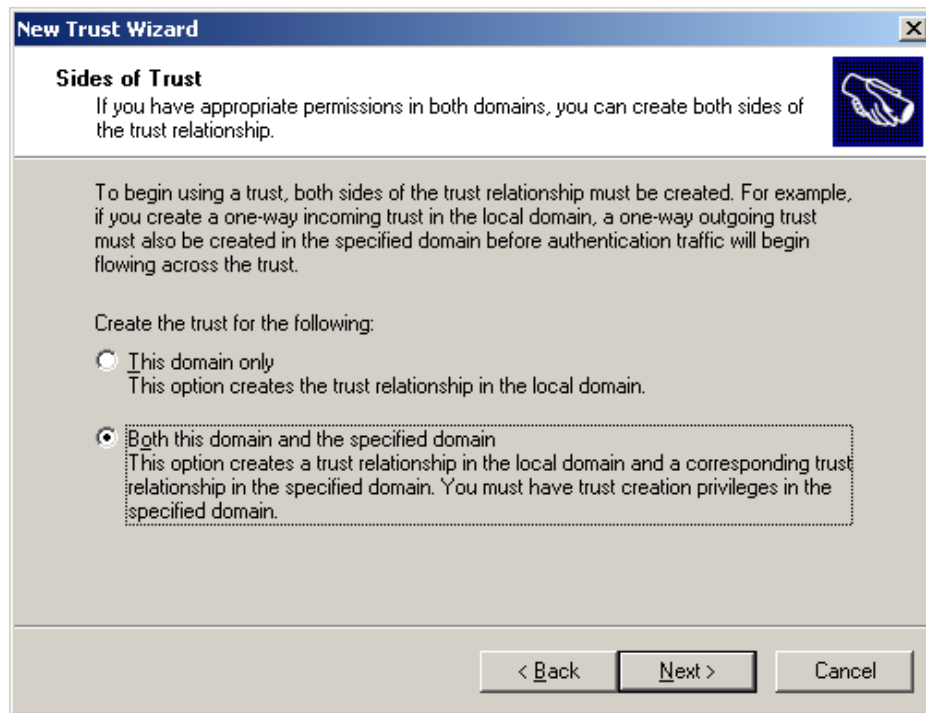
12 Specify the user name and password of the Active Directory domain administrator, then click *Next.*
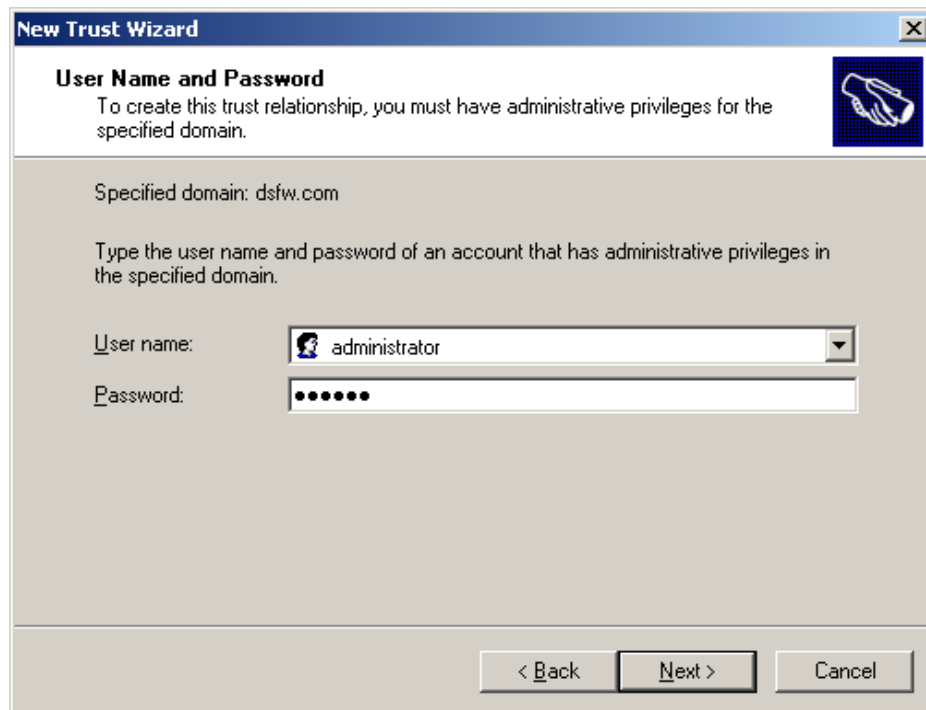
13 Select *Forest-wide authentication* to authorize users to use resources in the local forest or those identified by the administrator, then click *Next*.
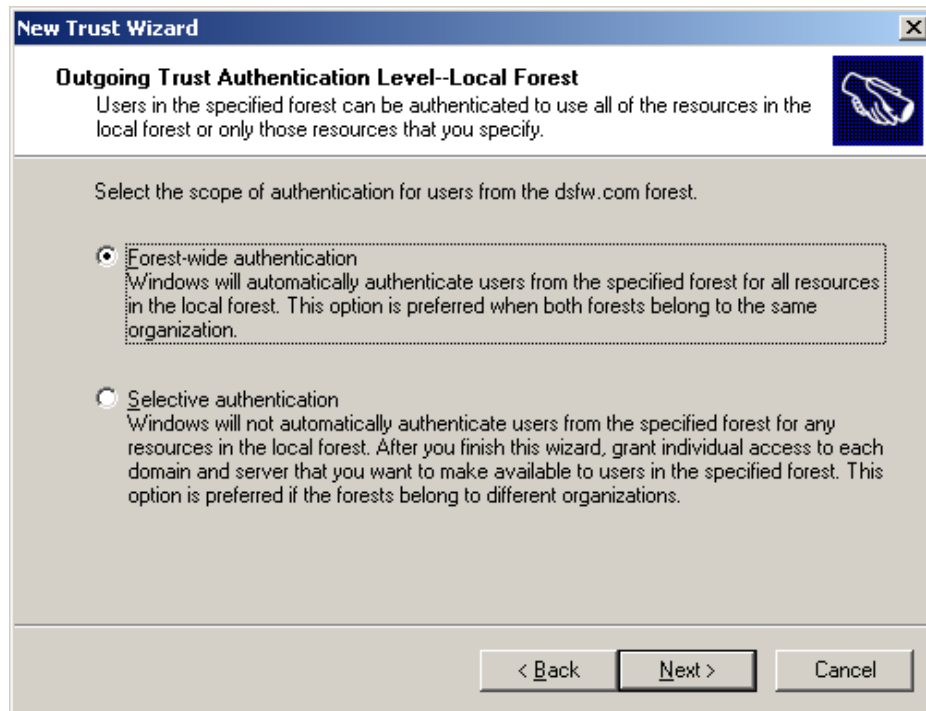
14 Select *Forest-wide authentication* to authenticate Active Directory forest users to use resources in the dsfw.com forest or those identified by the administrator, then click *Next*.
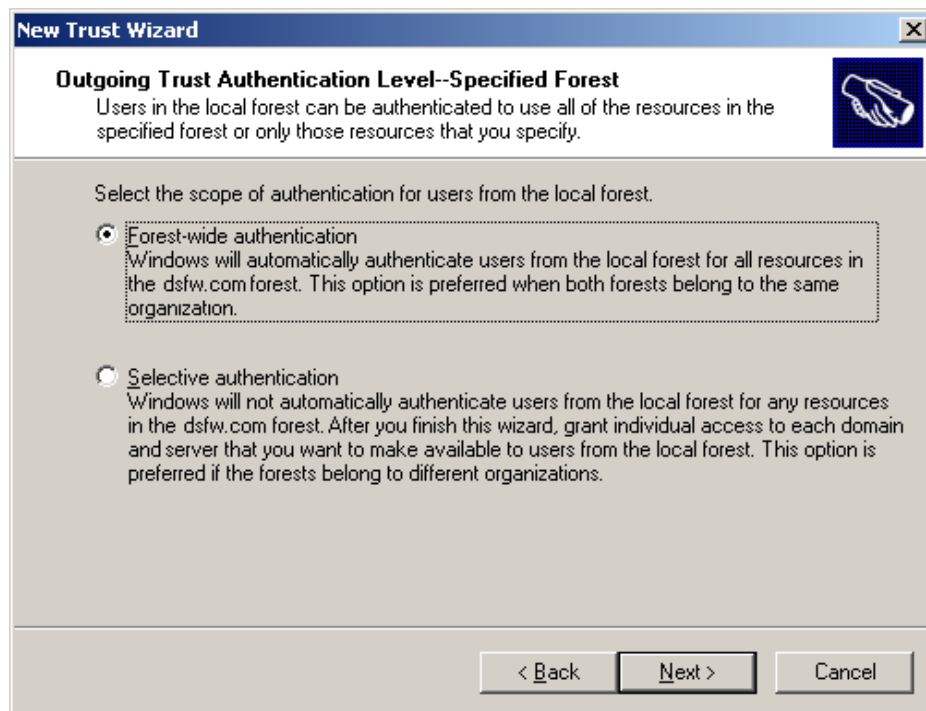
15 Review the trust settings and complete the creation of trust by clicking *Next*.
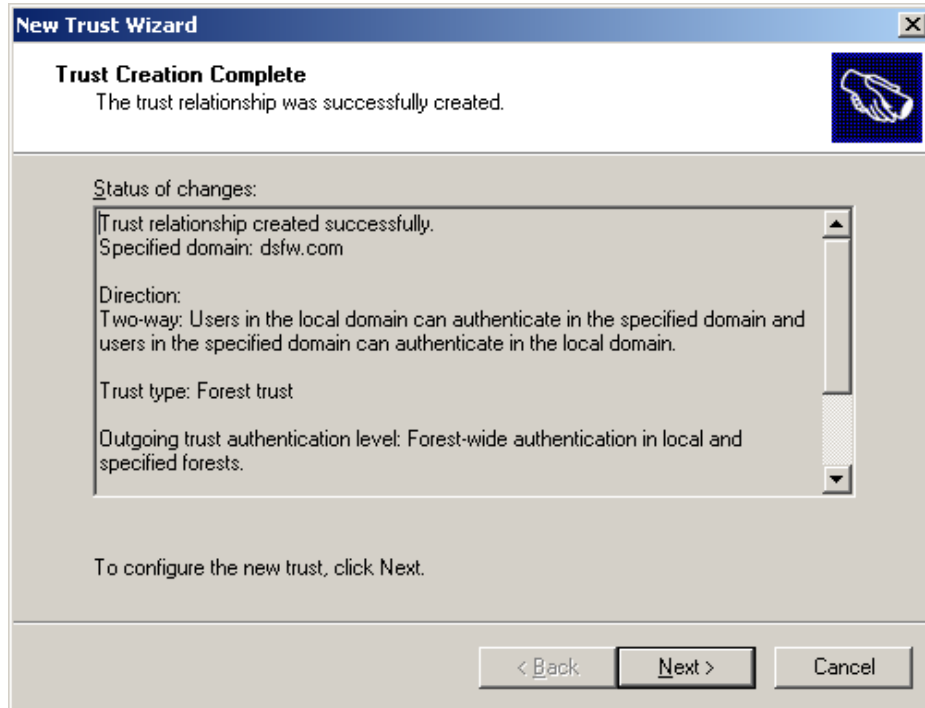
16 Click any option depending on your choice, then click *Next*.
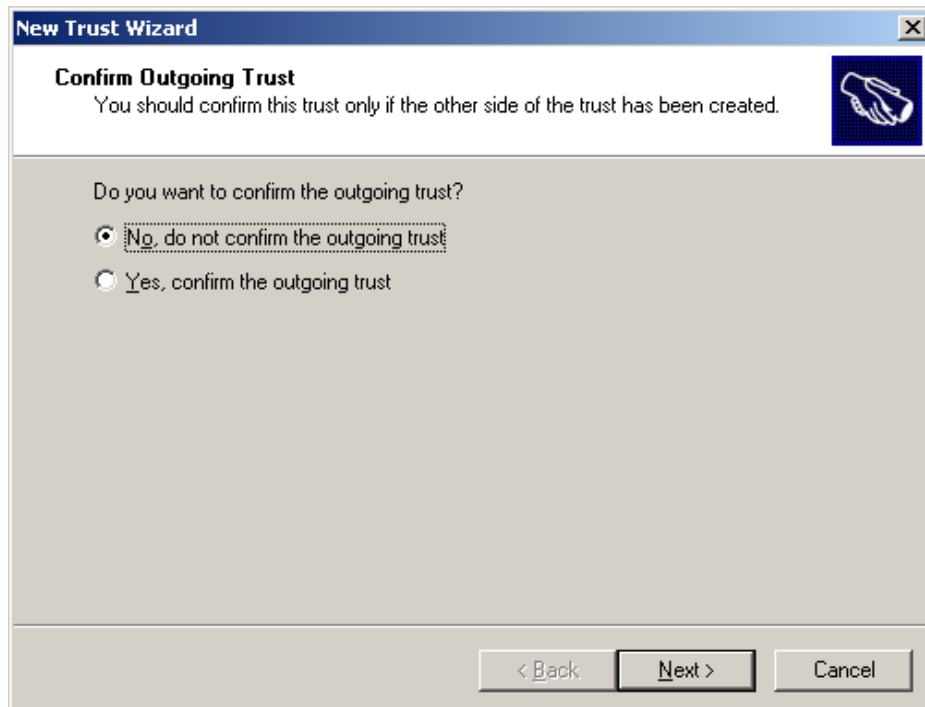
17 Click any option depending on your choice, then click *Next*.
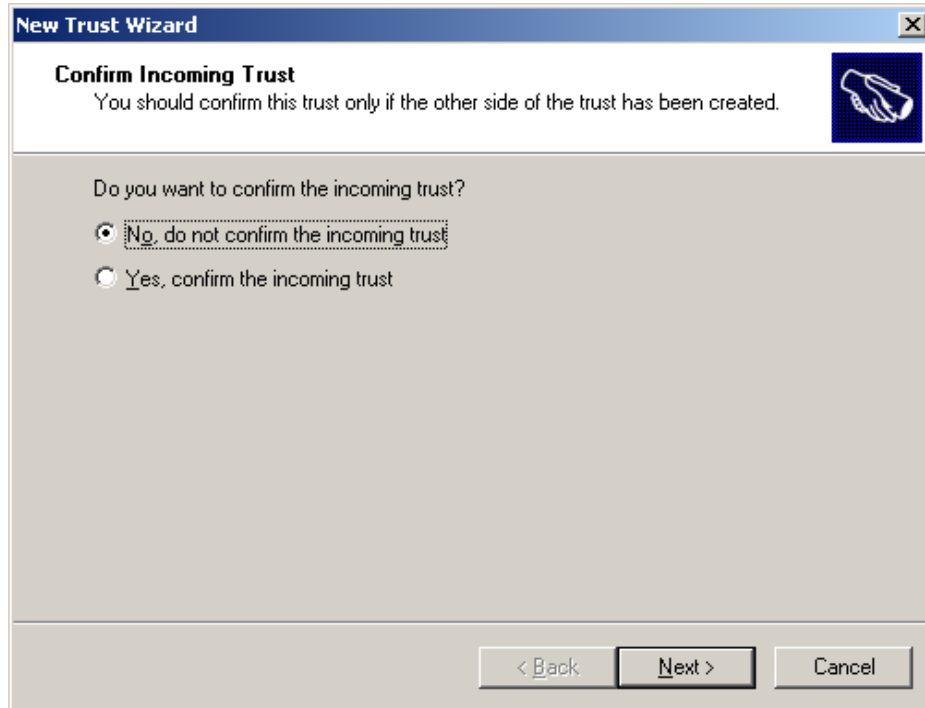
NOTE: In Step 16 and Step 17, if you select Yes option to confirm the trust, ensure that you validate the trust later by selecting *Properties>Validate* option.

18 Complete the trust creation by clicking *Finish*.
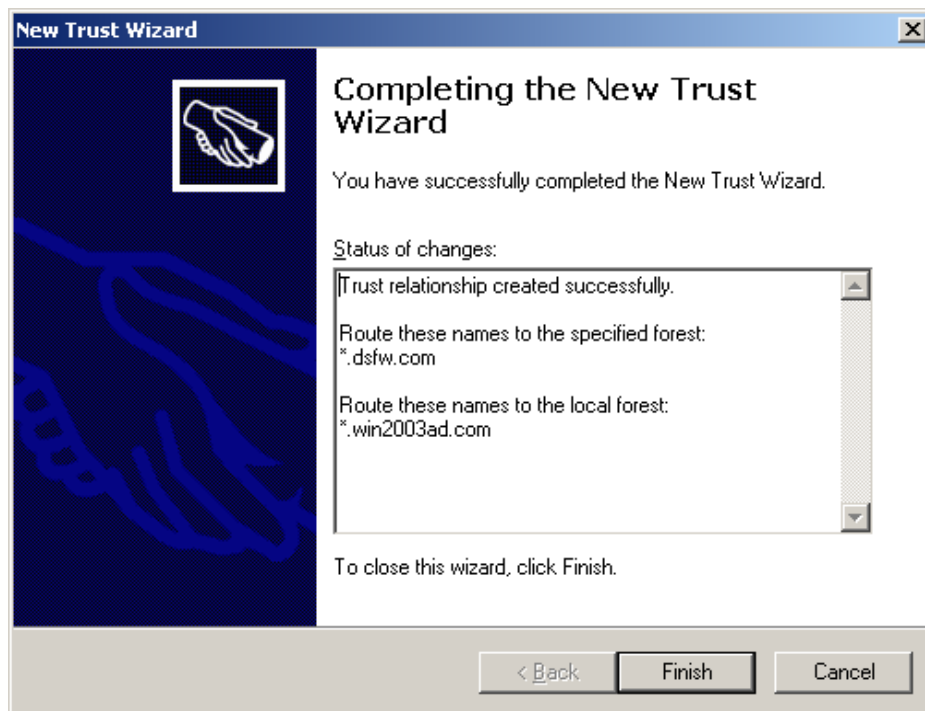
19 The new domain summary appears in the Trusts page.
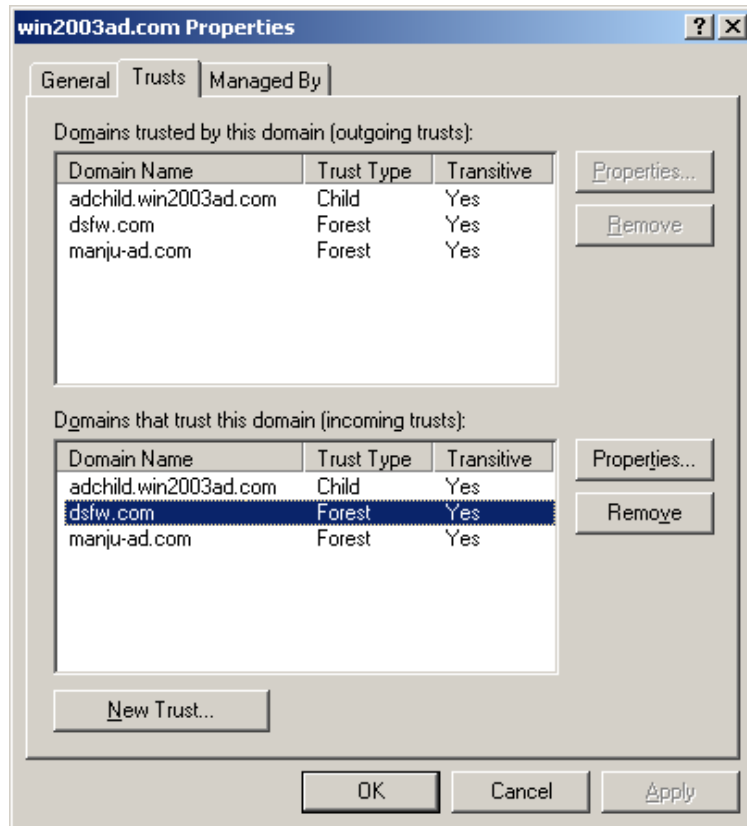
Verifying the Trust

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.mspx).

15.2.2 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).

15.3 Limitations with Cross-Forest Trust

- Trust created between DSfW and Active Directory, will only permit the DSfW users to access the resources on the Active Directory domain. The users in the Active Directory domain cannot access the resources on the DSfW domain.

16 Providing Access to Server Data

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

- Section 16.1, "Accessing Files by Using Native Windows Methods," on page 217
- Section 16.2, "Accessing Files by Using the Novell Client for Windows," on page 224
- Section 16.3, "Accessing Files in Another Domain," on page 225

16.1 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.

This section discusses the following topics:

- Section 16.1.1, "Prerequisites," on page 217
- Section 16.1.2, "Samba: A Key Component of DSfW," on page 218
- Section 16.1.3, "Samba in the DSfW Environment," on page 218
- Section 16.1.4, "Creating Samba Shares in iManager," on page 219
- Section 16.1.5, "Creating Samba Shares in the smb.conf File," on page 221
- Section 16.1.6, "Assigning Rights to Samba Shares," on page 221
- Section 16.1.7, "Adding a Network Place," on page 222
- Section 16.1.8, "Adding a Web Folder," on page 224
- Section 16.1.9, "Mapping Drives to Shares," on page 224

16.1.1 Prerequisites

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

- Section 11.1, "Joining a Windows Workstation to a DSfW Domain," on page 157
- Section 11.2, "Logging In to a DSfW Domain," on page 160
- Chapter 12, "Creating Users," on page 163

16.1.2   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 SP3 customers actually have three Samba configuration options:

- ◆ The open source Samba services that are provided with SUSE Linux Enterprise Server (SLES)10 SP4 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 16.1.3, "Samba in the DSfW Environment," on page 218 explains key differences between the Novell Samba configuration in OES 2 SP3 and the configuration that is included with DSfW.

16.1.3   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 SP3, but it is configured differently as outlined in Table 16-1.

Table 16-1   *Novell Samba in OES 2 SP3 vs. Samba in DSfW*

Item	Novell Samba in OES 2 SP3	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 "stor_nss_lx" in the *stor_nss_lx*	
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 Chapter 12, "Creating Users," on page 163. 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 SP3	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.

16.1.4 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 iManager 2.7.3 Documentation (http://www.novell.com/documentation/imanager27/)

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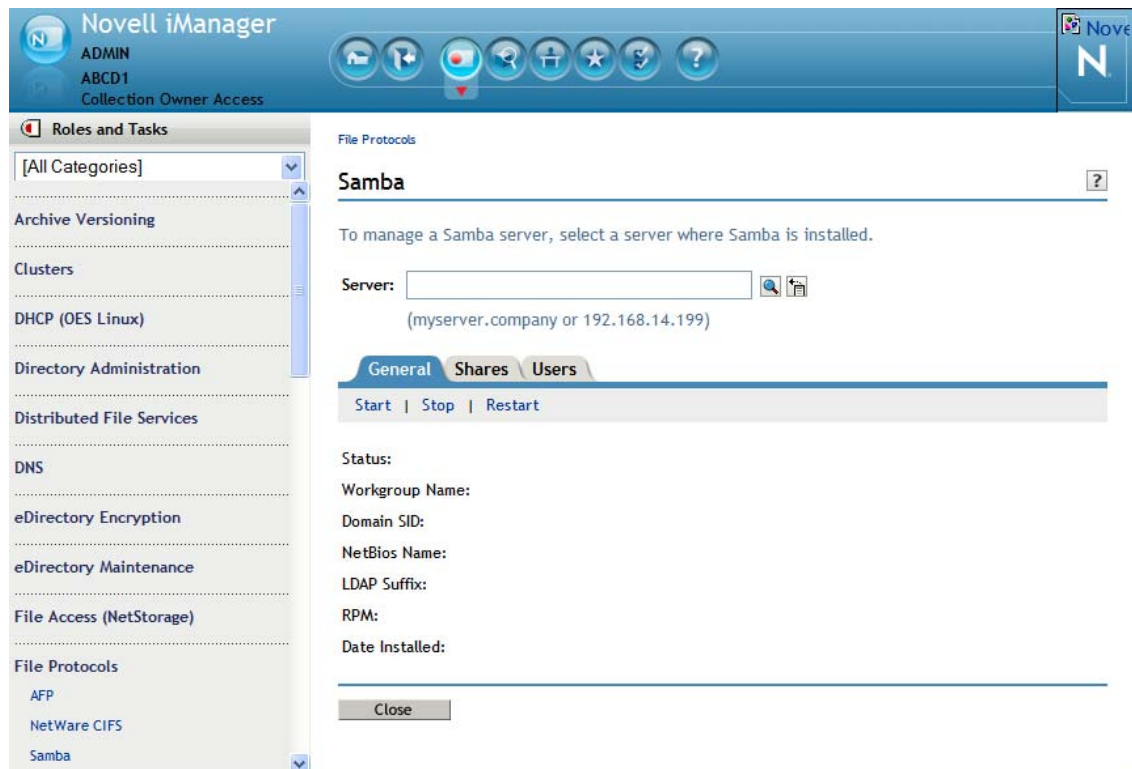
4 Specify the IP address of the server you want to manage, or use the Object Selector to browse to and select the server.

The NCP Server objects for DSfW servers are located in .OESSystemObjects.*domain_name*.com.

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

NOTE: The LDAP Suffix setting does not apply to DSfW servers.

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`.

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 16.1.6, "Assigning Rights to Samba Shares," on page 221 to assign users rights to access the new share.

16.1.5 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 to assign users rights to access the new share.

16.1.6 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 16-2 lists the management tools available for assigning rights to Samba shares created on various file systems.

Table 16-2   *Tools for Managing File System Rights*

File System	Rights Management Tools	Notes
Novell Storage Services (NSS)	*iManager > Files and Folders > Properties > Rights*	For more information on assigning file system rights on NSS volumes in iManager, see "stor_nss_lx"in the *stor_nss_lx*
		The `rights` command available at the terminal prompt is for working with NSS volumes only. For online help, enter `rights` with no options. For more information, see "stor_nss_lx"in the *stor_nss_lx*
	`rights` command	

File System	Rights Management Tools	Notes
NCP Volume on Linux POSIX file systems (no NSS)	iManager > Flies and Folders > Properties > *Rights* `ncpcon > rights`	For more information on assigning file system rights on NCP volumes in iManager, see "stor_nss_lx" in the *stor_nss_lx*. The `rights` command in the `ncpcon` utility is for working with any NCP volume, including NSS volumes and NCP volumes defined on Linux POSIX file systems. For online help, run `ncpcon` and enter `help rights`. For more information, see "stor_nss_lx" in the *stor_nss_lx*.

Linux POSIX file systems (no NSS or NCP)	`chmod`
	`chown`
	`chgrp`
		For information on assigning POSIX rights, see the SLES 10 Installation and Administration Guide (http://www.novell.com/documentation/sles10/book_sle_reference/?page=/documentation/sles10/book_sle_reference/data/cha_acls.html).

Example: Assigning Rights to Folders on an NSS Volume

The example below continues the steps described in Section 16.1.4, "Creating Samba Shares in iManager," on page 219 and Section 16.1.5, "Creating Samba Shares in the smb.conf File," on page 221.

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 -f /projects/doc -r rwemafc trustee user1.full_edir_context
```

```
rights -f /projects/doc -r rf trustee user1.full_edir_context
```

```
rights -f /projects/doc -r rwemafc trustee user2.full_edir_context
```

```
rights -f /projects/doc -r rf trustee user2.full_edir_context
```

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.

16.1.7 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 16.1.4, "Creating Samba Shares in iManager," on page 219 and Section 16.1.5, "Creating Samba Shares in the smb.conf File," on page 221.

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 16.1.4, "Creating Samba Shares in iManager," on page 219.

   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 16.1.4, "Creating Samba Shares in iManager," on page 219.

   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.

16.1.8 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 16.1.4, "Creating Samba Shares in iManager," on page 219 and Section 16.1.5, "Creating Samba Shares in the smb.conf File," on page 221.

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*.

16.1.9 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.

16.2 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.

16.3 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 subsequent 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 cross-forest 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.

With DSfW, you can establish an cross-forest trust between a DSfW domain and an Active Directory domain and thereby allow provisioned users to access files on servers in the Active Directory domain.

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.

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 15, "Managing Trust Relationships in Domain Services for Windows," on page 183.

17 Printing in the Domain Services for Windows Environment

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.

17.1 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) in the *OES2: iPrint for Linux Administration Guide.*

17.2 Special Handling for iPrint on DSfW

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

17.2.1 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 domain controller as well as the 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>`"

17.2.2 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.

17.3 iPrint Clustering in a DSfW Environment

-

17.3.1 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 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 'rwcemf' rights is, `var/opt/novell/iprint` on the specific clustered iPrint NSS Volume.

18 Flexible Single Master Operation (FSMO) Roles

This section provides details on the various FSMO roles and provides details on transferring and seizing FSMO roles.

18.1 FSMO Roles and Limitations

FSMO roles also known as Operations Master are roles performed by the domain controller to facilitate replication.

In a forest, there are five FSMO roles that are assigned to one or more domain controllers. By default the first domain controller in the domain holds all the roles. The five FSMO roles are as follows:

- RID Master
- PDC Emulator Master
- Infrastructure Master
- Schema Master
- Domain Master

18.1.1 RID Master

The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain

Limitations

We support this role completely and there are no known limitations.

18.1.2 PDC Emulator Master

The PDC emulator is a domain controller that advertises itself as the first domain controller to workstations, member servers, and domain controllers

In DSfW the PDC Emulator supports only the following functionality:

By default the editing or creation of Group Policy Objects (GPO) is always done from the GPO copy located in the PDC Emulator's SYSVOL share.

Limitations

All the other features of PDC Emulator are not supported.

18.1.3 Infrastructure Master

The infrastructure is responsible for updating references from objects in its domain to objects in other domains.

Limitations

This role is not defined in DSfW but all the functionalities provided by this role are supported.

18.1.4 Schema Master

The schema master domain controller controls all updates and modifications to the schema.

Limitations

This role is not defined in DSfW but all the functions provided by this role are supported.

18.1.5 Domain Master

The domain naming master domain controller controls the addition or removal of domains in the forest. There can be only one domain naming master in the whole forest.

Limitations

This role is not defined in DSfW but all the functions provided by this role are supported.

18.2 Transferring and Seizing FSMO Roles

The domain controller playing the role of PDC emulator hold the writable copy of SYSVOL while all other domain controllers host a read-only copy of SYSVOL. So for any updates to the group policies, the domain controller has to contact the PDC Emulator.

In event of a hardware or software failure on the domain, it is important to transfer or seize the PDC emulator role to ensure that the DSfW services are fully functional.

Transfer or Seizure of the PDC Emulator role can be done in the following methods:

- Section 18.2.1, "To Transfer the PDC Emulator Role from the First Domain Controller to a Subsequent Domain Controller," on page 231
- Section 18.2.2, "To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Functional)," on page 231
- Section 18.2.3, "To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Not Functional)," on page 232
- Section 18.2.4, "Transferring the ADPH Master Role to Other Domain Controllers," on page 232

IMPORTANT: If during installation of the subsequent domain controller, you haven't selected the Replicate schema and configuration Partitions option, the configuration and schema partition will not be available on the newly designated first domain controller. We strongly recommend that you replicate the schema and configuration partition to the new first domain controller using iManager. For more information, see Administering Replicas (http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html)

18.2.1 To Transfer the PDC Emulator Role from the First Domain Controller to a Subsequent Domain Controller

In this scenario, the machine functioning as the first domain controller is functional. But you want to transfer the PDC Emulator role from the first domain controller to an another domain controller for load-balancing purposes.

From the machine that will serve the new PDC Emulator role, execute the following steps:

1 Transfer all the FSMO roles using the MMC utility. For details, see How to View and Transfer FSMO Roles (http://support.microsoft.com/kb/255690)

2 Get the domain administrator's kerberos ticket by executing following command:

`/opt/novell/xad/bin/kinit Administrator@_DOMAIN NAME_`

3 Update the samba configuration, msdfs links and the DNS SRV record for the first domain controller by running the following script:

`/opt/novell/xad/share/dcinit/UpdatePDCMaster.pl`

18.2.2 To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Functional)

In this scenario, the directory services on the first domain controller has gone down but the DNS service is up. As the directory services are not functional, the FSMO roles have to be forcibly seized and transferred to an another domain controller using the following procedure:

1 From the Windows workstation joined to the domain, seize all the FSMO roles using the `ntsdutil` utility.

2 From the machine that will serve as the new domain controller, get the domain administrator's kerberos ticket by executing following command:

`/opt/novell/xad/bin/kinit Administrator@_DOMAIN NAME_`

3 Update the samba configuration, msdfs links and the DNS SRV record for first domain controller by running the following script:

`/opt/novell/xad/share/dcinit/UpdatePDCMaster.pl`

18.2.3 To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Not Functional)

In this scenario, the directory service and the DNS service is not functional. To resolve this, the DNS service has to be migrated to the new domain controller and the FSMO roles also have to be forcibly seized and transferred to an another domain controller using the following procedure:

1 From the Windows workstation joined to the domain, seize all the FSMO roles using the `ntsdutil` utility.

2 Migrate DNS from the first Domain Controller to another domain controller by using the procedure in Migrating DNS to Another Domain Controller. If the machine that will serve as the new domain controller is already configured as a DNS server, then you need not migrate DNS to the new domain controller. However, if you do not migrate DNS to the new domain controller, you must ensure that the new domain controller has been configured as a designated primary DNS server.

3 Get the domain administrator's kerberos ticket by executing following command:

`/opt/novell/xad/bin/kinit Administrator@_DOMAIN NAME_`

4 Update the samba configuration, msdfs links and the DNS SRV record for first domain controller by running the following script:

`/opt/novell/xad/share/dcinit/UpdatePDCMaster.pl`

18.2.4 Transferring the ADPH Master Role to Other Domain Controllers

You can transfer the RID master role by using the following methods:

- "Using MMC" on page 232
- "Using LDIF File" on page 232

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
```

19 Troubleshooting

Use the information in this section to resolve DSfW issues.

19.1 Troubleshooting DSfW

19.1.1 DSfW Fails to Set Up Signed NTP for Clients to Trust

During DSfW services startup, you might receive the following error:

```
/var/lib/ntp//var/opt/novell/xad/rpc/xadsd' to `/var/opt/novell/xad/rpc/
xadsd':Invalid cross-device link
```

This is because `/var/opt/` and `/var/opt/novell/` are in different partitions, so DSfW fails to set up signed NTP for clients to trust.

To set up the signed NTP for clients in a cross-partition environment:

1 Apply the November 2012 patch for OES 2 SP3.

2 Execute the following on the DSfW server:

- /usr/bin/perl /opt/novell/xad/sbin/cross_partition_ntp_setup.pl

  This tool populates the new mounted location for `/var/opt/` or `/var/opt/novell/` in `/etc/init.d/xadsd`, `/etc/init.d/rpcd`, `/etc/samba/smb.conf`, and `/etc/profile.d/novell-xad.sh`.

- /opt/novell/xad/bin/xadcntrl reload

- /usr/sbin/rcntp restart

19.1.2 W32Time Auth Provider for NTP Does Not Work in a Cross-Partition Setup

Apparmor abstraction has static information related to NTP. The static information represents a socket file `/var/lib/ntp/var/opt/novell/xad/rpc/xadsd`. This information is valid only when the system has a single partition for '/' (root partition) or `/var (var partition)`. However, in a multiple partition setup where `/var/opt`, `/var/opt/novell`, or `/var/opt/novell/xad` directory is

on a different partition, the above socket file path is no longer valid. In such a setup depending on a particular partition pattern, the socket file path is going to be different. Along with the static information a new dynamic information has to be set in the Apparmor abstraction for NTP profile.

On an OES2 SP3 server that is running as a DSfW domain controller if the `/var/opt`, `/var/opt/novell`, or `/var/opt/novell/xad` directory is on a different partition, you must change the AppArmor NTP profile from enforce mode to complain mode in order to allow the ntpd daemon to process signed NTP requests coming from the Windows workstations that are joined to the DSfW domain.

Do the following to change the NTP AppArmor profile from enforce to complain mode:

1 rcapparmor stop

2 rcntp stop

3 /usr/sbin/complain /etc/apparmor.d/usr.sbin.ntpd /usr/sbin/ntpd

4 rcapparmor start

5 rcntp start

Novell plans to address this issue in a future release.

19.1.3 setspn Tool Fails to Bind to a DSfW Domain Controller (DC) Using NetBIOS Domain Name

If you attempt to bind to a DSfW domain controller using the setspn tool by specifying the NetBIOS domain name, you will receive the following error:

```
Failed to bind to DC of domain DSFW, error 0x5/5 -> Access is denied.
```

This is because there is no corresponding servicePrincipalName value on the DC object. The DC object needs to be extended with the new servicePrincipalName value containing NetBIOS domain name. To apply this configuration change, ensure that you move to the latest OES patch level and run the following command on every domain controller.

```
$ /opt/novell/xad/share/dcinit/UpdateDC.pl poststage
```

19.1.4 Changing the User Password Requires Reimport of Third-Party Application Certificates

If a third-party application requires importing a certificate for authentication and a DSfW user changes the workstation login password after importing the certificate, then the user needs to reimport the certificate after the password change. This issue occurs only if the user password is changed at the workstation and does not occur if the password is changed using iManager.

NOTE: This issue occurs only with Windows 7 or later versions.

19.1.5 Kinit Not Working for Users

Kinit will not work for users if they were part of a non-dsfw partition that later got merged with the domain partition. This is because after merging the partition, users are not samified automatically. You must use domaincntrl --samify option to do this manually. However, if universal password is not enabled for a user, supplementalcredentials and unicodepwd attributes are not generated. If universal password is enabled, these attributes get populated as part of the samification.

19.1.6 Cleanup Task Fails in Name Mapped Scenarios

In name mapped installation scenarios, the cleanup task in the provisioning process fails to set the ldapserver attribute. This fails the provisioning process. This issue may occur when the netware server is holding the master replica and the time between the netware server and the domain controller is not in sync. To resolve the time synchronization issue, do the following:

1 Run the following command to display the REPLICA OPTIONS menu:

`ndsrepair -P -Ad`

2 To repair the time stamps and declare a new epoch, enter

`12`

3 You are prompted to perform a database repair and declare a new epoch, enter

`Y`

4 Proceed to provide administrator name and password.

After resolving the time synchronization issue, you must again run the cleanup task in the provisioning wizard.

19.1.7 MMC Fails to Create Users

If you receive the following message while creating users, it indicates a failure while setting Universal Password.
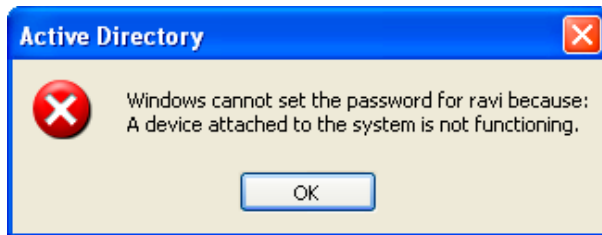
You must ensure that the user is associated to a password policy that has the Universal Password Policy turned on. The password policy can be directly associated to the user, the immediate container, or the partition.

19.1.8 Using DSfW Server as a WINS Server Results in an Error

On using DSfW as a WINS server, you may receive an error indicating that NetBIOS name is not registered. This is because the value of the parameter dns proxy in the `smb.conf` file is set to yes by default. You must ensure that the value of dns proxy is set to No.

19.1.9 iManager Fails to Create Samba Shares if the Administrator Name is Changed using MMC

If you change the administrator name using MMC after the installation and configuration of DSfW, iManager fails to create Samba Shares. This is because renaming the administrator name using MMC does not update the uniqueID attribute. You must explicitly modify the uniqueID attribute to reflect the changed administrator name using iManager.

19.1.10 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 command.

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
```

19.1.11 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 admingroup associated with the server.

This applies to any administrator that you want to manage DSfW on that server.

19.1.12 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.

19.1.13 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.

19.1.14 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/share/dcinit/provision/provision_samify.pl` on the DSfW server.

19.1.15 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.

The correct order to restart services are:

1. ndsd (eDirectory)
2. novell-named (DNS)
3. nscd (Name Server cache daemon)
4. rpcd (RPC server)
5. Xad-krb5kdc (Kerberos)
6. xad-kpasswdd (Kpassword)
7. xadsd (XAD daemon)
8. nmb (NMB server, NETBIOS lookup)
9. winbind (winbind)
10. smb (Samba)
11. sshd (SSH)
12. rsyncd (rsync)

To restart the services use the `xadcntrl reload` command.

19.1.16 Users Cannot Join a Workstation to a Domain

For joining domains, ensure that SLES 10 SP4 is installed first, updated with Samba 3.0.36 patch, and then OES2 SP3 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
```

19.1.17 Joining Multiple Workstations to the Domain at the Same Time Results in an Error

If you attempt to join multiple workstations to the domain at the same time it will result in an error. To resolve this issue, add the following line in the `/etc/init.d/smb` file:

```
export KRB5RCACHETYPE="none"
```

After making the changes, restart the Samba service.

19.1.18 Requirements for Samba/CIFS Access 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

To create Samba shares, the admingroup 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 `namgrouplist -x <o=organization> | grep admingroup` to list all the admingroups.

2 Add the listed admingroups 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.

19.1.19 Identifying novell-named Error

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.

19.1.20 Login Failure

One of the common reasons for this error is that the users are not samified. To verify if the users are samified, execute the following command:

```
ldapsearch -D <admin DN> -w <passwd> -b <user dn> -x samaccountname -LLL
```

This command returns the `dn` and `samaccountName` attribute. If the `samaccountName` attribute is missing, it indicates that the users are not samified.

To samify the users, run the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_samify.pl
```

19.1.21 Unable to Connect to Legacy Applications

To connect to legacy applications, you must either extend the object class or connect to a non-DSfW server.

19.1.22 User in a Domain Can Access Resources from Another Domain by Using the UID of the Foreign User

A foreign user is a user who is part of another domain. If this is the case, the administrator must ensure the UID allocation does not overlap between the domains.

19.1.23 Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition

If a user with a Universal password policy is moved from non-domain partition to a DSfW partition, the user will not be able to login into the DSfW domain.

To resolve this issue, delete the old password policy using iManager. After this step is done, the user will be able to login to the workstation.

19.1.24 Users Not Associated With a Universal Password Policy Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition

If a user that is not associated with a Universal password policy is moved from non-domain partition to a DSfW partition, the user will not be able to login into the DSfW domain.

To resolve this issue, attempt logging in using `ndsLogin` utility.

19.1.25 Child Domains Slow Down When the First Domain Controller is Not Functional

This issue is seen where there is a parent domain and one or more child domains in the DSfW forest.

If all of the domain controllers in a domain go down, requests to domains that are up and running might take a long time to respond.

To prevent this issue from occurring, make sure that at least one domain controller in a domain is up.

For more details on this issue, see TID 7003552. (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7003552&sliceId=1&docTypeID=DT_TID_1_1&dialogID=77853582&stateId=0%200%2077851408)

19.1.26 Making the DSfW Server work When The IP address is Changed

After the IP address is changed, execute the following instructions:

1 Execute the procedure listed in "Changing the Server's Address Configuration" in the *OES 2 SP3: Planning and Implementation Guide*.

2 Complete the server reconfiguration by executing the instructions in "DSfW "in the *OES 2 SP3: Planning and Implementation Guide*.

After executing these steps, if the IP address change is not effective, delete the `/etc/opt/novell/named/{DOMAIN}.db` file and restart `named`. The IP address changes will be effective.

19.1.27 Error Mapping SID to UID

This error will be recorded in the `/var/log/samba/log.winbindd` or any of the samba log files available at `/var/log/samba/` folder.

If you see a rec_free_read bad magic entry in the log files, it indicates that the `tdb` files are corrupted. Delete the `tdb` files in `/var/lib/samba/` folder and restart the samba services(smb, winbind, and nmb) to proceed.

19.1.28 After DSfW Installation, the Services are Not Working

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.

19.2 Error Messages in Log Files

19.2.1 ndsd Log File Error

NlGetLocatorConfiguration "Could not get forest name from directory

If this message appears continuously in the `/var/opt/novell/eDirectory/log/ndsd.log` file, it indicates that there is an error in name-mapping.

To resolve this error, reload the LDAP server by using the following commands:

```
nldap -u
```

```
nldap -l
```

19.3 iPrint Issues

 Section 19.3.1, "Driver Store Fails to Create," on page 245

19.3.1 Driver Store Fails to Create

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 the 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)
```

19.4   Novell SecureLogin Issues

- Section 19.4.1, "Novell SecureLogin LDAP Attribute Mappings," on page 246

19.4.1   Novell SecureLogin LDAP Attribute Mappings

When you install Novell SecureLogin (NSL) on an existing DSfW partition, it functions as expected. However, if DSfW is deployed on a tree that has SecureLogin already installed, then the existing NSL-LDAP mappings will need to be explicitly mapped in this new DSfW server. Otherwise, the NSL attributes will be auto-mapped to LDAP names (e.g. NDS Name Prot:SSO Auth mapped to LDAP name ProtSSOAuth), which is undesirable.

This difference in attribute mapping is because DSfW associates it's LDAP server to a new LDAP group object and does not associate to an existing LDAP group object which contains the NSL mapping.

19.5   Group Policy Management Issues

- Section 19.5.1, "Group Policy Operations are Failing," on page 246
- Section 19.5.2, "Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition," on page 246
- Section 19.5.3, "Members of GroupPolicy Creator Owner group cannot change the active DFS Referral," on page 246
- Section 19.5.4, "Ignore Warnings while Backing up Group Policies," on page 247
- Section 19.5.5, "WMI Filters Cannot be Applied for Processing GPOs," on page 247

19.5.1   Group Policy Operations are Failing

The execution of the login scripts and GPO's fail when the workstation connects to an additional domain controller during the login process. For more information, see TID 7009466.

19.5.2   Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition

If a user with a Universal password policy is moved from non-domain partition to a DSfW partition, the user will not be able to login into the DSfW domain.

To resolve this issue, delete the old password policy using iManager. After this step is done, the user will be able to login to the workstation.

19.5.3   Members of GroupPolicy Creator Owner group cannot change the active DFS Referral

If a member of the GroupPolicy Creator Owner group tries editing the group policy through the Group Policy Management Console(GPMC), and if the GPMC is referring the ADC, the user will not be permitted to change the DFS referral to make it point to the first domain controller. To make changes, you will require administrator privileges

19.5.4 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.

19.5.5 WMI Filters Cannot be Applied for Processing GPOs

WMI filters are not supported in this release.

A Executing Provisioning Tasks Manually

This section details the method of Provisioning DSfW server by using command line scripts.

A.1 Exporting Passwords

Before provisioning DSfW server using the command line scripts, it is important to export the passwords in order to authenticate and pass the credentials for the provisioning tasks.

You do not need to export the username. This is because the username used during YaST configuration is stored in the `xad.ini` file and reused for provisioning.

Table A-1   *Details of Passwords to be Exported*

Scenarios	Password Details
Forest Root Domain	export NDSEXISTINGADMINPASSWD and ADM_PASSWD with tree admin credentials
Child Domain	export ADM_PASSWD_DOMAIN = current domain password
	export ADM_PASSWD_PARENT = parent domain password
	export NDSEXISTINGADMINPASSWD = tree domain password.
	export NDSEXISTINGADMINNAME=tree admin
Subsequent Domain Controller	export ADM_PASSWD = current domain password
	export NDSEXISTINGADMINPASSWD = tree domain password

A.2 Provisioning Tasks

NOTE: To know about the provisioning tasks associated with each installation scenario, see, Section 7.6, "Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios," on page 131

- ◆ Section A.2.1, "Provisioning Precheck," on page 250
- ◆ Section A.2.2, "Configure DNS," on page 250
- ◆ Section A.2.3, "Configure SLAPI Plug-ins," on page 250

A.2.1 Provisioning Precheck

This task verifies the state of the servers to ensure that they are ready for provisioning.

As part of the provisioning precheck activity, a health check is performed in the background to validate the state of the system to avoid a stale state. Not validating the system state can lead to irrecoverable failures in the system. This makes the health check very important.

After you have exported the environment variable, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_precheck.pl
```

A.2.2 Configure DNS

This task configures DNS on the DSfW server. DSfW uses DNS as its location service, enabling computers to find the location of domain controllers.

> **NOTE:** As part of DSfW installation, the DNS server is configured in the first domain in the forest. For subsequent child domains, you can either link to the DNS server in the first domain or install a DNS server for the child domain.

After you have exported the environment variable, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_dns.pl
```

A.2.3 Configure SLAPI Plug-ins

This task loads the SLAPI plug-ins. The SLAPI plug-ins take care of maintaining the Active Directory information model. This ensures that the SLAPI framework is ready before any domain-specific data is added.

After you have exported the environment variable, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_config_slapi.pl
```

A.2.4 Create Domain Partition

This task creates a partition for the domain.

This partition has complete information about all the domain objects. Information about the domain objects is replicated to domain controllers in the same domain.

NOTE: This task is not executed in a name-mapped scenario.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_partition_domain.pl
```

A.2.5 Add Domain Replica

This task moves the replica of the domain partition from the master server to the local server.

NOTE: This task is executed for all provisioning scenarios except for non-name-mapped and forest root domain installation.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_add_domain_replica.pl
```

A.2.6 Add Domain Objects

This task adds the domain objects that represent the domain-specific information under the domain partition.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_add_domainobj.pl
```

A.2.7 Create Configuration Partition

This task partitions the configuration container (cn=configuration) created as part of the Domain Objects Addition task. This configuration partition contains information on the physical structure and configuration of the forest (such as the site topology).

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_partition_configuration.pl
```

A.2.8 Create Schema Partition

This task partitions the schema container (cn=schema) created during the Domain Objects Addition task.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_partition_schema.pl
```

A.2.9 Add Configuration Objects

This task adds the configuration and schema partition objects. It helps maintain integrity with the Active Directory information model.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_add_configobj.pl
```

A.2.10 Add Domain Controller

This task adds the domain controller to the domain.

This task creates additional objects that make your server act as a domain controller. The task is only executed if you have installed DSfW as an additional domain controller in the domain.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_domain_join.pl
```

A.2.11 Assign Rights

This task configures directory-specific access rights for the domain and the domain administrator being provisioned.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_config_acl.pl
```

A.2.12 Restart DSfW Services

This task restarts services in order of dependence.

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_restart_dsfw.pl
```

A.2.13 Set Credential for Accounts

This task sets the password and kerberizes the administrator, krbgt, and guest accounts.

After you have exported the environment variable, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_set_cred_foraccounts.pl
```

A.2.14 Enable Kerberos

In DSfW, Kerberos is the primary security protocol for authentication within a domain. The Kerberos authentication mechanism issues tickets for accessing network services.

As part of this task, the krb5.conf file is updated and a ticket is sent to the administrator principal.

After you have exported the passwords, execute the following script:

`/opt/novell/xad/share/dcinit/provision/provision_enable_local_krb.pl`

A.2.15   Samify Objects

This task is specific to a name-mapped installation. The existing user and group objects are extended to receive Active Directory attributes that allow them to be part of the domain being provisioned. Some of the extended attributes are supplementary Credentials, objectSid, and samAccountName.

After you have exported the passwords, execute the following script:

`/opt/novell/xad/share/dcinit/provision/provision_samify.pl`

A.2.16   Establish Trust

A trust is a relationship established between domains that enables users in one domain to be authenticated by a domain controller in the other domain. Authentication between domains occurs through trusts.

After you have exported the environment variable, execute the following script:

`/opt/novell/xad/share/dcinit/provision/provision_trusts_crossref.pl`

A.2.17   Update Service Configuration

This task modifies the configuration of services such as sshd, rsync and krb5. It configures the `sysvol` policies, synchronizes the group policies with NMAS, and adds a crontab entry for subsequent synchronization of policies.

After you have exported the passwords, execute the following script:

`/opt/novell/xad/share/dcinit/provision/provision_crontab_entry_add.pl`

A.2.18   Cleanup

This task removes files from a partial or failed installation. It also removes the temp directories and checkpoint files created during provisioning.

After you have exported the environment variable, execute the following script:

`/opt/novell/xad/share/dcinit/provision/provision_cleanup.pl`

B Schema

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 first 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 all the domain controllers of a domain to improve the response time and performance of the server.

B.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 B-1 *Some Attributes for the Attribute Schema 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.
lDAPDisplayName	Unicode	Name by which LDAP clients identify this attribute. lDAPDisplayName 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. **NOTE:** 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).
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.
systemFlags	Integer	Flags that determine specific system operations. This attribute cannot be set or modified. The following systemFlags attributes are relevant to the schema objects: • The attribute is required to be a member of the partial set = 0x00000002 • The attribute is not replicated = 0x00000001 • The attribute is a constructed attribute = 0x00000004 systemFlags is not a mandatory attribute.

Attribute	Syntax	Description
searchFlags	integer	The searchFlags property of each property's attributeSchema object defines different behaviors, including whether a property is indexed.
		The seven currently defined bits for this attribute are:
		◆ 1 = Index the attribute only
		◆ 2 = Index the container and the attribute
		◆ 4 = Add this attribute to the ambiguous name resolution (ANR) set
		◆ 8 = Preserve this attribute on logical deletion (not implemented)
		◆ 16 = Include this attribute when copying a user object
		◆ 32 = Create a Tuple index for the attribute to improve medial searches (not implemented)
		◆ 64 = Reserved for future use; the value should be 0.
		◆ 128 = Mark the attribute confidential (not implemented)
		searchFlags is not a mandatory attribute.
isMemberofPartialAttributeSet	BOOL	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.
		isMemberof PartialAttributeSet is not a mandatory attribute.
systemOnly	BOOL	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.
objectClass	Object identifier	The class of this object, which is always attributeSchema. objectClass is a mandatory and multivalued attribute.
nTSecurityDescriptor	NT-Sec-Des	The security descriptor on the attributeSchema object itself. inTSecurityDescriptor is a mandatory attribute.
oMObjectClass	String (Octet)	For attributes with object syntax (OM-syntax = 127), this is the Basic Encoding Rules (BER) encoded object identifier of the XOM object class.
		For more information about BER encoding, see *Request for Comments (RFC) 2251 (http://www.ietf.org/rfc/rfc2251.txt)* in the IETF RFC Database.
		oMObjectClass is not a mandatory attribute.
LinkID	Integer	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.
		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.
		An even integer denotes a forward link; an odd integer denotes a back link.
		LinkID is not a mandatory attribute.

B.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 B.2, "Extending the Third-Party Schema," on page 262 for more information on automating mapping.

Table B-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.
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.

Syntax	Attribute Syntax	oMSyntax	eDirectory Syntax	Description
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).

B.1.2 Attribute Mappings

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

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

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

B.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 B-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.
lDAPDisplayName	Unicode	The name by which LDAP clients identify this class. lDAPDisplayName is a mandatory attribute.
schemaIDGUID	String (Octet)	The GUID that uniquely identifies this class. schemaIDGUID 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.
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.

Attribute	Syntax	Description
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	The class types are defined as follows: ◆ Structural = 1 ◆ Abstract = 2 ◆ Auxiliary = 3 objectClassCategory is a mandatory attribute.
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.
nTSecurityDescriptor	NT-Sec-Desc	The security descriptor on the classSchema object. nTSecurityDescriptor is not a mandatory attribute.
defaultObjectCategory	Distinguished name	The default object category of new instances of this class. If none has been specified, the objectClass value is used. For example, suppose that 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. defaultObjectCategory is a mandatory attribute.

B.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 B-5   *Attributes for the AttributeSchema Class*

LDAP Classes	eDirectory Classes
ndsComputer	Computer
computer	mSDS:Computer
ndsDmd	dmd
dMD	mSDS:DMD
ndsServer	server

LDAP Classes	eDirectory Classes
server	mSDS:Server
ndsVolume	volume
volume	mSDS:Volume
organizationalPerson	Organizational Person
organizationalUnit	Organizational Unit
groupOfNames	Group
groupOfUniqueNames	Group
inetOrgPerson	User

B.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 DNs of the schema elements in the LDIF file as necessary.

B.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
```

C Understanding DSfW in Relation to IDM and Samba

This section analyses the features and capabilities of DSfW in relation to Samba and IDM.

C.1 Understanding DSfW in Relation to Samba

DSfW simulates Active Directory environment on eDirectory and provides interoperability between eDirectory and Active Directory. A suite of services integrated with Samba help in achieving Active Directory equivalent environment. SAMBA is by default packaged with SLES and has the capability to emulate NT4 domain controller. DSfW takes this functionality forward and uses it to emulate Active Directory.

This means that the DSfW server can inter-operate with Active Directory and provides a gateway for DSfW users to access Active Directory resources with the help of trusts.This facilitates an environment where SLES and Windows servers can co-exist in an organization that has only Active Directory or only eDirectory or a mix of both Active Directory and eDirectory environments.

It is important to note that apart from providing emulation services for Active Directory, DSfW continues to support existing OES (Open Enterprise Server) services for the users in the DSfW environment.

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.

A DSfW server uses the following services in order to provide Active Directory equivalent environment:

* SAMBA-3.0.x
* eDirectory
* Novell Bind (DNS)
* NTP server
* xadsd (For handling RPC calls over LSARPC, SAMR and NETLOGON)
* Kerberos KDC
* Kerberos password server

During installation through YaST, when the *Novell Domain Services for Windows* pattern is selected, a set of other dependant RPMs also get selected. Provisioning helps in configuring DSfW and the supporting services.

Table C-1   *DSfW and Samba*

Functionalities	Samba	DSfW
Emulation	Emulates NT4 Domain Controller or can be a member server of Active Directory or NT domain.	Emulates Active Directory and can also be a member server.
Management	Can be managed through Windows NT4 Domain Server Manager and the Windows NT4 Domain User Manager. But cannot be managed from MMC.	DSfW can be managed from Microsoft MMC as well as eDirectory web management tools like iManager. So any Windows member server/client joined to the DSfW domain can use the power of Active Directory for creating shares, assigning access rights, managing users, trusts and group policies. In DSfW the Samba-3 shares and access rights can be managed using iManager.
Group Policies	No support for group policies that are crucial to implement security settings and enforce IT policies.	Supports Group Policies. For more information, see Managing Group Policy Settings.
Trusts	Supports NT style manual trusts between two domains.	Supports Active Directory level trusts that includes automatic Kerberos transitive trusts and cross-forest trusts.
DNS and Secure Updates	Does not come with DNS. Has to be installed separately. The bind DNS does not support secure dynamic updates. So, the DNS records have to be manually managed by the Active Directory administrators. Active Directory administrator has to create records for the DCs and for every member server joined to the domain.	Comes packaged with Novell Bind DNS that supports secure dynamic updates. As it is integrated into eDirectory, it provides centralized Active Directory administration and enterprise-wide management of DNS using iManager or Java Management Console. It leverages the benefit of eDirectory as Novell DNS configuration information is replicated just like any other data in eDirectory.
Provisioning Users	Provisioning is performed by including only Samba-specific information in the user objects created in the LDAP backend.	Provisioning is performed by extending the existing eDirectory object class and including Active Directory information in the user objects. As a result, DSfW has the same information model as Active Directory.

Functionalities	Samba	DSfW
Access Control at File system/ Share level	Samba supports access control at both share level and file system level. It can be managed at share level from any Windows client. If the underlying file system is NSS and Novell Samba is installed, it can be managed using iManager.	DSfW supports access control at share level or at file system level. The access control can be managed at share level and file system level from a Windows client. If the underlying file system is NSS then it can be managed from iManager. It is recommended (but not required) that you create Samba shares on NSS data volumes in order to achieve this flexible dual access control.
Storage of security identities	Samba-3 stores security identities in local files. Whereas Novell SAMBA is integrated with eDirectory. This way it utilizes the power of eDirectory access control (trustee model) and data replication.	DSfW by default integrates SAMBA with eDirectory.
Password Policies	Supports NT domain type password policies.	Supports Active Directory domain password policies and existing eDirectory password policies.
Interoperability with Active Directory	SAMBA can be configured as a member server of the domain, but cannot be configured as domain controller.	With the help of cross-forest trust the users in DSfW environment will be able to access resources in Active Directory environment.

C.2 Understanding DSfW in Relation to IDM

IDM is a data sharing and synchronization service that enables applications, directories, and databases to share information. It links scattered information and enables you to establish policies that govern automatic updates to designated systems when identity changes occur. On the other hand DSfW allows Microsoft Windows users to work in a pure Windows desktop environment and still take advantage of some OES back-end services and technology, without the need for a Novell Client on the desktop.

The following table analyses the features of DSfW and IDM.

Table C-2   *DSfW and IDM*

Feature	IDM	DSfW
Purpose	Synchronization of user data and credentials between directory services and databases.	Allows existing eDirectory users or new DSfW users to access OES services as well as Microsoft Active Directory environment services with the help of trust.

Feature	IDM	DSfW
Storage of user data	Data is duplicated across directory services.	Data is stored in eDirectory, but the DSfW suite of services make it possible for the data to be accessed and retrieved from Active Directory environment.
Manageability	Can be managed from iManager.	DSfW can be managed from Microsoft MMC as well as eDirectory web management tools like iManager. So any Windows member server/client joined to the DSfW domain will be able to use the power of Active Directory which means share creation, assigning various access rights, managing users, trusts, group policies will be very much seamless. In DSfW the Samba-3 shares and access rights can be managed by eDirectory web based management i.e iManager.
Group Policy	No support for Group Policy.	Supports Group Policies. For more information, see Managing Group Policy Settings
Trusts	No concept of trusts. Data is duplicated and the access rights are evaluated on the local server.	Trusts are supported. This makes accessing inter-forest or inter-domain resources possible. Supports the following forms of trusts: ◆ External Trusts ◆ Forest Trusts ◆ Realm Trusts For more information see, Managing Trust Relationships in Domain Services for Windows

D 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 D-1 *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
NetBIOS Datagram Service	138/TCP, 138/UDP
NetBIOS Session Service	139/TCP, 139/UDP
Domain Service Daemon	8025/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 Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145 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.

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.

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 SP3 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 non-transitive 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.

3. Partition acts as a security boundary of a domain. Domain rules are valid till it encounters another partition boundary.

Provisioning. Provisioning is the process of configuring the services on a DSfW server. It is made up of a series of logical steps that execute in a predetermined order to complete the DSfW installation.

The provisioning tasks can be executed using the DSfW Provisioning Wizard or the command line scripts.

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.

Sysvol. The System Volume (Sysvol) is a shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain.

The Sysvol corresponds to the `/var/opt/novell/xad/sysvol/sysvol` directory on the domain controller.

Sysvolsync. The sysvolsync utility is introduced to provide synchronization of Sysvol and the underlying policies between the domain controllers of a domain.

This utility when invoked finds the domain controllers for the domain and initiates the synchronization process with them, contacting one domain controller at a time. During the synchronization only the changes are transferred and not the entire data.

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.

Subsequent Domain. A child domain for a domain that already exists. Organizations split the data into multiple domains to reduce administrative overhead.

Subsequent Domain Controller. An added server used to improve the availability and reliability of network services. If you have an subsequent domain controller, it helps in fault tolerance and balances the load of existing domain controllers. It also provides additional infrastructure support to the sites.

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.

E   Documentation Updates

This section contains information about documentation content changes made to the *OES 2: Novell Domain Services for Windows Administration Guide* since the initial release of Novell Open Enterprise Server 2.

September, 2011

Guide content revised to reflect support for SLES 10 SP4 as the base platform for OES 2 SP3.

July, 2010

- Added installation scenario Section 5.4, "Extending a Domain Boundary in a Name-Mapped Installation," on page 35.
- Added a new deployment scenario "Deploying DSfW by Skipping Containers" on page 27.
- Updated Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145 with information on modifying administrator details using MMC.
- Included support for Windows 2008 server to join DSfW domain as a member server in Chapter 2, "What's New," on page 17.
- Revised content of Section 7.5.4, "Add Domain Replica," on page 128.
- Added information about Restrictions with Domain Names.
- Updated the chapter Upgrading DSfW.

November 9, 2009

- Modified the contents of "Key Differences Between the DSfW LDAP Server and the eDirectory Server" on page 15 and converted it in form of a table to represent comparison.
- Included "What's New" on page 17 to capture additions to the Novell Domain Services for Windows (DSfW) service for the Novell Open Enterprise Server 2 SP2 Linux platform over the previous release.o
- Included new chapter on Use-Cases.
- Included new chapter on Deployment Scenarios.
- Included new chapter on Planning for DSfW
- Updated Installing Domain Services for Windows with information on integrated install.
- Included new chapter on Provisioning Domain Services for Windows.
- Updated Chapter 8, "Activities After DSfW Installation or Provisioning," on page 145 with steps to validate DSfW install.
- Updated Upgrading DSfW chapter with SP2-specific prerequisites and limitations.
- Included a chapter on Running Domain Services for Windows in a Virtualized Environment.

- Included Limitations in the Chapter 11, "Logging In from a Windows Workstation," on page 157.
- Included new chapter on Chapter 13, "Understanding DNS in Relation to DSfW," on page 169.
- Made the following changes in Chapter 14, "Managing Group Policy Settings," on page 175
  - Included details on "Editing an Existing Group Policy" on page 176
  - Included details on "Setting the DFS Referral of the Server Holding the PDC Emulator Role as Active on the Workstation" on page 177.
  - Updated Section 14.2.2, "gpo2nmas," on page 180
  - Included Section 14.3, "Sysvol," on page 180.
  - Updated Section 19.5, "Group Policy Management Issues," on page 246.
- Added Section 15.3, "Limitations with Cross-Forest Trust," on page 216 in Chapter 15, "Managing Trust Relationships in Domain Services for Windows," on page 183.
- Modified "Example: Assigning Rights to Folders on an NSS Volume" on page 222 in the Chapter 16, "Providing Access to Server Data," on page 217.
- Added Chapter 18, "Flexible Single Master Operation (FSMO) Roles," on page 229.
- Updated Chapter 19, "Troubleshooting," on page 235 chapter.
- Added the following Appendix files:
  - Appendix A, "Executing Provisioning Tasks Manually," on page 249
  - Appendix B, "Schema," on page 255
  - Appendix C, "Understanding DSfW in Relation to IDM and Samba," on page 263
  - Appendix D, "Network Ports Used by DSfW," on page 267
- Updated "Glossary" on page 269 with details on partition boundary, SYSVol and Provisioning.