opentext™

Open Enterprise Server 24.4
Domain Services for Windows Administration Guide

May 2025

Legal Notices

Copyright 2023 - 2025 Open Text

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

Contents

About This Guide 11

1 Overview of DSfW 13

1.1 Features and Benefits . . . 13
1.2 Architectural Overview . . . 15
1.3 Basic Directory Services Concepts . . . 16
1.3.1 Domains, Trees, and Forests . . . 16
1.3.2 Naming . . . 16
1.3.3 Security Model . . . 17
1.3.4 Groups . . . 17
1.4 Key Differences Between the DSfW LDAP Server and the eDirectory Server . . . 17

2 What's New or Changed in Domain Services for Windows 19

2.1 What's New or Changed in DSfW (OES 25.2) . . . 19
2.2 What's New or Changed in DSfW (OES 25.1) . . . 19
2.3 What's New or Changed in DSfW (OES 24.4) . . . 19

3 DSfW Interoperability with Third Party Software 21

3.1 OpenText Privileged Access Manager . . . 21
3.1.1 Overview . . . 21
3.1.2 Integration of PAM with DSfW . . . 22
3.2 Citrix Virtual Apps and Desktops . . . 23
3.2.1 Overview . . . 23
3.2.2 Architecture . . . 24
3.3 NetApp ONTAP Simulator . . . 24
3.4 NetIQ Advanced Authentication Framework Server . . . 25
3.5 OpenText Filr . . . 25
3.6 VMware . . . 25
3.6.1 Overview . . . 25
3.6.2 Architecture . . . 26

4 Use-Cases 27

4.1 Authenticating to Applications That Require Active Directory-Style Authentication . . . 27
4.1.1 Users Located in the DSfW Forest and Accessing Applications Hosted in the Active Directory Forest . . . 27
4.1.2 Users and Applications Hosted in the DSfW Forest . . . 28
4.2 Working With Windows Systems Without Client for Open Enterprise Server . . . 28
4.3 Leveraging an Existing eDirectory Setup . . . 29
4.4 Interoperability Between Active Directory and eDirectory . . . 29

5 Deployment Scenarios 31

5.1 Deploying DSfW in a Non-Name-Mapped Setup . . . 31

5.1.1 Deploying as a Single Domain . . . 31
5.1.2 Deploying as Multiple Domains in a Forest . . . 31
5.2 Deploying DSfW in a Name-Mapped Setup . . . 33
5.2.1 Deploying DSfW by Skipping Containers . . . 36
5.2.2 Custom Domain Name . . . 37

6 Planning for DSfW 39

6.1 Server Requirements for Installing DSfW . . . 39
6.2 Scalability Guidelines . . . 40
6.3 Deciding between Name-Mapped and Non-Name-Mapped Installation . . . 40
6.3.1 Impact of a Name Mapped / Non-Name-Mapped setup on a Tree . . . 42
6.4 Impact of Mixed Mode Configuration in a Forest or Domain . . . 43
6.5 Extending a Domain Boundary in a Name-Mapped Installation . . . 43
6.5.1 Prerequisite . . . 43
6.5.2 Use Case Scenario . . . 44
6.5.3 Caveat . . . 45
6.6 Meeting the Installation Requirements . . . 45
6.6.1 Installation Prerequisites For a Non-Name-Mapped Setup . . . 45
6.6.2 Installation Prerequisites for a Name-Mapped Setup . . . 48
6.7 Unsupported Service Combinations . . . 51
6.7.1 Installing Other Products in the DSfW Partition . . . 51
6.8 Operating System Version Support . . . 52
6.9 Client for Open Enterprise Server and Windows Co-existence . . . 53
6.10 Administrative Tools . . . 53
6.10.1 Windows Administration Tools . . . 53
6.10.2 Linux Administration Tools . . . 53
6.11 Utilities Not Supported in DSfW . . . 53
6.12 Limitations . . . 53
6.12.1 Hostname . . . 54
6.12.2 NetBIOS Names . . . 54
6.12.3 Installation Issue . . . 54
6.13 Restrictions with Domain Names . . . 54
6.13.1 DSfW Does Not Support Domain Names Ending with *.local . . . 54
6.13.2 DSfW Does Not Support A Single-Label Domain Name . . . 54
6.14 Supported Special Characters in DSfW Passwords . . . 55
6.15 Enabling Universal Password Policy for DSfW . . . 55
6.16 Ensuring Filesystem ACL Support . . . 55

7 Installing Domain Services for Windows 57

7.1 Installing and Configuring DSfW Using the YaST Administrative Tool . . . 57
7.1.1 Prerequisites for Installation . . . 57
7.1.2 Installation Scenarios . . . 57
7.1.3 Express Installation . . . 70
7.1.4 Using a Container Admin to Install and Configure DSfW . . . 70
7.2 Installing DSfW Using AutoYaST . . . 71
7.2.1 Prerequisites . . . 72
7.2.2 Installing DSfW . . . 72
7.2.3 Modifying Template Files . . . 72

8 Provisioning Domain Services for Windows 79

8.1 What Is Provisioning? . . . 79
8.2 Features and Capabilities of the Provisioning Wizard . . . 79
8.3 Provisioning Wizard Interface . . . 80
8.4 Using the Wizard to Provision the DSfW Server . . . 82
8.5 Provisioning Tasks . . . 83
8.5.1 Provisioning Precheck . . . 84
8.5.2 Configure DNS . . . 84
8.5.3 Configure DNS and WINS . . . 85
8.5.4 Create Domain Partition . . . 85
8.5.5 Add Domain Replica . . . 86
8.5.6 Configure SLAPI Plug-Ins . . . 86
8.5.7 Add Domain Objects . . . 86
8.5.8 Create Configuration Partition . . . 86
8.5.9 Create Schema Partition . . . 86
8.5.10 Add Configuration Objects . . . 87
8.5.11 Add Domain Controller . . . 87
8.5.12 Assign Rights . . . 87
8.5.13 Samify Objects . . . 87
8.5.14 Configure Site . . . 87
8.5.15 Restart DSfW Services . . . 88
8.5.16 Set Credentials for Accounts . . . 88
8.5.17 Enable Kerberos . . . 88
8.5.18 Establish Trust . . . 88
8.5.19 Cleanup . . . 89
8.6 Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios . . . 89
8.7 Logging . . . 92
8.8 Troubleshooting . . . 93
8.8.1 Troubleshooting Provisioning Tasks . . . 93
8.9 Executing Provisioning Tasks Manually . . . 101
8.9.1 Exporting Passwords . . . 101
8.9.2 Provisioning Tasks . . . 102

9 Types of Accounts in DSfW 109

10 Activities After DSfW Installation or Provisioning 111

10.1 Verifying the Installation . . . 111
10.2 Renaming Administrator Details Using MMC . . . 113
10.3 Extending the Domain Post Provisioning . . . 113
10.3.1 Examples . . . 115
10.4 Updating the Domain Functional Level and Forest Functional Level . . . 116
10.5 Validating the Schema Update . . . 116
10.6 Validating Domain and Forest Functional Level . . . 117

11 Upgrading DSfW 119

11.1 Upgrading DSfW to OES 24.4 . . . 119
11.1.1 Upgrade Scenario . . . 119
11.1.2 Prerequisite . . . 119
11.1.3 Media Upgrade . . . 120
11.1.4 AutoYaST Upgrade . . . 120

11.1.5 Configuring WINS and Sites in an Upgrade Scenario 120
11.1.6 Troubleshooting 121
11.2 Migrating Data to a Domain Services for Windows Server 121

12 Activities After Upgrade or Migration 123

12.1 Updating the Domain Functional Level and Forest Functional Level 123
12.2 Validating the Schema Update 123
12.3 Validating Domain and Forest Functional Level 124

13 Running Domain Services for Windows in a Virtualized Environment 125

14 Logging In from a Windows Workstation 127

14.1 Joining a Windows Workstation to a DSfW Domain 127
14.2 Logging In to a DSfW Domain 130
14.3 Logging Out 130
14.4 Support for SASL NTLMSSP Bind in LDAP 131
14.4.1 Planning for Support of SASL NTLMSSP Bind in LDAP 131
14.4.2 Troubleshooting 131

15 Creating Users 133

15.1 Creating Users in iManager 133
15.2 Creating Users in MMC 134
15.3 Creating Filr LDAP Proxy Users 135
15.4 Moving Users Associated with Password Policies 136
15.5 Limitations 136
15.5.1 User Samification Fails On Moving Users into a DSfW Domain 136
15.5.2 Moving User Objects Across Containers 136
15.5.3 Primary Group Appears Twice in the memberOf Properties Page 137
15.5.4 Adding Newly Created Users to a Group gives Error Message 137
15.5.5 Dynamic Groups Is Not Supported in DSfW 137

16 Understanding DNS in Relation to DSfW 139

16.1 DSfW and DNS 139
16.1.1 Limitations 140
16.2 Understanding DNS Settings in the DSfW Environment 140
16.2.1 General DNS Settings 140
16.2.2 Configuring a Domain Controller as a Primary DNS Server 141
16.2.3 Configuring a Domain Controller by Using an Existing DNS Server 141
16.3 Setting Up a Windows DNS Server for DSfW 141
16.4 Migrating DNS to Another Domain Controller 142
16.5 Restarting DNS 143

17 Understanding AES Encryption for Communication 145

18 Configuring DSfW Server as a WINS Server 147

18.1 Using WINS in DSfW Environment 147

18.1.1 Planning for WINS Support . . . 148
18.1.2 Configuring WINS Server and Client . . . 148
18.1.3 Migrating WINS Server . . . 149
18.1.4 Caveats . . . 149
18.2 Rectifying Duplicate Workstation Names . . . 150
18.3 Verifying Duplicate Workstation Names Prior to WINS Configuration . . . 152
18.4 Troubleshooting . . . 152
18.4.1 WINS Server Does not Report Duplicate Workstation Name . . . 152

19 Managing Group Policy and Fine-Grained Password Policy Settings 153

19.1 Configuring Group Policies . . . 153
19.2 Configuring Fine-Grained Password Policy . . . 156
19.2.1 Restrictions . . . 156
19.2.2 Creating the Fine-Grained Password Policy . . . 157
19.2.3 Setting the Password Policy on the User . . . 158
19.3 Group Policy Objects . . . 158
19.3.1 GPO Account Policies . . . 158
19.3.2 gposync . . . 160
19.3.3 Enforcing Computer Configuration and User Configuration . . . 160
19.3.4 Troubleshooting . . . 160
19.4 Sysvol . . . 161
19.4.1 sysvolsync Utility . . . 161
19.5 Limitations with Group Policy Management . . . 162
19.5.1 Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition . . . 162
19.5.2 Members of GroupPolicy Creator Owner group cannot change the active DFS Referral . . . 162
19.5.3 Ignore Warnings while Backing up Group Policies . . . 162
19.5.4 WMI Filters Cannot be Applied for Processing GPOs . . . 162

20 Managing Trust Relationships in Domain Services for Windows 163

20.1 What is a Trust? . . . 163
20.2 Cross-Forest Trust Relationships . . . 164
20.2.1 Creating a Cross-forest Trust between Active Directory and Domain Services for Windows Forests . . . 164
20.2.2 Creating a Cross-forest Trust between two Domain Services for Windows Forests . . . 170
20.2.3 Shortcut Trusts . . . 172
20.3 Limitations with Cross-Forest Trust . . . 173

21 NSS Volume Access by DSfW and Active Directory Users 175

21.1 Configuring NSS AD and DSfW in the same tree . . . 175

22 Providing Access to Server Data 177

22.1 Accessing Files by Using Native Windows Methods . . . 177
22.1.1 Prerequisites . . . 177
22.1.2 Samba: A Key Component of DSfW . . . 177
22.1.3 Samba in the DSfW Environment . . . 178
22.1.4 Creating Samba Shares in iManager . . . 178
22.1.5 Creating Samba Shares in the smb.conf File . . . 179

22.1.6 Assigning Rights to Samba Shares . . . 180
22.1.7 Adding a Network Place . . . 181
22.1.8 Adding a Web Folder . . . 182
22.1.9 Mapping Drives to Shares . . . 182
22.2 Accessing Files by Using the Client for Open Enterprise Server . . . 183
22.3 Accessing Files in Another Domain . . . 183

23 Printing in the Domain Services for Windows Environment 185

23.1 Setting Up iPrint . . . 185
23.2 Special Handling for iPrint on DSfW . . . 185
23.2.1 Secure and Non-Secure Printing . . . 185
23.2.2 Using a Common Driver Store in a DSfW partition . . . 186
23.3 iPrint Clustering in a DSfW Environment . . . 186
23.3.1 iPrint Clustering on NSS Clusters . . . 186

24 Flexible Single Master Operation (FSMO) Roles 187

24.1 FSMO Roles and Limitations . . . 187
24.1.1 RID Master . . . 187
24.1.2 PDC Emulator Master . . . 187
24.1.3 Infrastructure Master . . . 188
24.1.4 Schema Master . . . 188
24.1.5 Domain Master . . . 188
24.2 Transferring and Seizing FSMO Roles . . . 188
24.2.1 To Transfer the PDC Emulator Role from the First Domain Controller to an additional domain controller . . . 189
24.2.2 To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Functional) . . . 189
24.2.3 To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Not Functional) . . . 190
24.2.4 Transferring the ADPH Master Role to Other Domain Controllers . . . 190

25 Troubleshooting 193

25.1 Troubleshooting DSfW . . . 193
25.1.1 Logging In from a Workstation - Issues . . . 195
25.1.2 Unable to Add msDs-PrincipalName and Create Password Settings Container During Upgrade . . . 197
25.1.3 No Immediate Effect of the Applied Fine-Grained Password Policy . . . 197
25.1.4 MMC Fails to Display the “Properties” Option for Multiple Selected Users . . . 198
25.1.5 Remote Desktop License Server Cannot Update the License Attributes . . . 198
25.1.6 Editing GPO for Windows Server 2012 R2 Member Server Might Result in an Error . . . 199
25.1.7 The wbinfo Operation for winbind Daemon Fails if two IP Interfaces are Present in a Domain Controller . . . 199
25.1.8 DSfW Provisioning Fails When you Configure an Additional Domain Controller to an Existing Child Domain . . . 199
25.1.9 Error During DSfW Provisioning . . . 200
25.1.10 User Moved out of DSfW Domain is able to Access to DSfW Service . . . 200
25.1.11 Rename of User Object Using iManager Fails to Update the samAccountName and userPrincipalName . . . 201

25.1.12 Windows Password Synchronization Fails With DSfW Domain Users for Windows XP Clients 201
25.1.13 Workstation Login Fails With Samba Error 201
25.1.14 On a Non-DSfW Server, eDirectory Restart Results in an Error Message. 202
25.1.15 ADC Install Enters Wrong Context for Server 202
25.1.16 DSfW Fails to Set Up Signed NTP for Clients to Trust 202
25.1.17 Unable to Proceed with Installation of an Additional Domain Controller 203
25.1.18 Unable to Access Sysvol 203
25.1.19 Reverse Zone Record for Workstations Joined to CDC and ADC is Not Getting Updated 203
25.1.20 DSfW Provisioning Wizard Might Hang During the Restart DSfW Services Phase. 204
25.1.21 Citrix Xenserver Fails to Join a DSfW Domain. 204
25.1.22 Changing the User Password Requires Reimport of Third-Party Application Certificates 204
25.1.23 Administrative Templates in the Computer Configuration and User Configuration Are Empty 204
25.1.24 SLED or SLES Workstation Join to DSfW Triggers Traces in the log.smbd File 205
25.1.25 Extending the DSfW Object Classes with Mandatory Attributes Leads to Object Creation Failure in MMC 205
25.1.26 Kinit Not Working for Users 206
25.1.27 Cleanup Task Fails in Name Mapped Scenarios 206
25.1.28 MMC Fails to Create Users 206
25.1.29 Using DSfW Server as a WINS Server Results in an Error 206
25.1.30 iManager Fails to Create Samba Shares if the Administrator Name is Changed using MMC 207
25.1.31 If Administrator and Default Group Objects are Accidentally Deleted 207
25.1.32 Tree Admin is Not Automatically Granted Rights for DSfW Administration 208
25.1.33 DSfW Services Stop Working if the Concurrent LDAP Bind Limit is Set to 1 208
25.1.34 The Provision Utility Succeeds Only With the *--locate-dc* Option 208
25.1.35 Users Are Not Samified When the RID Master Role is Seized 208
25.1.36 Shared Volumes Are Not Accessible 209
25.1.37 Requirements for Samba/CIFS Access to NSS volumes via DSfW 209
25.1.38 Identifying novell-named Error 210
25.1.39 Login Failure 210
25.1.40 Unable to Connect to Legacy Applications 210
25.1.41 User in a Domain Can Access Resources from Another Domain by Using the UID of the Foreign User 211
25.1.42 Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition. 211
25.1.43 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 211
25.1.44 Child Domains Slow Down When the First Domain Controller is Not Functional 211
25.1.45 Error Mapping SID to UID. 211
25.1.46 After DSfW Installation, the Services are Not Working 212
25.1.47 Configuring eDirectory on a Non-Default Port Affects the Installation of DSfW in a Name-Mapped Scenario 212
25.1.48 Issues in Using iManager and MMC Interchangeably to Add Users in a Mixed OES (non-DSfW) and DSfW Environment 212
25.2 Error Messages in Log Files 212
25.2.1 ndsd Log File Error 212
25.3 Novell SecureLogin Issues 213
25.3.1 Novell SecureLogin LDAP Attribute Mappings 213
25.4 Known Issues 213
25.4.1 Cannot Configure UMC on DSfW Server 213

25.4.2 Cannot Create Samba Shares . . . 213
25.4.3 Warning Message Appears on ADC Installation . . . 214
25.4.4 Limitation for Number of Characters in Login Username . . . 214
25.4.5 Creating Filr LDAP Proxy Users with MMC Fails . . . 214
25.4.6 Domain Join with NetBIOS Name Fails . . . 214
25.4.7 NTLM Authentication Fails Over SSP . . . 214
25.4.8 Provisioning Fails for a New DC in the Forest When PDC is Not a DNS Server after PDC Role Transfer . . . 214
25.4.9 Password Setting Container Might Not Be Visible On Domain Controllers In A Mixed Mode Environment . . . 215
25.4.10 Restriction on Fine-Grained password Policy Attribute Name Length . . . 215
25.4.11 Fine-Grained Password Policy Limitations . . . 215
25.4.12 Copying a User Object from MMC Fails . . . 215
25.4.13 Users Must Change Their Own Passwords . . . 215

A Schema 217

A.1 Schema Objects . . . 217
A.1.1 Syntaxes . . . 220
A.1.2 Attribute Mappings . . . 221
A.1.3 Special Attributes . . . 222
A.1.4 Class Mappings . . . 224
A.2 Extending the Third-Party Schema using Traditional Methods . . . 225
A.3 Extending the Third-Party Schema using Microsoft Active Directory Standard Methods . . . 225
A.3.1 Manual Extension using the LDIFDE Tool . . . 225
A.3.2 Programmatic Extension . . . 227
A.4 Adding an Attribute to Partial Attribute Set (PAS) . . . 228

B Understanding DSfW in Relation to IDM and Samba 229

B.1 Understanding DSfW in Relation to Samba . . . 229
B.2 Understanding DSfW in Relation to IDM . . . 231

C Network Ports Used by DSfW 233

D DSfW Password Policy Attributes 235

Glossary 237

26 Configuring Sites and Subnets 241

26.1 Planning for Sites and Subnets Support . . . 242
26.2 Managing Sites and Subnets . . . 242
26.3 Troubleshooting . . . 242
26.3.1 Moving a DSfW Server to a Site Results in an Error Message . . . 242

About This Guide

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

This guide is divided into the following sections:

- Chapter 1, “Overview of DSfW,” on page 13
- Chapter 2, “What’s New or Changed in Domain Services for Windows,” on page 19
- Chapter 3, “DSfW Interoperability with Third Party Software,” on page 21
- Chapter 4, “Use-Cases,” on page 27
- Chapter 5, “Deployment Scenarios,” on page 31
- Chapter 6, “Planning for DSfW,” on page 39
- Chapter 7, “Installing Domain Services for Windows,” on page 57
- Chapter 8, “Provisioning Domain Services for Windows,” on page 79
- Chapter 9, “Types of Accounts in DSfW,” on page 109
- Chapter 10, “Activities After DSfW Installation or Provisioning,” on page 111
- Chapter 11, “Upgrading DSfW,” on page 119
- Chapter 12, “Activities After Upgrade or Migration,” on page 123
- Chapter 13, “Running Domain Services for Windows in a Virtualized Environment,” on page 125
- Chapter 14, “Logging In from a Windows Workstation,” on page 127
- Chapter 15, “Creating Users,” on page 133
- Chapter 16, “Understanding DNS in Relation to DSfW,” on page 139
- Chapter 17, “Understanding AES Encryption for Communication,” on page 145
- Chapter 18, “Configuring DSfW Server as a WINS Server,” on page 147
- Chapter 19, “Managing Group Policy and Fine-Grained Password Policy Settings,” on page 153
- Chapter 20, “Managing Trust Relationships in Domain Services for Windows,” on page 163
- Chapter 21, “NSS Volume Access by DSfW and Active Directory Users,” on page 175
- Chapter 22, “Providing Access to Server Data,” on page 177
- Chapter 23, “Printing in the Domain Services for Windows Environment,” on page 185
- Chapter 24, “Flexible Single Master Operation (FSMO) Roles,” on page 187
- Chapter 25, “Troubleshooting,” on page 193
- Appendix A, “Schema,” on page 217
- Appendix B, “Understanding DSfW in Relation to IDM and Samba,” on page 229
- Appendix C, “Network Ports Used by DSfW,” on page 233
- Appendix D, “DSfW Password Policy Attributes,” on page 235

- “Glossary” on page 237
- Chapter 26, “Configuring Sites and Subnets,” on page 241

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 `comment on this topic` feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Domain Services for Windows Administration Guide*, see the latest Open Enterprise Server 24.4 documentation (https://www.microfocus.com/documentation/open-enterprise-server/24.4/).

Additional Documentation

For information about security issues and recommendations for Domain Services for Windows see *OES 23.4: OES Domain Services for Windows Security Guide* (https://www.microfocus.com/documentation/open-enterprise-server/24.4/).

For online community resources, and tips and tricks, see (http://www.dsfwdude.com).

1 Overview of DSfW

Domain Services for Windows (DSfW) is a suite of technologies in Open Enterprise Server that allows Microsoft Windows users to access OES services through native Windows and Active Directory protocols. By allowing OES servers to behave as if they were Active Directory servers, this technology enables companies with Active Directory and NetIQ 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 Client for Open Enterprise Server on the desktop.

Administrators can use either 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 / DSfW servers by using iManager.

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

Users can access 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 and later.

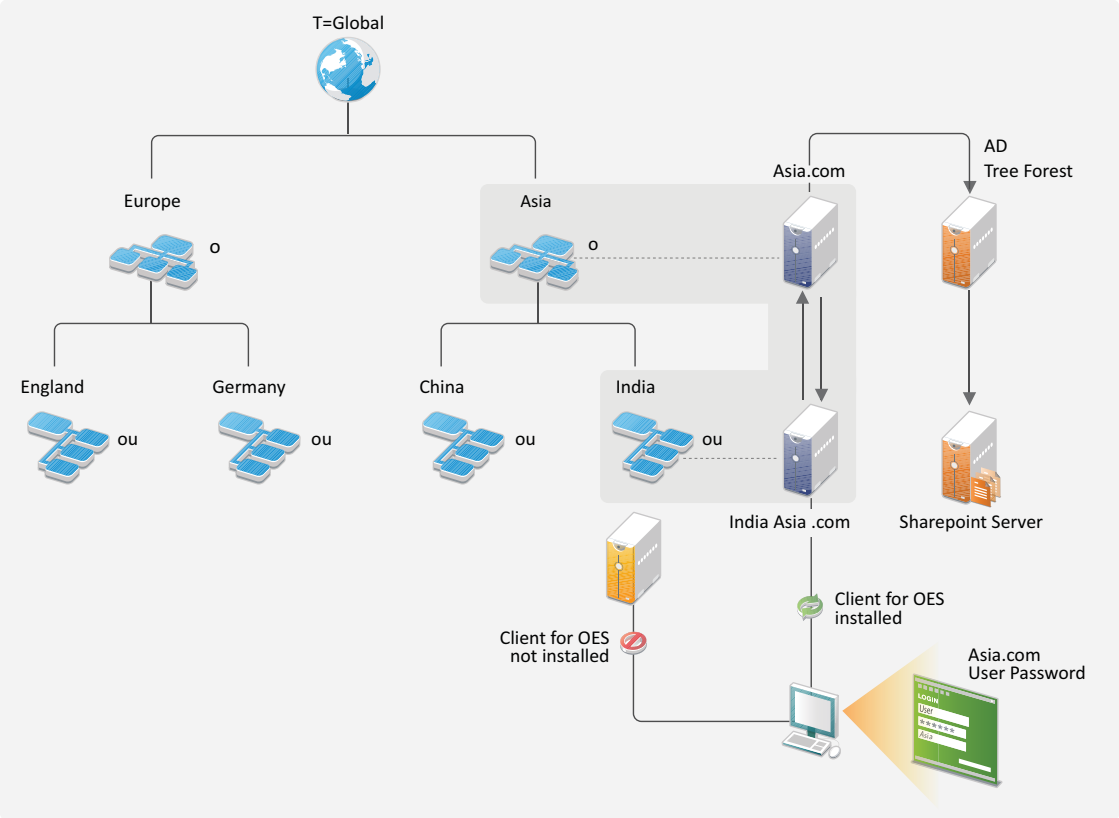
- Section 1.1, “Features and Benefits,” on page 13
- Section 1.2, “Architectural Overview,” on page 15
- Section 1.3, “Basic Directory Services Concepts,” on page 16
- Section 1.4, “Key Differences Between the DSfW LDAP Server and the eDirectory Server,” on page 17

1.1 Features and Benefits

DSfW is designed to simplify the network infrastructure in mixed Windows/OES 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 OpenText 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:

Figure 1-1 *Overview of DSfW*



- **Clientless login and cross-platform file access for Windows users:** From a standard Windows workstation, users can authenticate to an OES server running eDirectory without the need for the Client for Open Enterprise Server 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 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 (Windows 2003, Windows 2008 R2, Windows 2012 R2, Windows 2016) 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 and Microsoft Management Console (MMC) for Windows, thus eliminating the need for re-training.

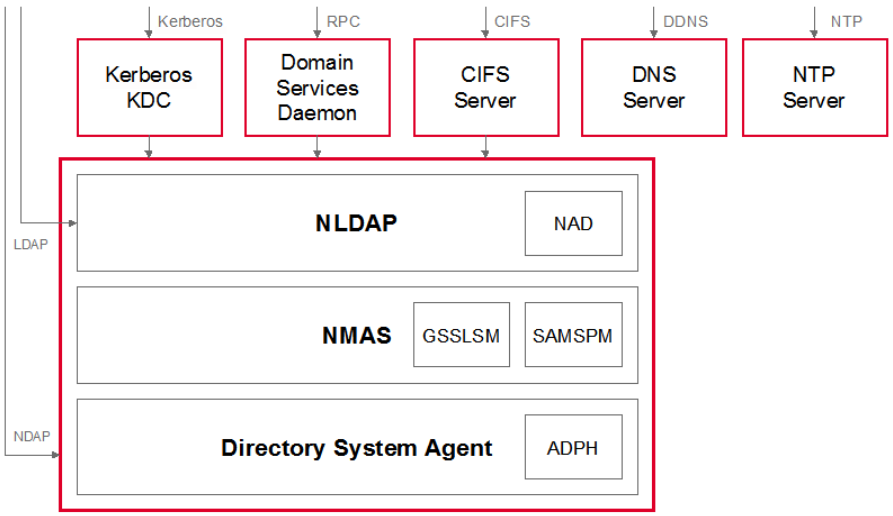
  Network administrators can manage file systems using the native tools of each server, as well as centrally administer Samba shares on OES /DSfW servers using iManager. Administrators can use MMC to create one-way cross-forest trusts between DSfW domains and Active Directory domains. For example, Windows 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 1-2 illustrates the components included in DSfW and how they interact.

Figure 1-2 *DSfW Components*



DSfW is made up of the following technologies:

- **eDirectory:** eDirectory 8.8 SP2 and later 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 software included with OES DSfW.
- **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 16
- Section 1.3.2, “Naming,” on page 16
- Section 1.3.3, “Security Model,” on page 17
- Section 1.3.4, “Groups,” on page 17

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.

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.

Function	DSfW LDAP Server	eDirectory Server
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
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 or Changed in Domain Services for Windows

- Section 2.1, "What's New or Changed in DSfW (OES 25.2)," on page 19
- Section 2.2, "What's New or Changed in DSfW (OES 25.1)," on page 19
- Section 2.3, "What's New or Changed in DSfW (OES 24.4)," on page 19

2.1 What's New or Changed in DSfW (OES 25.2)

Extending the Third-Party Schema using Microsoft Active Directory Standard Methods

Extend the schema for a DSfW server using standard Microsoft Active Directory mechanisms, either by manually applying LDIF files with the LDIFDE utility or by programmatically invoking directory service interfaces.

For more information, see Appendix A, "Schema," on page 217.

DSfW Interoperability with Third Party Software

Every release, the versions of third-party software that DSfW supports are verified. For more information, see Chapter 3, "DSfW Interoperability with Third Party Software," on page 21.

2.2 What's New or Changed in DSfW (OES 25.1)

DSfW Interoperability with Third Party Software

Every release, the versions of third-party software that DSfW supports are verified. For more information, see Chapter 3, "DSfW Interoperability with Third Party Software," on page 21.

2.3 What's New or Changed in DSfW (OES 24.4)

DSfW Interoperability with Third Party Software

Every release, the versions of third-party software that DSfW supports are verified. For more information, see Chapter 3, "DSfW Interoperability with Third Party Software," on page 21.

3 DSfW Interoperability with Third Party Software

This section helps you understand DSfW functionality with third-party software.

- Section 3.1, “OpenText Privileged Access Manager,” on page 21
- Section 3.2, “Citrix Virtual Apps and Desktops,” on page 23
- Section 3.3, “NetApp ONTAP Simulator,” on page 24
- Section 3.4, “NetIQ Advanced Authentication Framework Server,” on page 25
- Section 3.5, “OpenText Filr,” on page 25
- Section 3.6, “VMware,” on page 25

The following table lists the version of third-party softwares that are validated with DSfW:

Table 3-1 *Third-party validated versions*

DSfW Interoperability	Validated Version
OpenText Privileged Access Manager	4.5
Citrix Virtual Apps and Desktops	7 2305
NetApp ONTAP Simulator	9.12.1
NetIQ Advanced Authentication Framework Server	6.4.1.1
OpenText Filr	23.3
VMware	8.9.0-21593375

3.1 OpenText Privileged Access Manager

- Section 3.1.1, “Overview,” on page 21
- Section 3.1.2, “Integration of PAM with DSfW,” on page 22

3.1.1 Overview

Privileged Access Manager (PAM) helps an organization to protect its critical assets and maintain the compliance requirements by securing, managing, and monitoring privileged accounts for privileged access. It is capable of managing the shared accounts and also auditing those accounts. You can monitor all the actions performed in the servers for Windows, Linux, database, or any application such as, LDAP.

NetIQ Privileged Account Manager version **4.5** has been validated with DSfW version **24.4**.

For more information about OpenText Privileged Account Manager, see PAM Documentation (https://www.netiq.com/documentation/privileged-access-manager-45/).

NOTE: The NetIQ Privileged Account Manager has been renamed to OpenText Privileged Access Manager.

3.1.2 Integration of PAM with DSfW

- "Prerequisites" on page 22
- "Procedure" on page 22

Prerequisites

Download the following files from the NetIQ Downloads website (https://dl.netiq.com/index.jsp?product_id=5969):

- **PAM Manager**: `netiq-npam-manager-4.5.0-linux-3.0-x86_64.rpm`
- **Agentless Package**: `agentless-4-5-linux-x86_64-3.0.pak`

For more information, see Planning Your Privileged Access Manager Installation (https://www.netiq.com/documentation/privileged-access-manager-45/npam_install/data/bjjp4a8.html).

Procedure

1. Install Privileged Access Manager on the target system.
2. Using the command line, publish the package to the Package Manager.

   ```
   /opt/netiq/npum/sbin/unifi -u <username> -p <password> distrib publish
   -f <package>
   ```

   For more information about the command to publish packages to the package manager, see Package Distribution Options (https://www.netiq.com/documentation/privileged-access-manager-45/npam_admin/data/bm25zob.html).
3. Login to the `Legacy PAM Console` (https://<*ipaddress*>) and install the Agentless package (`agentless-4-5-linux-x86_64-3.0.pak`). See Installing Host Packages (https://www.netiq.com/documentation/privileged-access-manager-45/npam_admin/data/hosts_pkgs_install.html).
4. Login to the `New PAM Console` (https://<*ipaddress*/pam>).
   - **4a** Configure the DSfW server as an LDAP server. See Configuring LDAP Server Settings (https://www.netiq.com/documentation/privileged-access-manager-45/npam_admin/data/t4e4qyfkbp0g.html).
   - **4b** After adding DSfW as an LDAP server, log out as a PAM user and re-login as a DSfW domain user. This step confirms that domain user login is successful using the DSfW server as an LDAP server.

     NOTE: If the validation fails, review the log files and LDAP server configuration (Step 4a on page 22).

4c Configure **Linux Agentless Web SSH** and **Windows Agentless Web RDP**. See Agent and Agentless Capability (https://www.netiq.com/documentation/privileged-account-manager-44/npam_admin/data/t4dz7jk29x7n.html).

4d (*Optional*) View the logs and service files.

- Log Location: `/opt/netiq/npum/logs/unifid.log`
- Service status: `/etc/init.d/npum status`

For more information related to installing and removing the Framework Manager, see Installing the Framework Manager (https://www.netiq.com/documentation/privileged-account-manager-44/npam_install/data/bjh3j6x.html).

3.2 Citrix Virtual Apps and Desktops

- Section 3.2.1, “Overview,” on page 23
- Section 3.2.2, “Architecture,” on page 24

3.2.1 Overview

Citrix Virtual Apps and Desktops are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

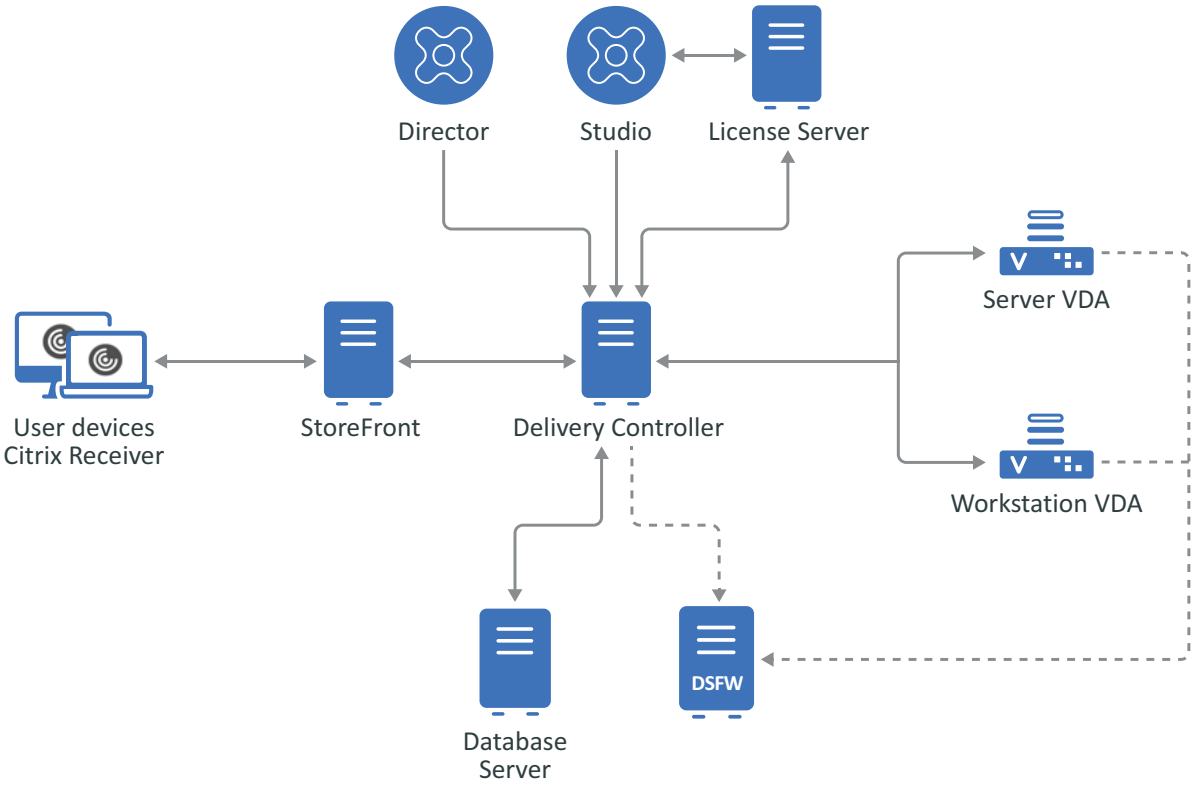
Citrix Virtual Apps and Desktops allow:

- End users to run applications and desktops independently of the device’s operating system and interface.
- Administrators to manage the network and control access from selected devices or from all devices.
- Administrators to manage an entire network from a single data center.

For more information about Citrix Virtual Apps and Desktops, see *Citrix Documentation*.

3.2.2 Architecture

Figure 3-1 *DSfW Interoperability with Citrix Virtual Apps and Desktops*



The integration of DSfW with Citrix Virtual Apps and Desktops enables DSfW users to access virtual applications and desktops that is created based on the rights assigned by the administrator.

For the integration, Citrix components such as Delivery Controller, Virtual Delivery Agent (VDA), and StoreFront must be joined to DSfW domain. For deployment, you can use Citrix Xen hypervisor, VMWare hypervisor, or the combination of both hypervisors.

Citirix Virtual Apps and Desktops **7 2305** has been validated with OES **23.4**

3.3 NetApp ONTAP Simulator

NetApp ONTAP is a powerful storage-software tool with capabilities such as an intuitive GUI, REST APIs with automation integration, AI-informed predictive analytics and corrective action, non-disruptive hardware upgrades, and cross-storage import.

NetApp ONTAP Simulator **9.12.1** has been validated with DSfW.

For more information about the NetApp ONTAP storage system, see *NetApp ONTAP*.

3.4 NetIQ Advanced Authentication Framework Server

Advanced Authentication™ is a multi-factor authentication solution that goes beyond the typical username-and-password-based authentication, enabling you to protect your IT infrastructure and sensitive data more effectively and securely. Advanced Authentication allows you to authenticate on diverse platforms using various devices and methods such as Fingerprint, Card readers, Facial Recognition, and One-Time Passwords (OTP). In addition, Advanced Authentication's authentication framework is both comprehensive and intuitive, ensuring secure access to all your devices while minimizing administrative overhead.

NetIQ Advanced Authentication Framework Server version **6.4.1.1** has been validated with DSfW using methods: LDAP password, secondary password, Email OTP, SMS OTP and security questions.

For more information about the NetIQ Advanced Authentication, see NetIQ Documentation (https://www.netiq.com/documentation/advanced-authentication-64/).

3.5 OpenText Filr

OpenText Filr provides file access and sharing, and lets users access their home directories and network folders from desktops, mobile devices, and the Web. Users can also synchronize their files to their PC or Mac. Changes that they make to downloaded copies are kept in sync with the originals on their network file servers. And finally, users can also share files internally and externally, and those with the share can collaborate with each other by commenting on the files.

Filr version **23.3** has been validated with DSfW.

For more information about Filr, see Filr Documentation (https://www.microfocus.com/documentation/filr/filr-23.2/).

3.6 VMware

- Section 3.6.1, "Overview," on page 25
- Section 3.6.2, "Architecture," on page 26

3.6.1 Overview

VMware vSphere is VMware's virtualization platform, which transforms data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. vSphere manages these infrastructures as a unified operating environment, and provides you with the tools to administer the data centers that participate in that environment.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources. For more information about VMware vSphere, see *VMware vSphere Documentation*.

VMware Horizon provides centralized desktops and apps which ensure strong security with no data residing on the device, streamlined patching, complete access control, and the delivery of trusted images every time. For more information about VMware Horizon, see *VMware Horizon Documentation*.

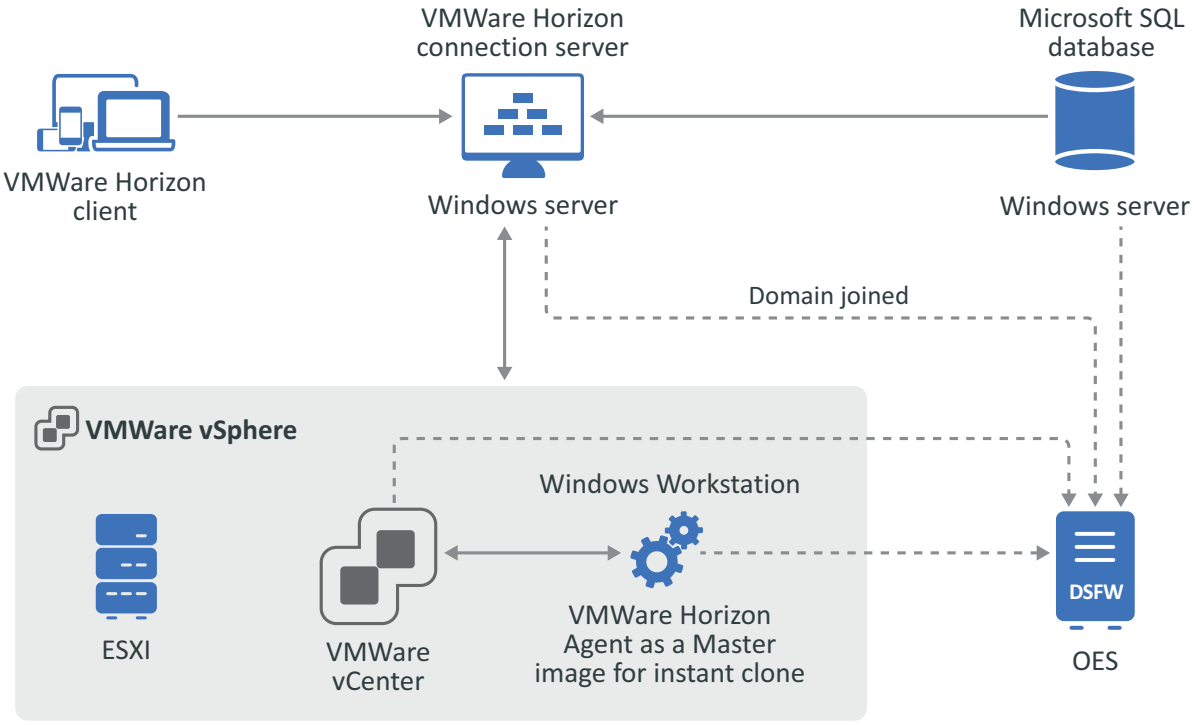
A full clone is a complete and independent copy of a virtual machine. A full clone shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is separate from the parent virtual machine.

Because a full clone duplicates only the state of the virtual machine at the instant of the cloning operation, it does not have access to snapshots of the parent virtual machine.

For more information about Full Clones, see *VMware Fusion Documentation*.

3.6.2 Architecture

Figure 3-2 *DSfW Interoperability with VMWare*



The integration of DSfW with VMware enables DSfW users to access full clones that is created based on the rights assigned by the administrator.

For the integration of DSfW with VMware, VMware components such as VMware Horizon connection server, database, and golden image were joined to DSfW domain. Pointed vCenter to DNS of DSfW domain and added compatible ESXi as a host in vCenter for the cloning.

The integration is tested and verified using OES **23.4** with VMware Horizon **8.9.0-21593375**, vCenter **7.0.0.10100**, and ESXi **7.0.3**.

For more information, see Domain Services for Windows (DSfW) integration with VMware.

4 Use-Cases

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

- Section 4.1, “Authenticating to Applications That Require Active Directory-Style Authentication,” on page 27
- Section 4.2, “Working With Windows Systems Without Client for Open Enterprise Server,” on page 28
- Section 4.3, “Leveraging an Existing eDirectory Setup,” on page 29
- Section 4.4, “Interoperability Between Active Directory and eDirectory,” on page 29

4.1 Authenticating to Applications That Require Active Directory-Style Authentication

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

- Section 4.1.1, “Users Located in the DSfW Forest and Accessing Applications Hosted in the Active Directory Forest,” on page 27
- Section 4.1.2, “Users and Applications Hosted in the DSfW Forest,” on page 28

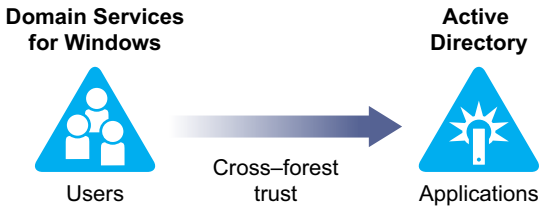
4.1.1 Users Located in the DSfW Forest and Accessing Applications Hosted in the Active Directory Forest

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 4-1 *DSfW users Accessing Resources on Active Directory*



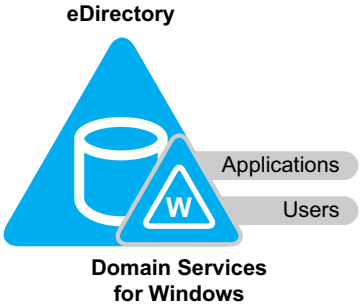
4.1.2 Users and Applications Hosted in the DSfW Forest

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 4-2 *Users and Applications in DSfW Forest*



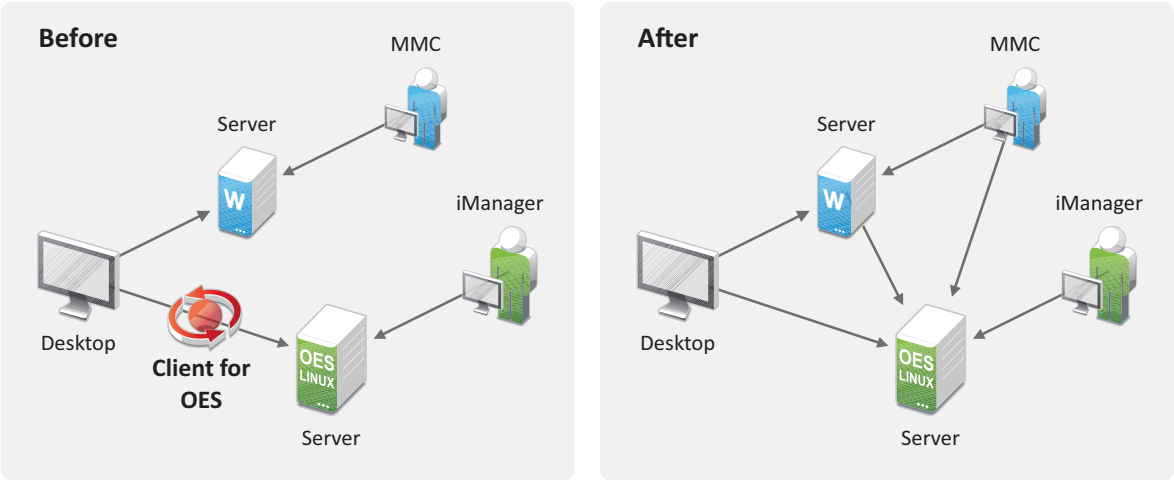
4.2 Working With Windows Systems Without Client for Open Enterprise Server

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 Client for Open Enterprise Server on the desktop.

Administrators can either use 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 /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 OES Storage Services (NSS) file system. Client for Open Enterprise Server 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 4-3 *Accessing applications without Client for Open Enterprise Server*



4.3 Leveraging an Existing eDirectory Setup

If you already have an eDirectory setup but want to install DSfW in your environment, it is recommended you utilize 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 6.6.2, “Installation Prerequisites for a Name-Mapped Setup,” on page 48 and Section 5.2, “Deploying DSfW in a Name-Mapped Setup,” on page 33

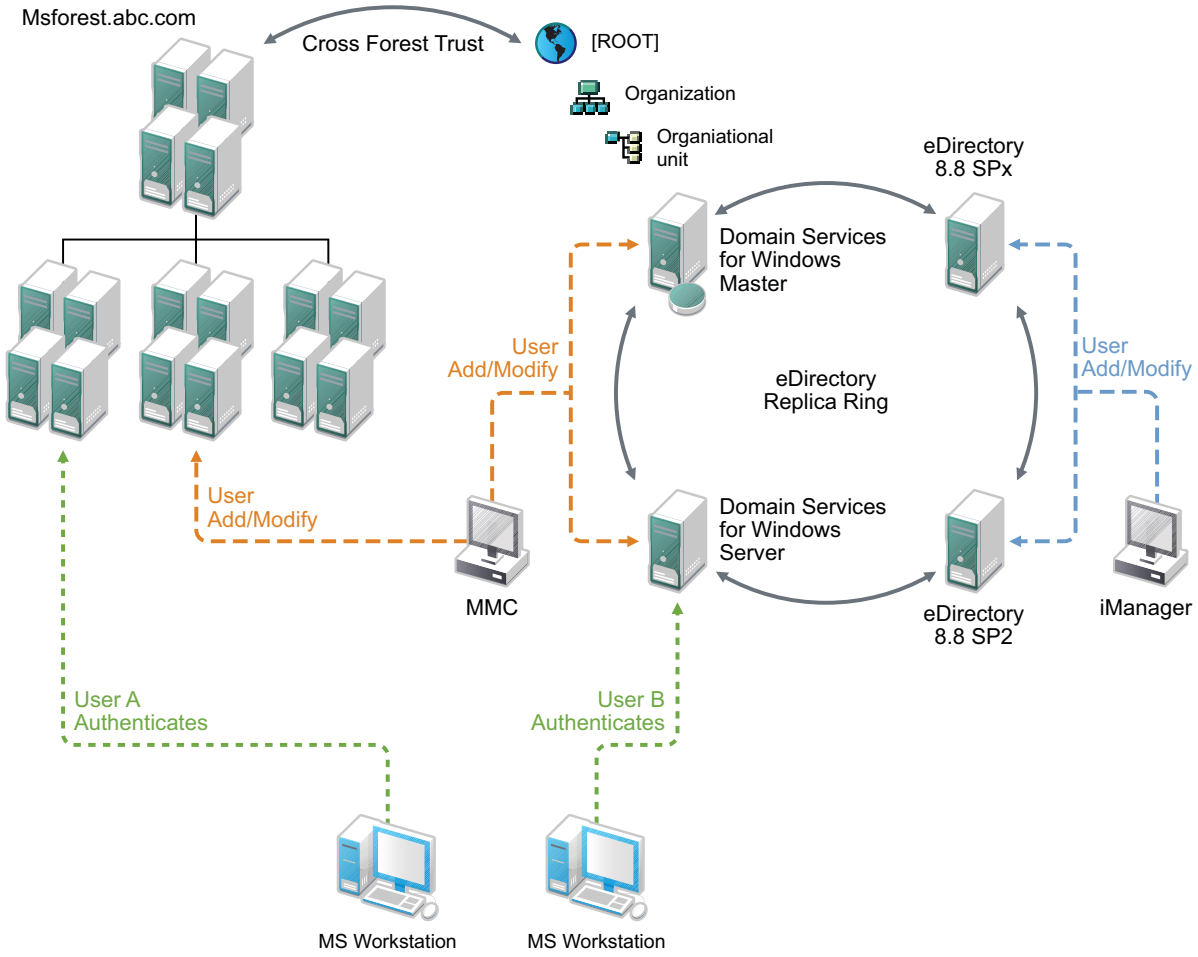
4.4 Interoperability Between Active Directory and eDirectory

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 4-4 illustrates a typical deployment scenario in a mixed OpenText/Microsoft environment.

Figure 4-4 *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 SP2 server, and an eDirectory 8.8 SPx server, configured in the same replica ring. The 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.

For more information on creating cross-forest trust, see Chapter 20, “Managing Trust Relationships in Domain Services for Windows,” on page 163.

5 Deployment Scenarios

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

- Section 5.1, “Deploying DSfW in a Non-Name-Mapped Setup,” on page 31
- Section 5.2, “Deploying DSfW in a Name-Mapped Setup,” on page 33

5.1 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.

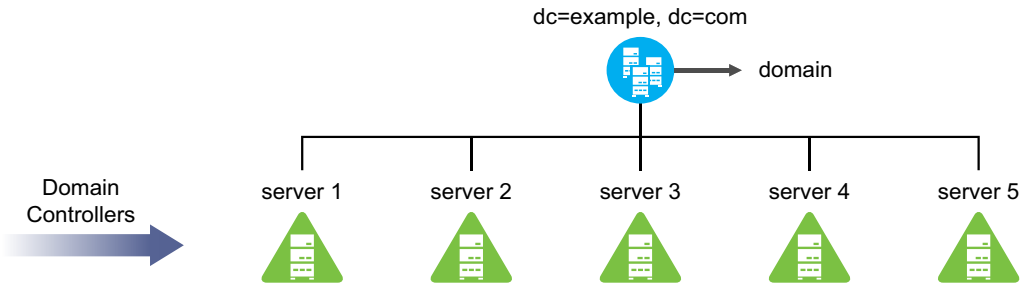
The scenarios explained here are only indicative of the various ways in which you can deploy DSfW server in your environment. Here the tree structure overlaps with the DNS namespace. For instance, the domain example.com will be mapped to dc=example,dc=com FQDN.

- Section 5.1.1, “Deploying as a Single Domain,” on page 31
- Section 5.1.2, “Deploying as Multiple Domains in a Forest,” on page 31

5.1.1 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 5-1 *Deploying DSfW as a Single Domain*



In Figure 5-1 the example.com domain is served by 5 domain controllers.

5.1.2 Deploying as Multiple Domains in a Forest

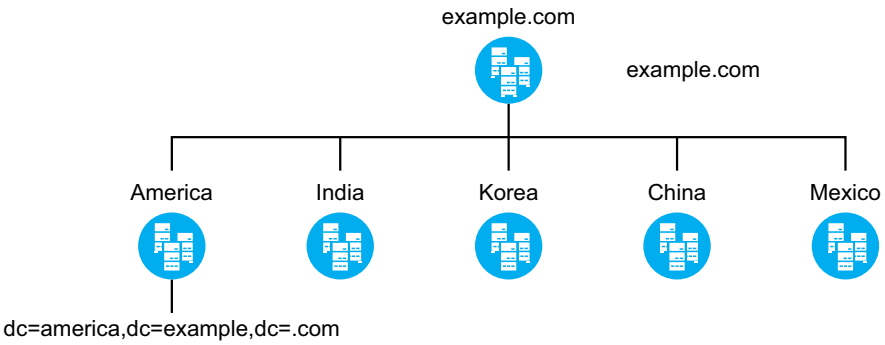
- “Width” on page 32
- “Depth” on page 32
- “Depth and Width” on page 32

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.

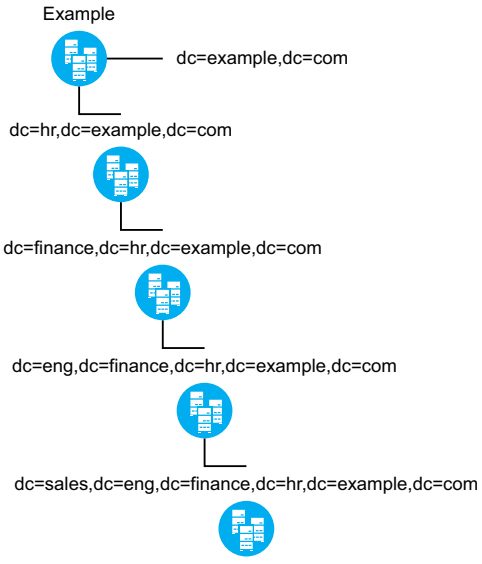
Figure 5-2 *Deploying DSfW in a Horizontally Spread Tree*



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.

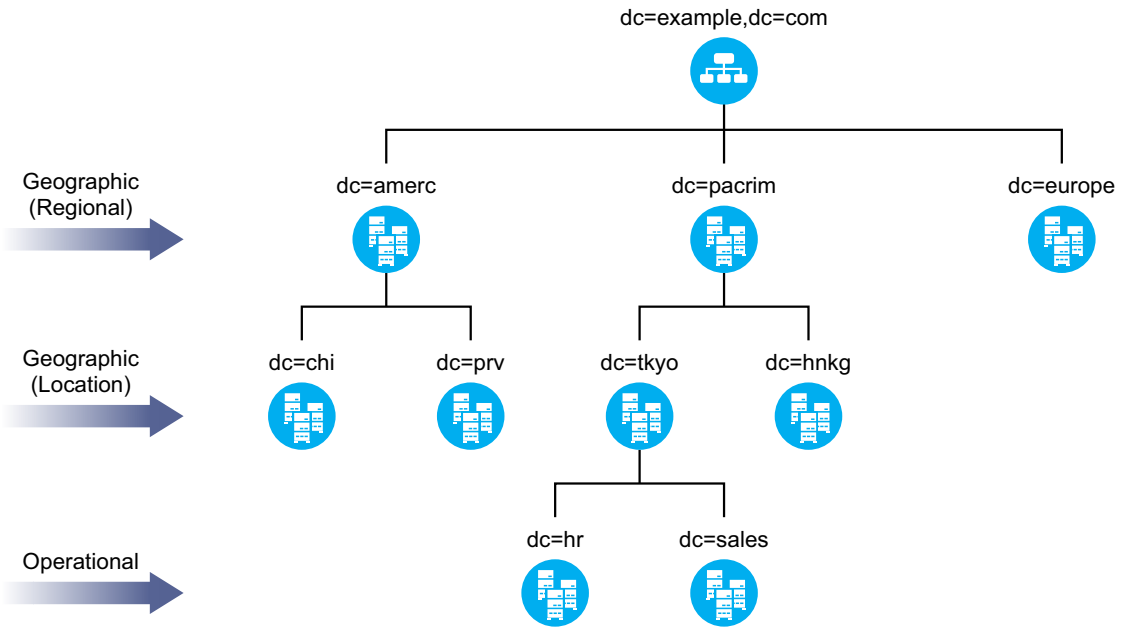
Figure 5-3 *Deploying DSfW in a Vertically Structured Tree*



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 5-4 *Deploying DSfW in a Combination Structure*



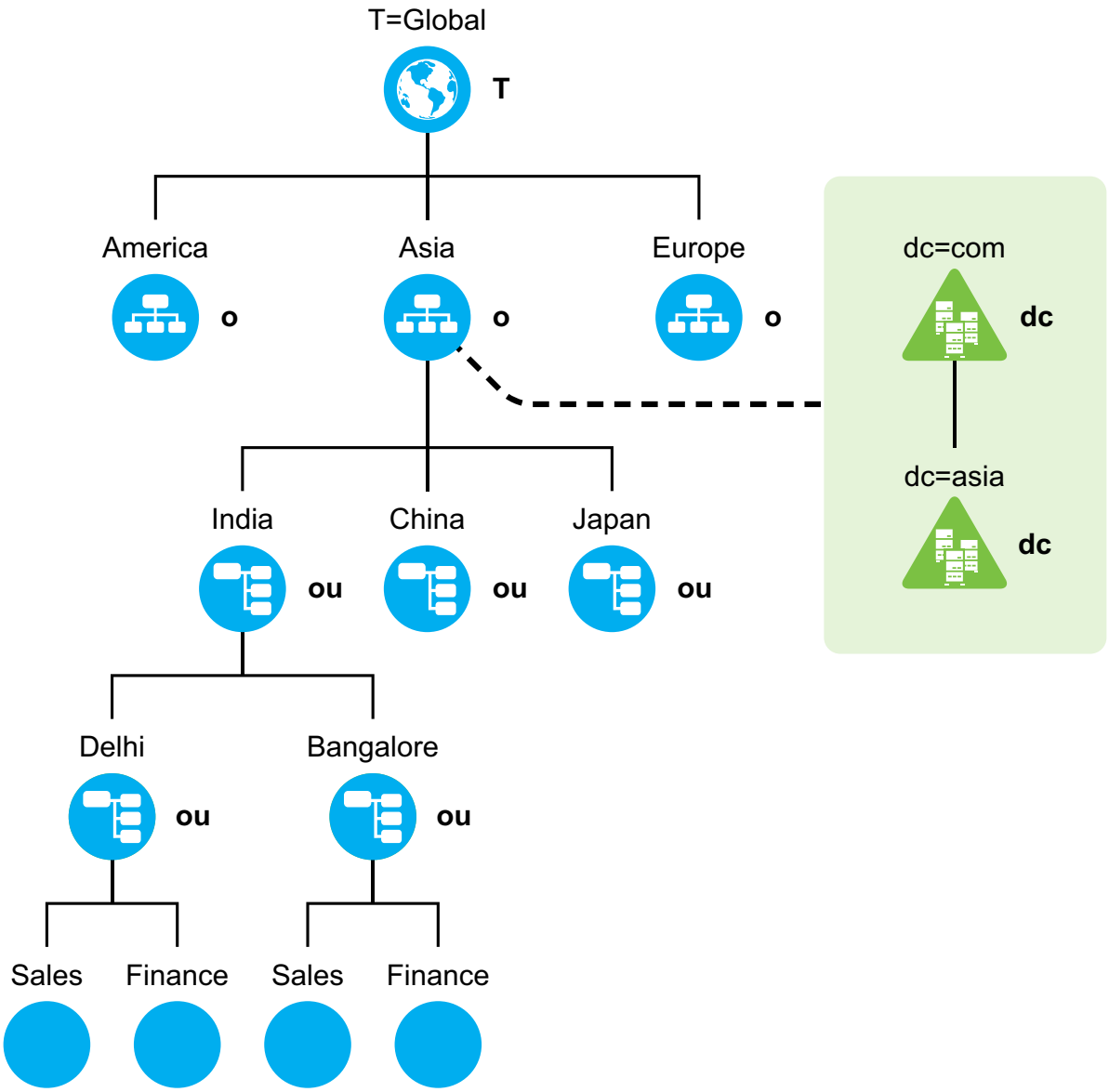
5.2 Deploying DSfW in a Name-Mapped Setup

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 5-5 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 5-5 *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 5.2.1, “Deploying DSfW by Skipping Containers,” on page 36. 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 5-5, 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 5-5, 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 8, “Provisioning Domain Services for Windows,” on page 79.

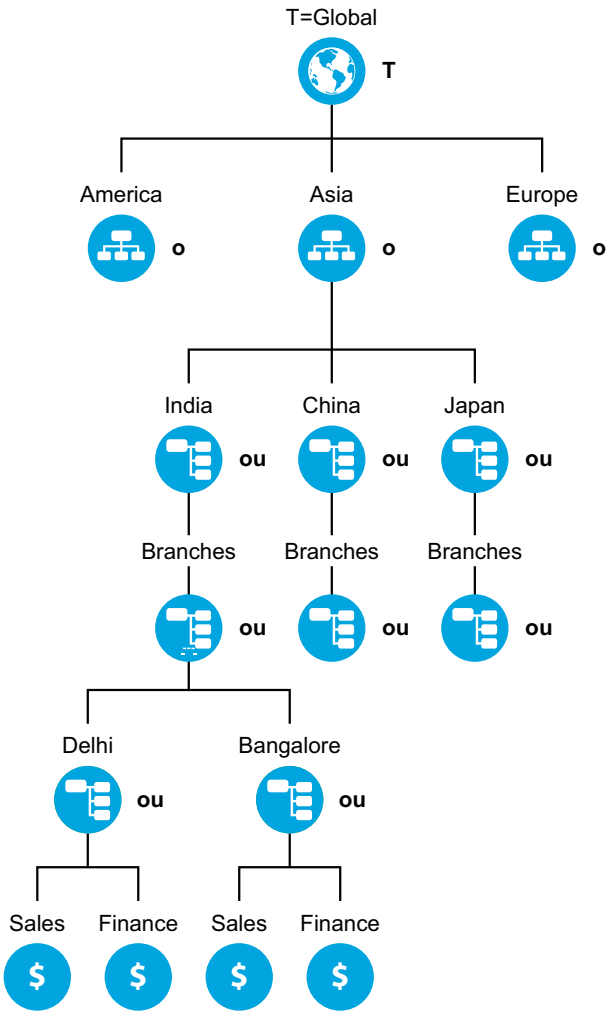
WARNING: If you deploy the forest root domain too deep down in the tree, further child domain installation may be difficult because the DN mapping range will exhaust.

5.2.1 Deploying DSfW by Skipping Containers

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.

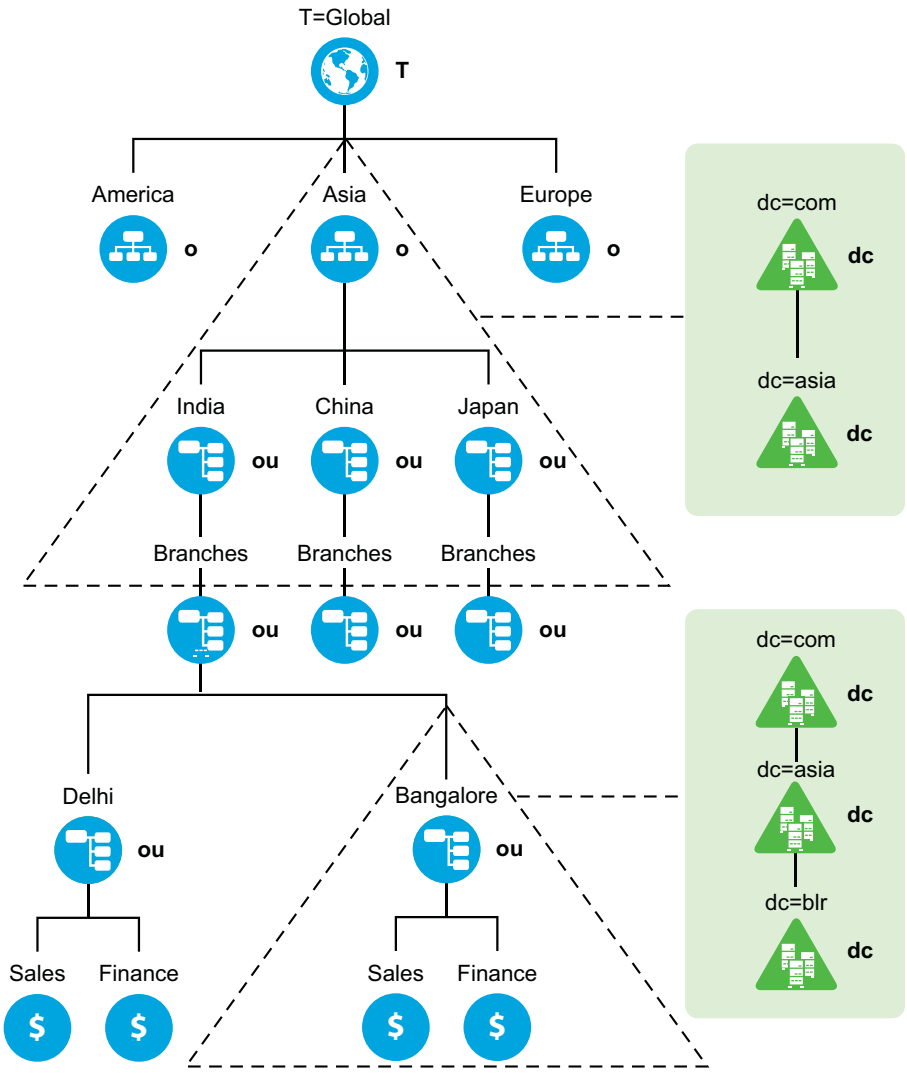
Consider a scenario with an eDirectory tree, as represented in the following figure.

Figure 5-6 *Existing eDirectory Tree*



As illustrated in Figure 5-7, 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 5-7 *Deploying DSfW by Skipping Containers*



5.2.2 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 5-7, 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.

6 Planning for DSfW

This section describes requirements and guidelines for using the OES Domain Services for Windows on an Open Enterprise Server.

IMPORTANT: If your deployment has more than 3 domain controllers or more than 2000 active users, you must contact OpenText Consulting Services or a qualified OpenText Partner for Deployment Assistance.

- Section 6.1, “Server Requirements for Installing DSfW,” on page 39
- Section 6.2, “Scalability Guidelines,” on page 40
- Section 6.3, “Deciding between Name-Mapped and Non-Name-Mapped Installation,” on page 40
- Section 6.4, “Impact of Mixed Mode Configuration in a Forest or Domain,” on page 43
- Section 6.5, “Extending a Domain Boundary in a Name-Mapped Installation,” on page 43
- Section 6.6, “Meeting the Installation Requirements,” on page 45
- Section 6.7, “Unsupported Service Combinations,” on page 51
- Section 6.8, “Operating System Version Support,” on page 52
- Section 6.9, “Client for Open Enterprise Server and Windows Co-existence,” on page 53
- Section 6.10, “Administrative Tools,” on page 53
- Section 6.11, “Utilities Not Supported in DSfW,” on page 53
- Section 6.12, “Limitations,” on page 53
- Section 6.13, “Restrictions with Domain Names,” on page 54
- Section 6.14, “Supported Special Characters in DSfW Passwords,” on page 55
- Section 6.15, “Enabling Universal Password Policy for DSfW,” on page 55
- Section 6.16, “Ensuring Filesystem ACL Support,” on page 55

6.1 Server Requirements for Installing DSfW

To install DSfW, you need a server that meets the system requirements for Open Enterprise Server. For more information, see “Installing OES as a New Installation” in the *Installation Guide*.

You should have access to the installation media for OES, either on physical CD/DVD media or on a networked installation source server. For more information about installing OES from an installation source, see “Setting Up a Network Installation Source” in the *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.

6.2 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:

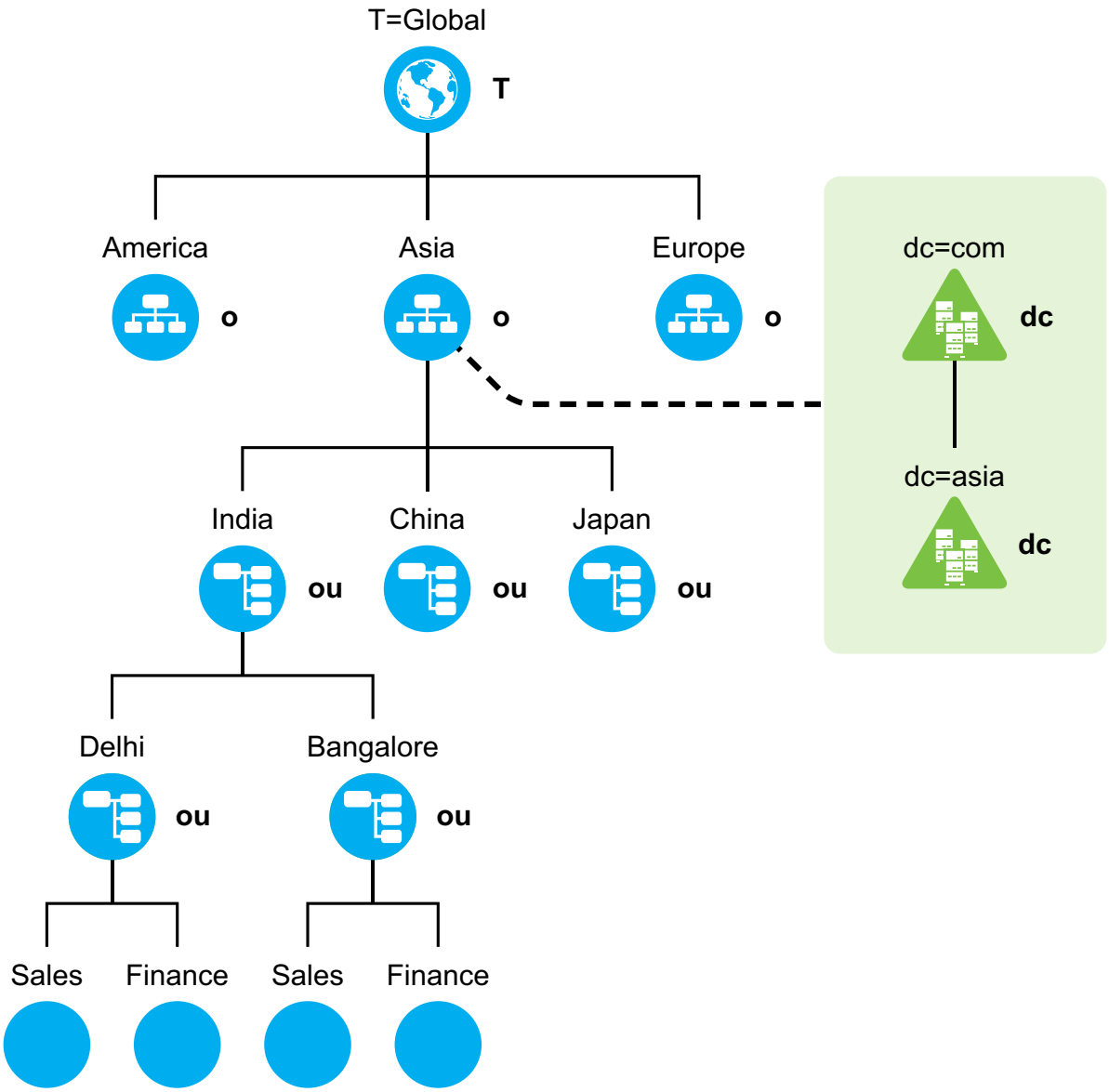
- If the number of users in your environment is high (in thousands), it is recommended to use a dedicated server such as the OES CIFS server for your file server needs. In such scenarios, the DSfW server should be used only as a domain controller managing domain logins.
- The number of domain controllers 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 34.

6.3 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 6-1 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 6-1, 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.

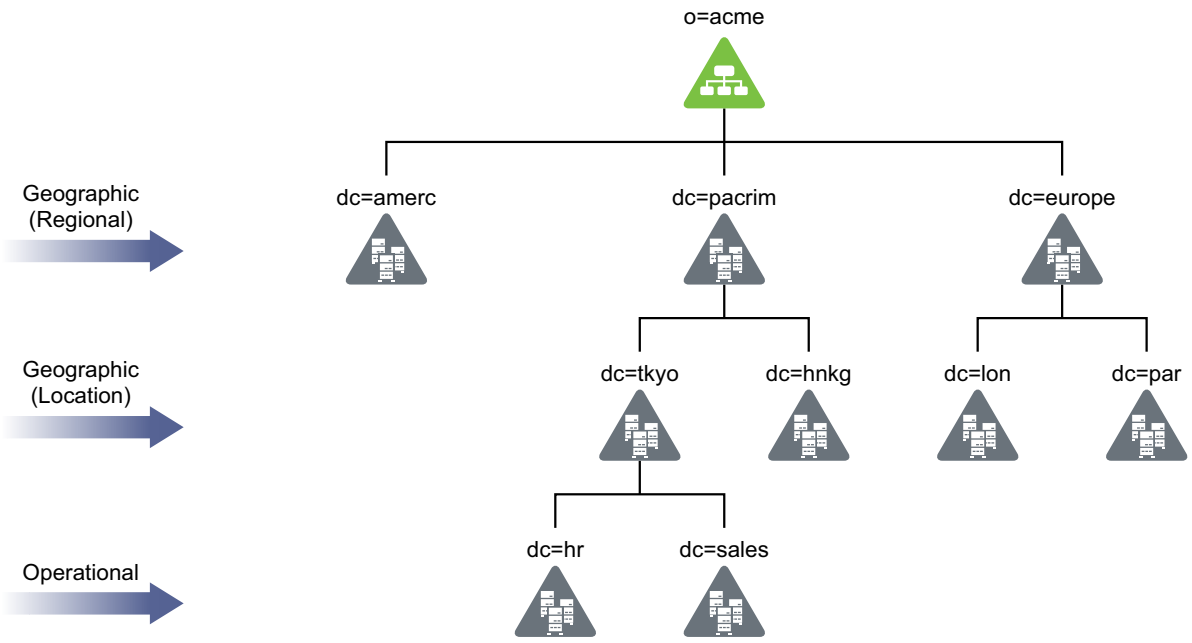
IMPORTANT: In name-mapped installations, you install DSfW in an existing eDirectory tree inside a specific container. However, DSfW must be installed on a separate server and not on the server where eDirectory is installed.

Figure 6-1 *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 6-2 *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.

6.3.1 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 42
- "Using a Flat Design" on page 42

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 Your NetIQ eDirectory Network in the NetIQ eDirectory Administration Guide.

6.4 Impact of Mixed Mode Configuration in a Forest or Domain

In OES 2018 SP1 or later because of the incompatibilities introduced from the updated versions of Kerberos and Samba, the domain controller having OES 24.4 cannot coexist with domain controllers having the earlier OES versions. The mixed mode configuration is not supported.

For the forest or domain to be operational, all the existing domain controllers must have the same OES version and the same patch applied. A new OES 24.4 domain controller can be added to the existing forest only after all the existing domain controllers are upgraded to OES 24.4.

It is recommended to perform upgrade in the following order in a forest:

- Within the domain, upgrade the Primary Domain Controller (PDC) first and then upgrade other domain controllers.
- Within the forest, upgrade the Forest Root Domain (FRD) first and then upgrade the child domains.

6.5 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 2015 or later.
- 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 OES 2015 or later. 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.

6.5.1 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.

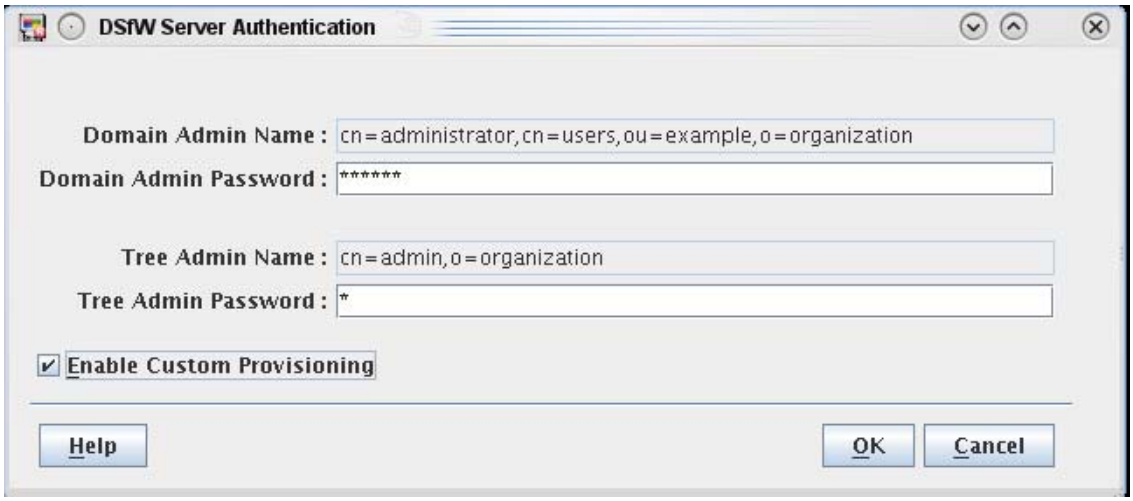
6.5.2 Use Case Scenario

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.

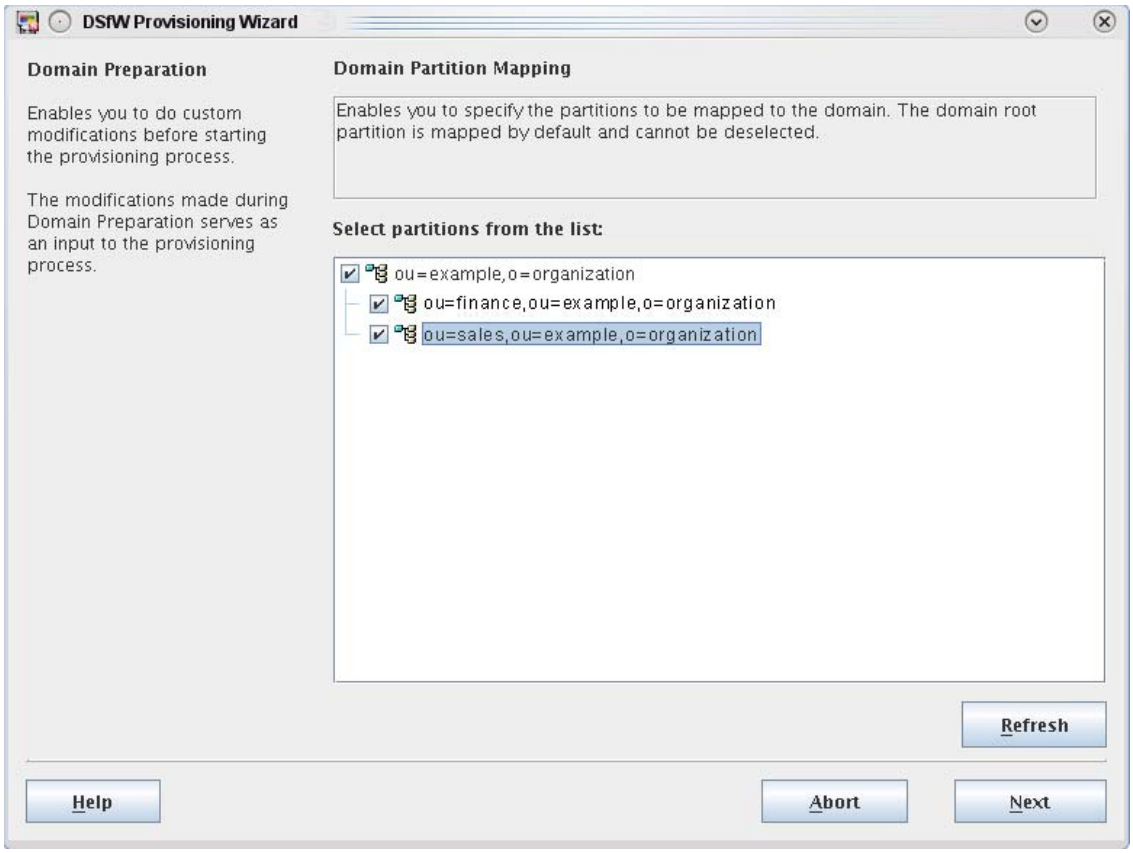
NOTE: The RDN of the mapped partition need not match the domain name. For instance, the partition ou=example,o=organization can be mapped to dsfw.com.

Along with the ou=example,o=organization partition, there are some additional partitions such as ou=finance,ou=example,o=organization and ou=sales, 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=finance, ou=example,o=organization and ou=sales, ou=example,o=organization.



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

6.5.3 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.

6.6 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 6.6.1, “Installation Prerequisites For a Non-Name-Mapped Setup,” on page 45
- Section 6.6.2, “Installation Prerequisites for a Name-Mapped Setup,” on page 48

6.6.1 Installation Prerequisites For a Non-Name-Mapped Setup

- “Domain Name and Name Server Configuration is Correct” on page 46
- “DNS Server is Installed” on page 47
- “Time is Synchronized” on page 48
- “Server State in the Replica Ring” on page 48

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 Devices>Network Settings**. Select the **Hostname/DNS** tab.

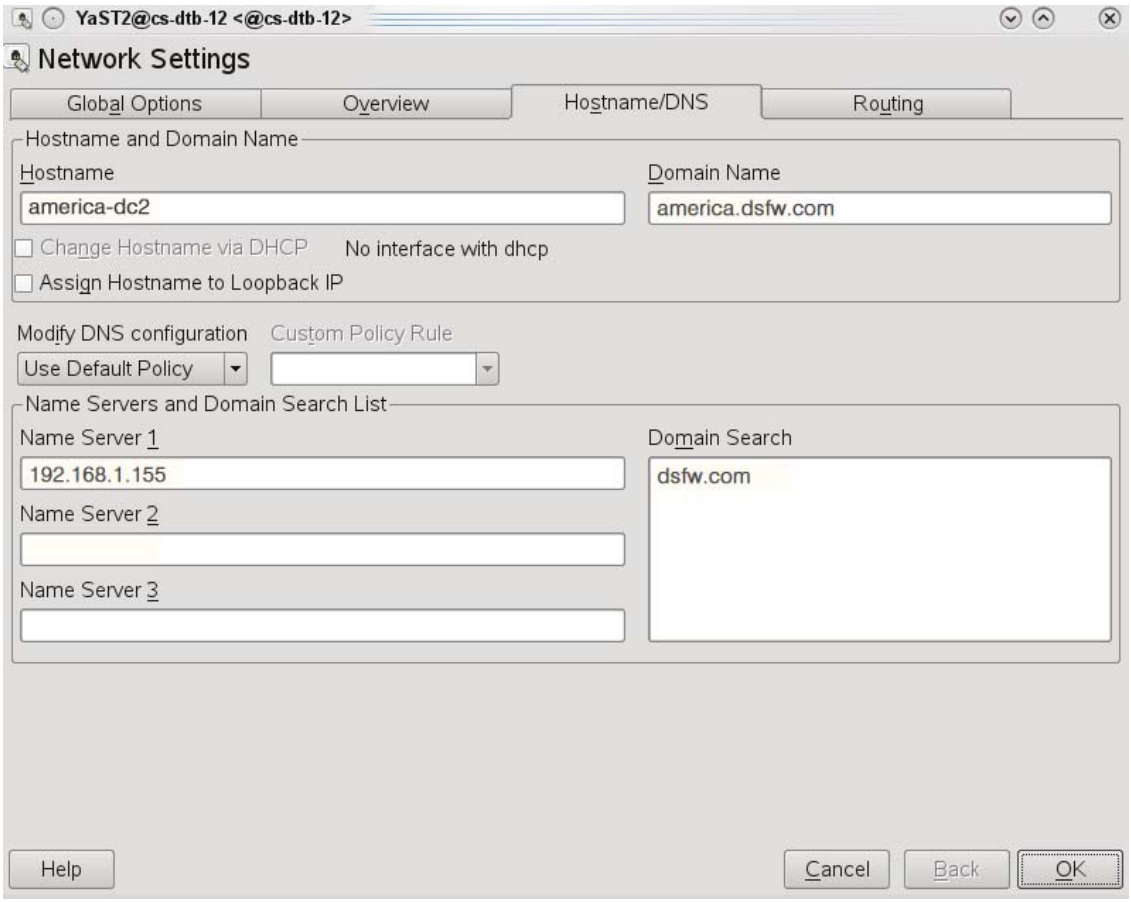
NOTE: You must ensure that the hostname in the properties of the active ethernet controller is a FQDN. For example, if the hostname in the **Hostname/DNS** tab is *dsfw-dc1* and domain name is *dsfw.com,* then the hostname of the active ethernet controller must be *dsfw-dc1.dsfw.com*. You can modify the hostname of the active ethernet controller by using the **Edit** option in the **Overview** tab.

---

2 Verify that the domain name is correct.

3 Ensure that you follow the guidelines given below to configure the name server on a DSfW domain controller:

- While configuring the forest root domain, for DNS name resolution during installation, the name server must point to a valid DNS server. After the DSfW server is configured successfully, the forest root domain controller will always act as the DNS server for the first DSfW domain. To ensure that the forest root domain DNS sever resolves other existing domains in your environment, complete the necessary forwarder settings.
- To configure the subsequent DSfW domain controllers or DSfW domains, the **Name Server 1** entry must point to the forest root domain's IP address.
- If the existing DNS infrastructure is running on OES DNS server and the zone for the DSfW domain being configured is already existing, the DSfW configuration has the built-in capability to extend the existing zone. Ensure that the correct DNS-DHCP locater object is specified during DSfW configuration in YaST. For more information, see Step 17.



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.

4 Click **OK** to save the changes.

DNS Server is Installed

In a default configuration, there is only one DNS server in a DSfW forest which is the first domain controller of the first DSfW domain. You must ensure that the DNS configuration (/etc/resolv.conf) of all domain controllers in all domains of a DSfW forest point to this DNS server. This applies to all workstations or member servers joined to any DSfW domain.

To split the DNS information across a domain, you must do the following:

- For every DSfW domain that is configured, specify one or more domain controllers of a given domain to host the DNS server.
- Ensure that all the workstation or domain servers joined to a particular domain point to one of the DNS servers hosting the domain.
- After the DNS information is split, verify that any name or address resolution to all domains of a DSfW forest works fine. To verify this, you must set up two-way forwarders between the DSfW domains.

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.

6.6.2 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 48
- "eDirectory Version" on page 49
- "Container is Partitioned" on page 49
- "DNS Server is Installed" on page 49
- "Time is Synchronized" on page 50
- "Schema is Synchronized" on page 50
- "Server State in the Replica Ring" on page 50
- "Permissions for Objects" on page 50
- "Container Names" on page 50

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 Devices>Network Settings**. Select the **Hostname/DNS** tab.

NOTE: You must ensure that the hostname in the properties of the active ethernet controller is a FQDN. For example, if the hostname in the **Hostname/DNS** tab is *dsfw-dc1* and domain name is *dsfw.com,* then the hostname of the active ethernet controller must be *dsfw-dc1.dsfw.com*. You can modify the hostname of the active ethernet controller by using the **Edit** option in the **Overview** tab.

---

2 Verify that the domain name is correct.

3 Ensure that you follow the guidelines given below to configure the name server on a DSfW domain controller:

- While configuring the forest root domain, for DNS name resolution during installation, the name server must point to a valid DNS server. After the DSfW server is configured successfully, the forest root domain controller will always act as the DNS server for the first DSfW domain. To ensure that the forest root domain DNS sever resolves other existing domains in your environment, complete the necessary forwarder settings.
- To configure the subsequent DSfW domain controllers or DSfW domains, the **Name Server 1** entry must point to the forest root domain's IP address.
- If the existing DNS infrastructure is running on OES DNS server and the zone for the DSfW domain being configured is already existing, the DSfW configuration has the built-in capability to extend the existing zone. Ensure that the correct DNS-DHCP locator object is specified during DSfW configuration in YaST. For more information, see Step 17.

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.

---

4 Click **OK** to save the changes.

eDirectory Version

Before installing DSfW, ensure that the eDirectory version is 8.8 SP2 or later. 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 later.

Container is Partitioned

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

DNS Server is Installed

In a default configuration, there is only one DNS server in a DSfW forest which is the first domain controller of the first DSfW domain. You must ensure that the DNS configuration (/etc/resolv.conf) of all domain controllers in all domains of a DSfW forest point to this DNS server. This applies to all workstations or member servers joined to any DSfW domain.

To split the DNS information across a domain,you must do the following:

- For every DSfW domain that is configured, specify one or more domain controllers of a given domain to host the DNS server.
- Ensure that all the workstation or domain servers joined to a particular domain point to one of the DNS servers hosting the domain.
- After the DNS information is split, verify that any name or address resolution to all domains of a DSfW forest works fine. To verify this, you must set up two-way forwarders between the DSfW domains.

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

6.7 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, OpenText does not support any of the following combinations:

- File Server (SLES 11 - Samba)
- OES AFP
- OES CIFS
- OES Cluster Services (NCS)
- OES FTP
- OES NetStorage
- OES Pre-Migration Server
- OES Samba

6.7.1 Installing Other Products in the DSfW Partition

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

Some products might be supported in name-mapped implementations of DSfW. Consult the Product Documentation (https://www.microfocus.com/documentation/open-enterprise-server/) and the OpenText Support site (https://www.microfocus.com/en-us/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 OpenText products that are not included with OES, such as GroupWise. It doesn’t apply to services included with OES, such as OpenText iPrint.

Limitations for installing OES services on the same server are outlined in Section 6.7, “Unsupported Service Combinations,” on page 51.

6.8 Operating System Version Support

The following table lists the version of operating systems that are supported with DSfW:

Table 6-1 *OS version support*

	Workstation	Member Server	Cross Forest Trust	
Windows	Windows 2022 (64 Bit)			
	Windows 2019 (64 Bit)			
	Windows 11 (64 Bit)	Windows 2022		
	Windows 10 RS1, RS2, RS3 (64 Bit and 32 Bit)	Windows 2016	Windows 2016 AD	Functional Level 2008 R2, 2012 R2
		Windows 2012, 2012 R2	Windows 2012 R2 AD	Functional Level 2008 R2, 2012 R2
		Windows 2008, 2008 R2	Windows 2008 R2 AD	Functional Level 2003, 2008 R2
	N/A	Windows 2003	Windows 2003 AD	Functional Level 2003
Linux	SLED 12 SP2 (64 Bit)	SLES 12 SP2	OES 2015 SP1 OES 2018 OES 2018 SP1 OES 2018 SP2 OES 2018 SP3 OES 2023 OES 23.4 OES 24.4	
Mac	Mac OS 11.5 (ARM)			
	Mac OS 11			
	Mac OS 10.15			
	Mac OS 10.14			
	Mac OS X 10.11			
	Mac OS X 10.10.3			
	Mac OS X 10.9.5			
	Mac OS X 10.8.5			

6.9 Client for Open Enterprise Server and Windows Co-existence

The following table lists the version of Client for Open Enterprise Server and Windows that can co-exist.

Table 6-2 *Client for Open Enterprise Server and Windows Co-existence*

OES Version	Client for Open Enterprise Server Version	Windows Version
OES 24.4	Client for Open Enterprise Server 2 SP7	Windows 10
		Windows 11

6.10 Administrative Tools

The following administrative tools are supported in DSfW:

- Section 6.10.1, “Windows Administration Tools,” on page 53
- Section 6.10.2, “Linux Administration Tools,” on page 53

6.10.1 Windows Administration Tools

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

6.10.2 Linux Administration Tools

For managing DSfW server, use iManager.

6.11 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.

6.12 Limitations

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

- Section 6.12.1, “Hostname,” on page 54
- Section 6.12.2, “NetBIOS Names,” on page 54
- Section 6.12.3, “Installation Issue,” on page 54

6.12.1 Hostname

If the hostname of a primary domain controller or an additional domain controller (ADC) has more than 15 characters, you must ensure that the first 15 characters of a new ADC that is added to the domain is different from the first 15 characters of the primary domain controller or any existing ADC in the domain. Not complying with this guideline will lead to failure in provisioning of the new ADC.

6.12.2 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

6.12.3 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.

6.13 Restrictions with Domain Names

- Section 6.13.1, “DSfW Does Not Support Domain Names Ending with *.local,” on page 54
- Section 6.13.2, “DSfW Does Not Support A Single-Label Domain Name,” on page 54

6.13.1 DSfW Does Not Support Domain Names Ending with *.local

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. Therefore, avoid specifying a domain name such as `example.local`.

6.13.2 DSfW Does Not Support A Single-Label Domain Name

Single-label domain name does not contain a suffix, such as `*.com`, `*.corp`, `*.net`, `*.org`, or `companyname`. For instance, the *host* is a single-label DNS name.

DSfW domain names must consist of one or more subdomains that are combined with a top-level domain that is separated by a dot character ("."). For example: `example.com` or `corp.example.com`.

6.14 Supported Special Characters in DSfW Passwords

You may use the following special characters while specifying passwords for eDirectory tree administrator or domain administrator or users during DSfW install:

```
/ * ? $ ( ) - { } [ ] ~ & ^ % @
```

6.15 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. 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. 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 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.

6.16 Ensuring Filesystem ACL Support

Ensure that the `user_xattr` option is set for the filesystem on which `/var` resides. If the `user_xattr` option is not set, then the sysvol ACLs will be missing on `/var/opt/novell/xad/sysvol` directory and users will not be able to access sysvol. For more information, refer to the mount (8) manpage.

7 Installing Domain Services for Windows

This section describes how to install and configure Domain Services for Windows (DSfW). You can install DSfW by using the YaST administrative tool or using the AutoYaST feature.

In, OES 2018 and later, DSfW supports schema level and features equivalent to AD 2012.

- Section 7.1, “Installing and Configuring DSfW Using the YaST Administrative Tool,” on page 57
- Section 7.2, “Installing DSfW Using AutoYaST,” on page 71

7.1 Installing and Configuring DSfW Using the YaST Administrative Tool

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

- Section 7.1.1, “Prerequisites for Installation,” on page 57
- Section 7.1.2, “Installation Scenarios,” on page 57
- Section 7.1.3, “Express Installation,” on page 70
- Section 7.1.4, “Using a Container Admin to Install and Configure DSfW,” on page 70

7.1.1 Prerequisites for Installation

- Before you proceed with the installation, please review the details in “Planning for DSfW” on page 39.
- If you are installing a Child Domain Controller (CDC) or an Additional Domain Controller (ADC) in a domain with OES 24.4, ensure to upgrade all the existing domain controllers (FRD, CDC, and ADC) in the domain to OES 24.4. The domain controllers in a domain having different OES versions (mixed mode configuration) is not supported in OES 2018 SP1 and later.

  If such a configuration is attempted, an error message is displayed and the installation does not proceed.

7.1.2 Installation Scenarios

DSfW can be installed in the following scenarios:

- “Installing a Forest Root Domain” on page 58
- “Installing a Child Domain” on page 62
- “Installing DSfW as an Additional Domain Controller in a Domain” on page 66

Installing a Forest Root Domain

1 In the YaST install for OES, on the Software Selections page, ensure that DNS is selected. Then select the **OES Domain Services for Windows** pattern.

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

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

2 Click **Accept**.

3 Select the type of Domain Services for Windows configuration you want:

3a To install a forest root domain (FRD), select the **New Domain Services for Windows Forest** option.

3b Select the **Express Install** option to deploy a domain controller by automatically populating certain YaST configuration fields. For more information, see Section 7.1.3, "Express Installation," on page 70.

3c Click **Next**.

4 On the eDirectory configuration page, choose whether to install into an existing eDirectory tree or create a new tree.

New Tree: Select the **New Tree** option if this is the first server to go into the tree or if this server requires a separate tree. Keep in mind that this server will have the master replica for the new tree, and that users must log in to this new tree to access its resources.

Existing Tree: Select the **Existing Tree** option if you want to incorporate this server into an existing eDirectory tree. This server might not have a replica copied to it, depending on the tree configuration.

Use eDirectory Certificates for HTTPS Services: 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.

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

By default, the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols are not enabled in Active Directory.

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

5 Click **Next** to continue.

6 Specify information to access the existing eDirectory tree.

This screen is displayed only of you select the **Existing Tree** option in Step 4.

6a Specify the IP address of an existing eDirectory server.

6b Do not change the NCP Port, LDAP Port, and Secure LDAP Port information.

6c Specify the tree admin credentials for the administrator to log in to the eDirectory tree. For information about the special characters that you can use while specifying the password, see Section 6.14, "Supported Special Characters in DSfW Passwords," on page 55.

6d Click **Next**.

7 Specify the Domain Name and NetBIOS information:

DNS Name for New Domain: The DNS name for the new domain is automatically populated based on the Hostname and DNS configuration settings.

You must ensure that the host name in the properties of the active Ethernet controller is an FQDN. For example, if the host name is dc1 and the domain name is dsfw.com, then the host name in the **YaST > Network Devices > Network Settings > Hostname/DNS** tab of the active Ethernet controller must be dc1.dsfw.com. You can modify the host name of the active Ethernet controller by using the **Edit** option in the **Overview** tab of the LAN settings in YaST.

Configure this Server as a DNS Server: If you want this server to be a DNS server for the domain, select the **Configure this server as a DNS Server** option. If this option is not selected, you must ensure that a DNS server that contains the domain names for Domain Services for Windows is available somewhere in the network.

NetBIOS Domain Name: The NetBIOS Domain name is automatically populated based on the Hostname and DNS configuration settings.

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

Configure this machine to be a WINS server: If you want this server to be a WINS server, select the **Configure this machine to be a WINS server** option. For more information about WINS, see Chapter 18, "Configuring DSfW Server as a WINS Server," on page 147.

Site Name of Domain Controller: `Default-First-Site-Name` is specified as the site name by default. To create a new site, specify the site name or click **Browse** to specify a site from the list of sites. For more information about sites and subnets, see Chapter 26, "Configuring Sites and Subnets," on page 241.

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

This screen is displayed only of you select the **Existing Tree** option in Step 4.

Specify the domain administrator password in both fields. For information about the special characters that you can use while specifying the password, see Section 6.14, "Supported Special Characters in DSfW Passwords," on page 55.

The administrator name is hard-coded. However, after you finish DSfW installation and configuration (post provisioning), you can modify administrator details such as the administrator name. For more information, see Section 10.2, "Renaming Administrator Details Using MMC," on page 113.

FQDN of the eDirectory Container: Specify the Fully Qualified Domain Name of the existing eDirectory container that you want to be mapped 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.

Retain Existing NMAS Password Policies: If you select the **Retain existing NMAS Password Policies** option, the password policies assigned to the users within the container that is mapped to the new domain do not change. However, the password policies outside the partition boundary are not carried forward. You need to create a new password policy assigned to the partition root. For details on creating a new password policy, see "Creating Password Policies". For information about default password policy settings for DSfW, see Appendix D, "DSfW Password Policy Attributes," on page 235.

9 Specify a reliable Network Time Protocol (NTP) provider.

eDirectory requires that all servers in a tree be time-synchronized. To add multiple time servers to the list of NTP servers, click the **Add** button and specify the IP address or DNS host name of the NTP server. In a single-server scenario, you can select the **Use local clock** check box and specify the local machine as the NTP provider.

10 Click **Next**.

NOTE: If you are using the Express install, Step 11 through Step 17 are not displayed.

---

11 Specify the settings to configure the local server in the eDirectory tree:

11a Leave the location of the Directory Information Base (DIB) at the default setting.

11b Leave the **iMonitor Port** settings at the defaults unless you need to change them to avoid port conflicts with other services.

11c Leave the **Secure iMonitor Port** settings at the defaults unless you need to change them to avoid port conflicts with other services.

11d Click **Next** to continue.

12 Specify details to configure SLP:

Multicast to access SLP: Select the **Use multicast to access SLP** option to request SLP information through a multicast packet.

Configure SLP to use an Existing Directory Agent: 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.

Configuring Directory Agent: 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.

Service Location Protocol Scopes: In the **Service Location Protocol Scopes** field, specify the scope that a User Agent (UA) or Service Agent (SA) is allowed when making requests or when registering services, or specify the scope that a Directory Agent (DA) must support.

The default value is DEFAULT. Use commas with no space to separate each scope. For example:

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

Configuring SLP Directory Agents: In the **Configured SLP Directory Agents** field, specify the host name or IP address of one or more external servers on which an SLP Directory Agent is running. Do not specify the local host.

To add an agent, click **Add**. In the **SLP DA Server** field, specify a server's DNS name or IP address, then click **Add**.

To remove an agent, select one or more agents to remove, then click **Delete**.

13 Click **Next.**

14 Select the authentication service you want to install:

NOTE: The SASL GSSAPI mechanism is an eDirectory-specific SASL mechanism. It is not used on a DSfW server. The DSfW-specific SASL GSSAPI mechanism is extended during DSfW configuration by default.

15 Click **Next**.

16 Specify the common proxy details:

16a To use a 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 are enabled. These fields are populated with a system-generated user name and password. To change these values, see Step 16b.

or

If you do not want to use a common proxy, clear the check box and click **Next**. Then continue with Step 17.

16b Specify the following information:

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

16c To assign a common proxy password policy to the proxy user, select the **Assign Common Proxy Password Policy to Proxy User** check box.

16d Click **Next** to continue.

17 Specify the details to configure the DNS server:

17a 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 retrieves the Locator, Root Server Info, and Group contexts.

NOTE: Before running the configure DNS task in the DSfW provisioning wizard, ensure that the partition hosting the Locator, Root Server Info, and Group contexts has a local replica on the DSfW server that is being configured.

17b If there is no existing DNS server in the tree, specify the following information:

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

17c Specify the fully distinguished, typeful name of the proxy user that will be used for DNS management, such as `cn=OESCommonProxy_server1,ou=OESSystemObjects,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.

17d Specify the password of the proxy user for accessing DNS.

If you selected the **Use Common Proxy User as default for OES Products** check box in Step 16a, the proxy user and password fields are populated with common proxy user name and password.

17e Decide whether to use a secure LDAP port.

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.

17f Specify the **Credential Storage Location** as OES Credential Store.

17g Click **Next** to continue.

18 After the installation is complete, the OES Configuration Summary page is displayed. Review the settings, then click **Next** to start the DSfW installation.

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

This completes the DSfW installation. However, the server is not ready for use until you provision DSfW and the supporting services.

20 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 79.

21 When provisioning is complete, the DSfW server is ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by using the instructions in Chapter 10, "Activities After DSfW Installation or Provisioning," on page 111.

Installing a Child Domain

1 In the YaST install for OES, on the Software Selections page, ensure that DNS is selected. Then select the **OES Domain Services for Windows** pattern.

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

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

2 Click **Accept**.

3 Select the type of Domain Services for Windows configuration you want:

3a To create a new Domain in an existing Windows forest, select the **New Domain in an Existing Domain Services for Windows Forest** option.

3b Select the **Express Install** option to deploy a Domain Controller by automatically populating certain YaST configuration fields. For more information, see Section 7.1.3, "Express Installation," on page 70.

3c Click **Next**.

4 On the eDirectory configuration page in YaST, specify the following:

Use eDirectory Certificates for HTTPS Services: 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.

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

By default, the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols are not enabled in Active Directory.

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

Enable NMAS-based login for LDAP Authentication: Select this option if you want to enable NMAS-based login for LDAP authentication.

5 Click **Next** to continue.

6 Specify information to access the existing eDirectory Tree.

6a Do not change the NCP Port, LDAP Port, and Secure LDAP Port information.

6b Specify the tree admin credentials for the administrator to log in to the eDirectory tree. For information about the special characters that you can use while specifying the password, see Section 6.14, “Supported Special Characters in DSfW Passwords,” on page 55.

6c Click **Next**.

7 Specify the Domain Name and NetBIOS information:

DNS Name for New Domain: The DNS name for the new domain is automatically populated based on the Hostname and DNS configuration settings.

You must ensure that the host name in the properties of the active Ethernet controller is an FQDN. For example, if the host name is dc1 and the domain name is dsfw.com, then the host name in the **YaST > Network Devices > Network Settings > Hostname/DNS** tab of the active Ethernet controller must be dc1.dsfw.com. You can modify the host name of the active Ethernet controller by using the **Edit** option in the **Overview** tab of the LAN settings in YaST.

Configure this Server as a DNS Server: If you want this server to be a DNS server for the domain, select the **Configure this server as a DNS Server** option. If this option is not selected, you must ensure that a DNS server that contains the domain names for Domain Services for Windows is available somewhere in the network.

NetBIOS Domain Name: The NetBIOS Domain name is automatically populated based on the Hostname and DNS configuration settings.

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

Configure this machine to be a WINS server: If you want this server to be a WINS server, select the **Configure this machine to be a WINS server** option. For more information about WINS, see Chapter 18, “Configuring DSfW Server as a WINS Server,” on page 147.

Site Name of Domain Controller: `Default-First-Site-Name` is specified as the site name by default. To create a new site, specify the site name or click **Browse** to specify a site from the list of sites. For more information about sites and subnets, see Chapter 26, “Configuring Sites and Subnets,” on page 241.

8 Specify details to map the existing container to the new domain.

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

New Domain Administrator Name: 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.

FDN of the container that needs to be mapped: Specify the FDN of the container that you want to map 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.

Retain Existing NMAS Password Policies: If you select the **Retain existing NMAS Password Policies** option, the password policies assigned to the users within the container that is mapped to the new domain do not change. However, the password policies outside the partition boundary are not carried forward. You need to create a new password policy assigned to the partition root. For details on creating a new password policy, see "Creating Password Policies". For information about default password policy settings for DSfW, see Appendix D, "DSfW Password Policy Attributes," on page 235.

9 Specify a reliable Network Time Protocol (NTP) provider.

eDirectory requires that all servers in a tree be time-synchronized. To add multiple time servers to the list of NTP servers, click the **Add** button and specify the IP address or DNS host name of the NTP server. In a single-server scenario, you can select the **Use local clock** check box and specify the local machine as the NTP provider.

10 Click **Next**.

NOTE: If you are using express install, Step 11 to Step 17 is not displayed.

---

11 Specify the settings to configure the local server in the eDirectory tree:

11a Leave the location of the Directory Information Base (DIB) at the default setting.

11b Leave the **iMonitor Port** settings at the defaults unless you need to change them to avoid port conflicts with other services.

11c Leave the **Secure iMonitor Port** settings at the defaults unless you need to change them to avoid port conflicts with other services.

11d Click **Next** to continue.

12 Specify details to configure SLP:

Multicast to access SLP: Select the **Use multicast to access SLP** option to request SLP information through a multicast packet.

Configure SLP to use an Existing Directory Agent: 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.

Configuring Directory Agent: 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.

Service Location Protocol Scopes: In the **Service Location Protocol Scopes** field, specify the scope that a User Agent (UA) or Service Agent (SA) is allowed when making requests or when registering services, or specify the scope that a Directory Agent (DA) must support.

The default value is DEFAULT. Use commas with no space to separate each scope. For example:

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

Configuring SLP Directory Agents: In the **Configured SLP Directory Agents** field, specify the host name or IP address of one or more external servers on which an SLP Directory Agent is running. Do not specify the local host.

To add an agent, click **Add**. In the **SLP DA Server** field, specify a server's DNS name or IP address, then click **Add**.

To remove an agent, select one or more agents to remove, then click **Delete**.

13 Click **Next.**

14 Select the authentication service you want to install:

NOTE: The SASL GSSAPI mechanism is an eDirectory-specific SASL mechanism. It is not used on a DSfW server. The DSfW-specific SASL GSSAPI mechanism is extended during DSfW configuration by default.

---

15 Click **Next**.

16 Specify the common proxy details:

16a To use a 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 are enabled. These fields are populated with a system-generated user name and password. To change these values, see Step 16b.

or

If you do not want to use a common proxy, clear the check box and click **Next**. Then continue with Step 17.

16b Specify the following information:

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

16c To assign a common proxy password policy to the proxy user, select the **Assign Common Proxy Password Policy to Proxy User** check box.

16d Click **Next** to continue.

17 Specify the details to configure the DNS server.

17a 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 retrieves the Locator, Root Server Info, and Group contexts.

NOTE: Before running the configure DNS task in the DSfW provisioning wizard, ensure that the partition hosting the Locator, Root Server Info, and Group contexts has a local replica on the DSfW server that is being configured.

17b Specify the following information:

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

17c Click **Next** to continue.

18 After the installation is complete, the OES Configuration Summary page is displayed. Review the settings, then click **Next** to start the DSfW installation.

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

This completes the DSfW installation. However, the server is not ready for use until you provision DSfW and the supporting services.

20 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 79.

21 When provisioning is complete, the DSfW server is ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by using the instructions in Chapter 10, "Activities After DSfW Installation or Provisioning," on page 111.

Installing DSfW as an Additional Domain Controller in a Domain

1 In the YaST install for OES, on the Software Selections page, ensure that DNS is selected. Then select the **OES Domain Services for Windows** pattern.

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

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

2 Click **Accept**.

3 Select the type of Domain Services for Windows configuration you want:

3a To create a new domain controller in an existing Domain Services for Windows domain, select the **New Domain in an Existing Domain Services for Windows Domain** option.

3b Select the **Express Install** option to deploy a domain controller by automatically populating certain YaST configuration fields. For more information, see Section 7.1.3, "Express Installation," on page 70.

4 On the eDirectory configuration page in YaST, specify the following:

Use eDirectory Certificates for HTTPS Services: 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.

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

By default, the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols are not enabled in Active Directory.

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

Enable NMAS-based login for LDAP Authentication: Select this option if you want to enable NMAS-based login for LDAP authentication.

5 Click **Next** to continue.

6 Specify information to access the existing eDirectory tree.

6a Do not change the NCP Port, LDAP Port and Secure LDAP Port information.

6b Specify the tree admin credentials for the administrator to log in to the eDirectory tree. For information about the special characters that you can use while specifying the password, see Section 6.14, “Supported Special Characters in DSfW Passwords,” on page 55.

6c Click **Next**.

7 Specify the Domain Name and NetBIOS information:

DNS Name for New Domain: The DNS name for the new domain is automatically populated based on the Hostname and DNS configuration settings.

You must ensure that the host name in the properties of the active Ethernet controller is an FQDN. For example, if the host name is dc1 and the domain name is dsfw.com, then the host name in the **YaST > Network Devices > Network Settings > Hostname/DNS** tab of the active Ethernet controller must be dc1.dsfw.com. You can modify the host name of the active Ethernet controller by using the **Edit** option in the **Overview** tab of the LAN settings in YaST.

Configure this Server as a DNS Server: If you want this server to be a DNS server for the domain, select the **Configure this server as a DNS Server** option. If this option is not selected, you must ensure that a DNS server that contains the domain names for Domain Services for Windows is available somewhere in the network.

NetBIOS Domain Name: The NetBIOS Domain name is automatically populated based on the Hostname and DNS configuration settings.

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

Configure this machine to be a WINS server: If you want this server to be a WINS server, select the **Configure this machine to be a WINS server** option. For more information about WINS, see Chapter 18, “Configuring DSfW Server as a WINS Server,” on page 147.

Site Name of Domain Controller: `Default-First-Site-Name` is specified as the site name by default. To create a new site, specify the site name or click **Browse** to specify a site from the list of sites. For more information about sites and subnets, see Chapter 26, “Configuring Sites and Subnets,” on page 241.

8 Specify the domain administrator password in the **Enter Administrator Password** field. For information about the special characters that you can use while specifying the password, see Section 6.14, “Supported Special Characters in DSfW Passwords,” on page 55.

9 Specify a reliable Network Time Protocol (NTP) provider.

eDirectory requires that all servers in a tree be time-synchronized. To add multiple time servers to the list of NTP servers, click the **Add** button and specify the IP address or DNS host name of the NTP server. In a single-server scenario, you can select the **Use local clock** check box and specify the local machine as the NTP provider.

10 Click **Next**.

NOTE: If you are configuring using Express install, then Step 11 through Step 16 will not be displayed.

11 Specify the settings to configure the local server in the eDirectory tree:

11a Leave the location of the Directory Information Base (DIB) at the default setting.

11b Leave the **iMonitor Port** settings at the defaults unless you need to change them to avoid port conflicts with other services.

11c Leave the **Secure iMonitor Port** settings at the defaults unless you need to change them to avoid port conflicts with other services.

11d Click **Next** to continue.

12 Specify details to configure SLP:

Multicast to access SLP: Select the **Use multicast to access SLP** option to request SLP information through a multicast packet.

Configure SLP to use an Existing Directory Agent: 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.

Configuring Directory Agent: 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.

Service Location Protocol Scopes: In the **Service Location Protocol Scopes** field, specify the scope that a User Agent (UA) or Service Agent (SA) is allowed when making requests or when registering services, or specify the scope that a Directory Agent (DA) must support.

The default value is DEFAULT. Use commas with no space to separate each scope. For example:

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

Configuring SLP Directory Agents: In the **Configured SLP Directory Agents** field, specify the host name or IP address of one or more external servers on which an SLP Directory Agent is running. Do not specify the local host.

To add an agent, click **Add**. In the **SLP DA Server** field, specify a server's DNS name or IP address, then click **Add**.

To remove an agent, select one or more agents to remove, then click **Delete**.

13 Select the authentication service you want to install.

NOTE: The SASL GSSAPI mechanism is an eDirectory-specific SASL mechanism. It is not used on a DSfW server. The DSfW-specific SASL GSSAPI mechanism is extended during DSfW configuration by default.

14 Click **Next**.

15 Specify the common proxy details:

15a To use a 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 are enabled. These fields are populated with a system-generated user name and password. To change these values, see Step 15b.

or

If you do not want to use a common proxy, deselect the check box and click **Next**. Then continue with Step 16.

15b Specify the following information:

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

15c To assign a common proxy password policy to the proxy user, select the **Assign Common Proxy Password Policy to Proxy User** check box.

15d Click **Next** to continue.

16 Specify the details to configure the DNS server:

16a 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 retrieves the Locator, Root Server Info, and Group contexts.

NOTE: Before running the configure DNS task in the DSfW provisioning wizard, ensure that the partition hosting the Locator, Root Server Info, and Group contexts has a local replica on the DSfW server that is being configured.

16b Specify the following information:

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

16c Click **Next** to continue.

17 After the installation is complete, the OES Configuration Summary page is displayed. Review the settings, then click **Next** to start the DSfW installation.

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

This completes the DSfW installation. However, the server is not ready for use until you provision DSfW and the supporting services.

19 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 79.

20 When provisioning is complete, the DSfW server is ready for use. Verify that eDirectory and DSfW have been installed and configured correctly by using the instructions in Chapter 10, "Activities After DSfW Installation or Provisioning," on page 111.

7.1.3 Express Installation

Beginning in OES 11 SP2, DSfW enables you to easily configure a domain controller by using the **Express Install** option. An Express Install simplifies the installation of a domain controller and reduces user intervention by automatically populating certain YaST configuration fields. This is done by assigning default values for the Local server configuration, NMAS, SLP, DNS, and common proxy pages to minimize the number of configuration pages.

You cannot use an Express Install to customize configuration parameters for components such as DNS.

7.1.4 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.

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 on the server that is holding the name-mapped container. This is required for creating partitions during DSfW configuration.

To configure a container admin and use it to install DSfW:

1 Create a container in an existing tree. For example:

`ou=india.o=novell`

2 Create a `cn=localadmin` user under the `ou=india.o=novell` container.

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 a subsequent domain or an additional domain controller as a container admin.

  For example, `ou=OESSystemObjects,dc=parent,dc=com` where `dc=parent,dc=com` is the forest root domain.
- Supervisor rights on the configuration partition and schema partition to create a subsequent domain or an additional domain controller.

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

For more information on installing a secondary server into an existing tree as a non-administrator user, refer to the *eDirectory 9.2.x Installation Guide* (https://www.netiq.com/documentation/edirectory-92/edir_install/data/a7ivcnh.html).

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

4a On an existing OES server, run the Novell Schema tool found in *YaST > Open Enterprise Server > Novell Schema Tool* and specify the IP address of the eDirectory server with a writable replica of the root.

or

Use the OES schema tool or iManager to extend the schema.

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

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

5 Use YaST with container admin credentials to configure OES DSfW.

For information on installing and configuring the OES DNS service, refer to "Installing the DNS Server" and "eDirectory Permissions " in the *DNS/DHCP Services for Linux 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.

7.2 Installing DSfW Using AutoYaST

DSfW AutoYaST Installation feature enables you to install and configure DSfW without any manual intervention. You can use this feature to install DSfW for a new forest domain, new domain in an existing forest, and new domain controller in an existing domain.

To use DSfW AutoYaST feature, you must first download the template file for Name-Mapped or Non-Name-Mapped installation scenarios and then modify the values of certain tags to install a Forest Root Domain (FRD), Additional Domain Controller (ADC), or Child domain controller (CDC).

The following sections will take you through the procedure to install DSfW using AutoYaST.

- Section 7.2.1, "Prerequisites," on page 72
- Section 7.2.2, "Installing DSfW," on page 72
- Section 7.2.3, "Modifying Template Files," on page 72

7.2.1 Prerequisites

- Modified template file that must be copied to a web server.
- A boot scenario set up. You can boot from media or from an installation source.

- One or more target computers to install the server software to and the following information about each:
  - Hostip
  - Netmask
  - Gateway
  - Install path of SUSE iso
  - Path of the modified template file located on the web server
- To determine the NCP server object location, follow the guideline given below:

  The NCP server object of the DSfW domain controller that is being configured must be placed under the container `ou=0ESSystemObjects`. This container is present or created below the eDirectory partition that is mapped to the DSfW domain.

  For example, assume that the partition `ou=example,o=organization` is being mapped to a DSfW domain. The NCP server object container will be `ou=0ESSystemObject,ou=example,o=organization`.

7.2.2 Installing DSfW

1. Download the template file and modify parameters in the template file based on your installation scenario. For more information, see Section 7.2.3, “Modifying Template Files,” on page 72.
2. Copy the modified template file to a web server.
3. Start the target server and specify the following options during boot up:
   - Hostip- IP address of the target server.
   - Netmask-Subnet mask of the network.
   - Gateway- Gateway IP address of the network
   - Install- SLES iso path
   - Autoyast- Complete path (including filename) of the modified template file in the web server.

Modifications to the template file depends on the installation scenarios. Following sections take you through the various installation scenarios and the modifications required.

7.2.3 Modifying Template Files

Follow the sections below to modify the template files based on your installation scenario.

- “Name-Mapped Environment” on page 73
- “Non-Name-Mapped Environment” on page 75

Name-Mapped Environment

Template file modifications for eDirectory tags in name-mapped environment

Table 7-1 *Template file modifications for eDirectory tags in a name-mapped installation*

Tag	FRD	ADC	CDC
<domain_name>	<domain name>	Empty when it is not DNS server and <Domain name> when it is DNS server	Empty when it is not DNS server and <Domain name> when it is DNS server
<group_context>	FQDN of the DNS group object	FQDN of the DNS group object	FQDN of the DNS group object
<host_name>	<Hostname>	<Hostname> when it is DNS server or Empty when it is not DNS server	<Hostname> when it is DNS server or Empty when it is not DNS server
<ldap_basedn>	FQDN of the DNS objects container	Empty when it is not DNS server and FQDN of the DNS objects container, when it is DNS server	Empty when it is not DNS server and FQDN of the DNS objects container, when it is DNS server
<ldap_server>	<FRD IP address>	Empty when it is not DNS server and ADC IP address when it is DNS server	Empty when it is not DNS server and CDC IP address when it is DNS server
<locater_context>	FQDN of the base container that has the DNS locator object.	FQDN of the base container that has the DNS locator object.	FQDN of the base container that has the DNS locator object.
<replica_server>	IP address of the existing eDirectory replica server	IP address of the existing eDirectory replica server	IP address of the existing eDirectory replica server
<runtime_admin>	cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the FRD base container>	Empty when it is not DNS server and cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the domain root partion > when it is DNS server	Empty when it is not DNS server and cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the domain root partion > when it is DNS server
<runtime_admin_password>	Specify the common proxy DNS password.	Empty or Specify the common proxy DNS password.	Specify the common proxy DNS password.
<server_context>	ou=OESSystemObjects.<FQDN of the FRD base container>	ou=OESSystemObjects.<FQDN of the domain root partion>	ou=OESSystemObjects.<FQDN of the domain root partition>

Tag	FRD	ADC	CDC
<server_object>	cn=DNS_edir<hostname>,ou=OESSystemObjects,<FQDN of the FRD base container>	cn=DNS_edir<hostname>,ou=OESSystemObjects,<FQDN of the domain root partition>	cn=DNS_edir<hostname>,ou=OESSystemObjects,<FQDN of the domain root partition>
<tree_type>	existing	existing	existing
<xad_admin_password>	Specify the domain administrator password.	Specify the domain administrator password.	Specify the domain administrator password.
<xad_config_dns>	yes	yes or no	yes or no
<xad_convert_existing_container>	yes	Empty	yes
<xad_domain_name>	<FRD domain name>	<domain name> of the domain to which it is added	<CDC domain name>
<xad_domain_type>	forest	controller	domain
<xad_existing_container>	<FQDN of the FRD base container>	Empty	<FQDN of the CDC base container>
<xad_forest_root>	<Domain Name>	<Domain Name>	<Domain Name>
<xad_ldap_admin_context>	<FQDN of tree admin>	<FQDN of tree admin>	<FQDN of tree admin>
<xad_ldap_admin_password>	<tree admin password>	<tree admin password>	<tree admin password>
<xad_netbios>	Unique netBIOS in the subnet	Unique netBIOS in the subnet	Unique netBIOS in the subnet
<xad_parent_domain/>	Empty	Empty	<Domain name>
<xad_parent_domain_address/>	Empty	Empty	IP address of FRD server.
<xad_parent_domain_admin_context/>	Empty	Empty or <FQDN of parent domain administrator>	FQDN of parent domain administrator
<xad_parent_domain_admin_password>	Empty	Empty or <Administrator password>	<Administrator password>
<xad_replicate_partitions/>	Empty	Empty or <yes>	Empty
<xad_retain_policies>	no	no	no
<xad_service_configured>	yes	yes	yes
<xad_site_name>	<Site_Name>	<Site_Name>	<Site_Name>
<xad_wins_server	yes or no	yes or no	yes or no

Template file modifications for OES-Ldap tags in name-mapped environment

Table 7-2 *Template file modifications for OES-Ldap tags in a name-mapped installation*

Tag	FRD	ADC	CDC
<admin_context>	cn=Administrator.cn=Users.<FQDN of the domain root partition >	cn=Administrator.cn=Users.<FQDN of the domain root partition >	cn=Administrator.cn=Users.<FQDN of the domain root partition >
<admin_password>	<Tree admin password>	<Tree admin password>	<Tree admin password>
<ip_address>	<local server's FQDN name>	<local server's FQDN name>	<local server's FQDN name>
<ip_address>	<IP address of the edirectory server>	<IP address of the edirectory server>	<IP address of the edirectory server>
<ip_address>	<IP address of the local server>	<IP address of the local server>	<IP address of the local server>
<proxy_context>	cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the FRD base container>	cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the ADC base container>	cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the CDC base container>
<proxy_password>	Specify the common proxy user password.	Specify the common proxy user password.	Specify the common proxy user password.
<tree_name>	<tree name>	<tree name>	<tree name>
<use_common_proxy>	yes	yes	yes
<xad_tree_admin_context/>	<edirectory admin context>	<edirectory admin context>	<edirectory admin context>
<xad_tree_admin_password>	<Tree admin Password>	<Tree admin Password>	<Tree admin Password>

Non-Name-Mapped Environment

Template file modifications for eDirectory tags in non-name-mapped environment

Table 7-3 *Template file modifications for eDirectory tags in a non-name-mapped installation*

Tags	FRD	ADC	CDC
<domain_name>	<Domain_name>	Empty when it is not DNS server and <Domain name> when it is DNS server	Empty when it is not DNS server and <Domain name> when it is DNS server
<group_context>	FQDN of the DNS group object.	FQDN of the DNS group object.	FQDN of the DNS group object.

Tags	FRD	ADC	CDC
<host_name>	<Hostname>	<Hostname> when it is DNS server or Empty when it is not DNS server	<Hostname> when it is DNS server or Empty when it is not DNS server
<ldap_basedn>	FQDN of the DNS objects container	Empty when it is not DNS server and FQDN of the DNS objects container, when it is DNS server	Empty when it is not DNS server and FQDN of the DNS objects container, when it is DNS server
<ldap_server>	<FRD IP address>	Empty when it is not DNS server and ADC IP address when it is DNS server	Empty when it is not DNS server and CDC IP address when it is DNS server
<locater_context>	FQDN of the base container that has the DNS locator object.	FQDN of the base container that has the DNS locator object.	FQDN of the base container that has the DNS locator object.
<replica_server/>	Empty	IP address of the existing eDirectory replica server	IP address of the existing eDirectory replica server
<runtime_admin>	cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the domain root partion >	Empty when it is not DNS server and cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the domain root partion > when it is DNS server	Empty when it is not DNS server and cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,<FQDN of the domain root partion > when it is DNS server
<runtime_admin_password>	Specify the common proxy DNS password.	Empty or Specify the common proxy DNS password.	Empty or Specify the common proxy DNS password.
<server_context>	ou=OESSystemObjects.dc=<FQDN of the domain root partition>	ou=OESSystemObjects.<FQDN of the domain root partition>	ou=OESSystemObjects.<FQDN of the domain root partition>
<server_object>	cn=DNS_edir-<hostname>, ou=OESSystemObjects,<FQDN of the domain root partition >	cn=DNS_edir-<hostname>, ou=OESSystemObjects,<FQDN of the domain root partition >	cn=DNS_edir-<hostname>,ou=OESSystemObjects,<FQDN of the domain root partition >
<tree_type>	New	existing	existing
<xad_admin_password>	<admin_Password>	<admin_Password>	<admin_Password>
<xad_config_dns>	Yes	yes or no	yes or no
<xad_convert_existing_container>	Empty	Empty	Empty
<xad_domain_name>	<Domain_name_of_FRD>	<Domain_name_of_PDC> (To whichever domain this ADC is added)	<Domain_name_of_CDC>

Tags	FRD	ADC	CDC
<xad_domain_type>	forest	controller	domain
<xad_existing_container/>	Empty	Empty	Empty
<xad_forest_root>	<Domain_Name>	<FRD_Domain_Name>	<FRD_Domain_Name>
<xad_ldap_admin_context>	cn=xad_provisioning_user.dc=<domain_name_prefix>,dc=<domain_name_suffix>	cn=Administrator.cn=Users.dc=<domain_name_of_frd prefix>.dc=<domain_suffix>	cn=Administrator.cn=Users.dc=<domain name_of_frd prefix>.dc=<domain suffix>
<xad_ldap_admin_password>	Password of domain administrator	Password of domain administrator	Password of domain administrator
<xad_netbios>	Unique netBIOS in the subnet	Unique netBIOS in the subnet	Unique netBIOS in the subnet
<xad_parent_domain/>	Empty	Empty	Domain name of FRD server.
<xad_parent_domain_address/>	Empty	Empty	IP address of FRD server
<xad_parent_domain_admin_context/>	Empty	Empty if it is ADC for FRD or cn=Administrator.cn=Users.<FQDN of domain root partition> for any child partitions	cn=Administrator.cn=Users.<FQDN of domain root partition of parent domain>
<xad_parent_domain_admin_password>	Empty	Empty or <Administrator_Password>	<Administrator Password>
<xad_replicate_partitions/>	Empty	Empty	Empty
<xad_retain_policies>	no	no	no
<xad_service_configured>	yes	yes	yes
<xad_site_name>	<Site_Name>	<Site_Name>	<Site_Name>
<xad_wins_server	yes or no	yes or no	yes or no

Template file modifications for OES-Ldap tags non-name-mapped environment

Table 7-4 *Template file modifications for OES-Ldap tags in a non-name-mapped installation*

Tags	FRD	ADC	CDC
<admin_context>	cn=Administrator.cn=Users.dc=<domain_name_prefix>.dc=<domain_name_suffix>	cn=Administrator.cn=Users.dc=<domain_name_prefix>.dc=<domain_name_suffix>	cn=Administrator.cn=Users.dc=<domain_name_prefix>.dc=<domain_name_suffix>
<admin_password>	<Password of domain administrator>	<Password of domain administrator>	<Password of domain administrator>
<ip_address>	<local server's FQDN name>	<local server's FQDN name>	<local server's FQDN name>
<ip_address>	<IP address of local server>	<IP address of any dsfw server in the same domain or parent domain>	<IP address of any dsfw server in the same domain or parent domain>
<ip_address>	NA	IP address of the local server	IP address of the local server
<proxy_context>	cn=OESCommonProxy_<hostname>,ou=OESSystemObjects,dc=<domain name prefix>,dc=<domain name suffix>	cn=OESCommonProxy_<hostname_of_ADC>,ou=OESSystemObjects,dc=<domain name prefix>,<domain name suffix>	cn=OESCommonProxy_<hostname_of_cdc>,ou=OESSystemObjects,<FQDN of the base container>
<proxy_password>	Specify the common proxy user password.	Specify the common proxy user password.	Specify the common proxy user password.
<tree_name>	<edirectory tree name>	<edirectory tree name>	<edirectory tree name>
<use_common_proxy>	yes	yes	yes
<xad_tree_admin_context/>	Empty	cn=Administrator.cn=Users.dc=<FRD_domain_name_prefix>.dc=<domain_name_suffix>	cn=Administrator.cn=Users.dc=<FRD_domain name_prefix>.dc=<domain_name_suffix>
<xad_tree_admin_password>	Empty	Password	Password

8 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.

- Section 8.1, “What Is Provisioning?,” on page 79
- Section 8.2, “Features and Capabilities of the Provisioning Wizard,” on page 79
- Section 8.3, “Provisioning Wizard Interface,” on page 80
- Section 8.4, “Using the Wizard to Provision the DSfW Server,” on page 82
- Section 8.5, “Provisioning Tasks,” on page 83
- Section 8.6, “Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios,” on page 89
- Section 8.7, “Logging,” on page 92
- Section 8.8, “Troubleshooting,” on page 93
- Section 8.9, “Executing Provisioning Tasks Manually,” on page 101

8.1 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.

8.2 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/lib64/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.

- **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. A validation is done to ensure that the task that is skipped has been performed manually. The logging feature is available only for tasks performed through the Provisioning Wizard. If you execute tasks manually by using the process in Section 8.9, “Executing Provisioning Tasks Manually,” on page 101, 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.

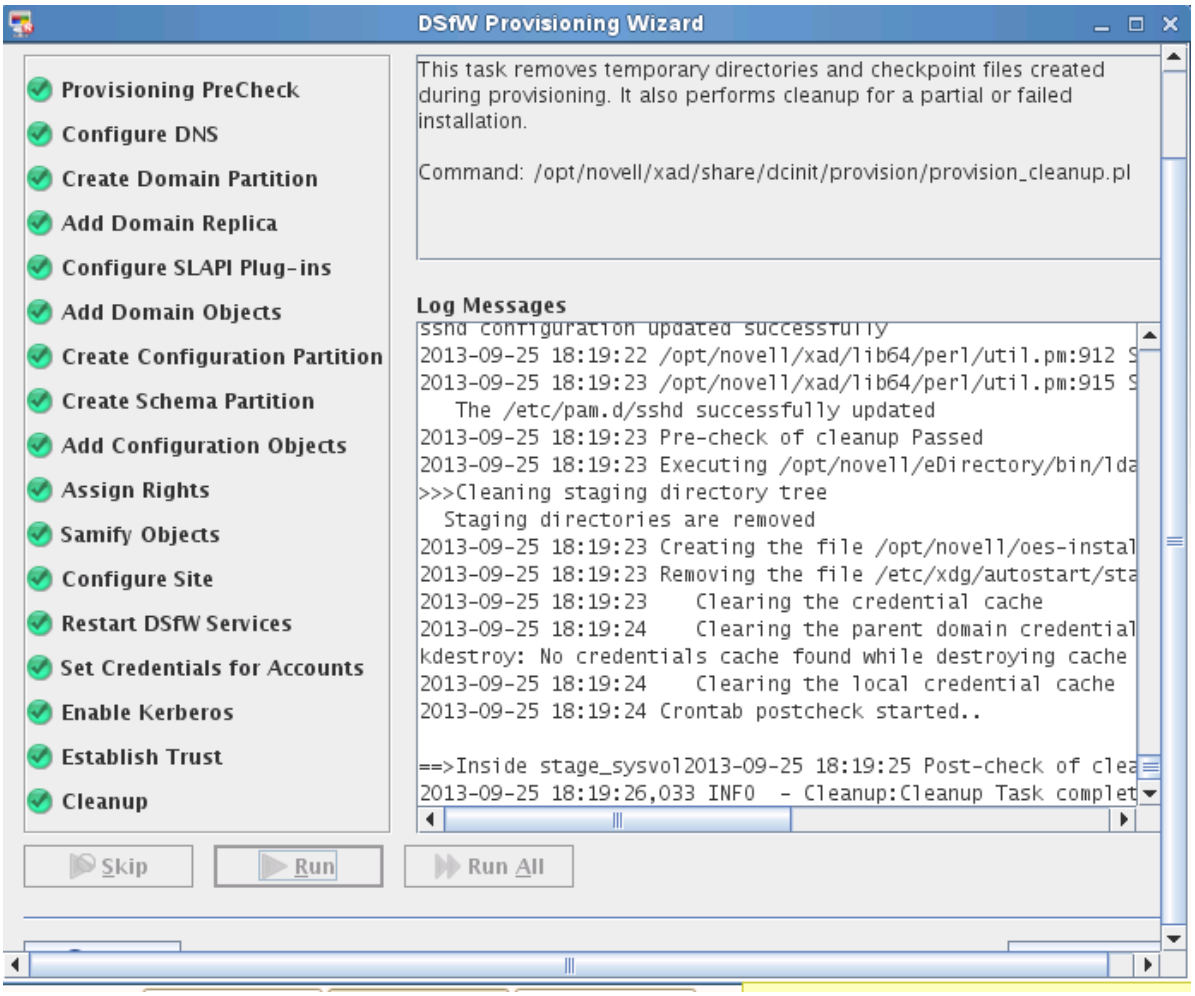
- **Error Handling and Logging** : During execution of each provisioning task, any errors or warnings are logged in the `/var/opt/novell/xad/log/provisioning.log` file. The log file records details and error codes that help you when you need to debug errors. For more information about logging, see Section 8.7, “Logging,” on page 92.

8.3 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 8-1 *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 8.6, “Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios,” on page 89.

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 8.7, “Logging,” on page 92.

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

Table 8-1 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.

8.4 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 8-2 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.
additional 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 Step 3.

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.

8.5 Provisioning Tasks

NOTE: To know about the provisioning tasks associated with each installation scenario, see Section 8.6, "Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios," on page 89.

The Provisioning Wizard lets you perform the following tasks:

- Section 8.5.1, "Provisioning Precheck," on page 84
- Section 8.5.2, "Configure DNS," on page 84
- Section 8.5.3, "Configure DNS and WINS," on page 85
- Section 8.5.4, "Create Domain Partition," on page 85
- Section 8.5.5, "Add Domain Replica," on page 86
- Section 8.5.6, "Configure SLAPI Plug-Ins," on page 86
- Section 8.5.7, "Add Domain Objects," on page 86
- Section 8.5.8, "Create Configuration Partition," on page 86
- Section 8.5.9, "Create Schema Partition," on page 86
- Section 8.5.10, "Add Configuration Objects," on page 87
- Section 8.5.11, "Add Domain Controller," on page 87
- Section 8.5.12, "Assign Rights," on page 87
- Section 8.5.13, "Samify Objects," on page 87
- Section 8.5.14, "Configure Site," on page 87

- Section 8.5.15, “Restart DSfW Services,” on page 88
- Section 8.5.16, “Set Credentials for Accounts,” on page 88
- Section 8.5.17, “Enable Kerberos,” on page 88
- Section 8.5.18, “Establish Trust,” on page 88
- Section 8.5.19, “Cleanup,” on page 89

8.5.1 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, 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.

8.5.2 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 OES 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.

8.5.3 Configure DNS and WINS

This task configures DNS and WINS on the DSfW server. DSfW uses DNS as its location service, enabling computers to find the location of domain controllers. You can also configure a DSfW server as a WINS server. WINS is a name server and service for NetBIOS computer names. It provides NetBIOS name to IP address mapping for the client workstations in different subnets.

As part of DNS configuration, 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 OES DNS and needs at least one DNS server to run on a domain controller, but there are future plans to provide support for any DNS server capable of supporting secure DNS updates.

By default, the DNS server is configured on the first domain controller in a forest. For any additional domain controller in the forest, you can either use the existing DNS server in the forest or configure this server as a DNS server. Before configuring any additional domain controller in the domain, ensure that the nameserver entry in `/etc/resolv.conf` points to the DNS server that the first domain controller of the domain is using.

As part of WINS configuration, the following actions are performed:

- The DNS entry in the corresponding zone object is created.
- The `/etc/samba/smb.conf file` is updated with the parameters required for Samba services to act as a WINS server.
- The nmb process is restarted.

The post-check operation for the task checks if the DNS entry and data files corresponding to WINS are created.

8.5.4 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.

8.5.5 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.

8.5.6 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.

8.5.7 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.

8.5.8 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.

8.5.9 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 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.

8.5.10 Add Configuration Objects

This task adds the configuration and schema partition objects.

It helps maintain integrity with the Active Directory information model.

8.5.11 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.

8.5.12 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.

8.5.13 Samify Objects

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.

8.5.14 Configure Site

This task partitions the domain controller object (mSDS:Server), which is represented as a container object in eDirectory. This domain controller object is located under `cn=Servers,cn=<sitename>,cn=Sites,cn=Configuration,dc=<domain name>`

This task performs the following actions:

- Pre-checks the DSfW environment before partitioning of the object.
- Partitions the domain controller object.
- Post-checks the DSfW environment after partitioning of the object.

8.5.15 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. nmbd (NMB server, NETBIOS lookup)
9. winbindd
10. smbd (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.

8.5.16 Set Credentials for Accounts

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

8.5.17 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.

8.5.18 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.

8.5.19 Cleanup

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

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

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

Table 8-3 *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 **NOTE:** If you have selected the `Configure this server as a WINS server` option in YaST, the Configure DNS and WINS task is executed instead of the Configure DNS task. ◆ Create Domain Partition ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Samify Objects ◆ Configure Site ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Cleanup

Installation Scenario	Provisioning Tasks
Installing DSfW in a Name-Mapped Setup (Forest Root Domain)	◆ Provisioning Precheck ◆ Configure DNS **NOTE:** If you have selected the `Configure this server as a WINS server` option in YaST, the Configure DNS and WINS task is executed instead of the Configure DNS task. ◆ Add Domain Replica ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Samify Objects ◆ Configure Site ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Cleanup
Installing DSfW in a Name-Mapped Setup (Child domain)	◆ Provisioning Precheck ◆ Configure DNS **NOTE:** If you have selected the `Configure this server as a WINS server` option in YaST, the Configure DNS and WINS task is executed instead of the Configure DNS task. ◆ Add Domain Replica ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Samify Objects ◆ Configure Site ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Establish Trust ◆ Cleanup

Installation Scenario	Provisioning Tasks
Installing DSfW in a Non-Name-Mapped Setup (Child domain)	◆ Provisioning Precheck ◆ Configure DNS **NOTE:** If you have selected the `Configure this server as a WINS server` option in YaST, the Configure DNS and WINS task is executed instead of the Configure DNS task. ◆ Create Domain Partition ◆ Add Domain Replica ◆ Configure SLAPI Plug-Ins ◆ Add Domain Objects ◆ Create Configuration Partition ◆ Create Schema Partition ◆ Add Configuration Objects ◆ Assign Rights ◆ Samify Objects ◆ Configure Site ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Establish Trust ◆ Cleanup
Installing DSfW as an additional 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 ◆ Configure Site ◆ Restart DSfW Services ◆ Set Credentials for Accounts ◆ Enable Kerberos ◆ Configure DNS **NOTE:** If you have selected the `Configure this server as a WINS server` option in YaST, the Configure DNS and WINS task is executed instead of the Configure DNS task. ◆ Cleanup

8.7 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 8-4 *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 8-5 *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.

8.8 Troubleshooting

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

- Section 8.8.1, “Troubleshooting Provisioning Tasks,” on page 93

8.8.1 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 93
- “Configure DNS” on page 94
- “Configure SLAPI Plug-in” on page 94
- “Create Domain Partition” on page 95
- “Add Domain Replica” on page 96
- “Add Domain Objects” on page 97
- “Create Configuration Partition” on page 97
- “Create Schema Partition” on page 98
- “Add Configuration Objects” on page 99
- “Assign Rights” on page 99
- “Establish Trust” on page 100
- “Update Service Configuration” on page 100
- “Cleanup” on page 101

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 in the NetIQ eDirectory Administration Guide.

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 94
- "Entry already Exists" on page 94
- "ldapmodify Failed" on page 94

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)

Configure SLAPI Plug-in

- "Error: Insufficient Access" on page 95
- "Entry already Exists" on page 95
- "ldapmodify Failed" on page 95

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 95
- “Error: 625 Transport Failure/ Unknown Error” on page 95
- “Error: 30 Retry Entries to Get the Replica Status in the Log File” on page 96

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, Section 8.9, “Executing Provisioning Tasks Manually,” on page 101.

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 96
- “Error: 625 Transport Failure/ Unknown Error” on page 96
- “Error: 30 Retry Entries to Get the Replica Status in the Log File” on page 96

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, Section 8.9, “Executing Provisioning Tasks Manually,” on page 101.

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 97
- "Entry already Exists" on page 97
- "ldapmodify Failed" on page 97

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 97
- "Error: 625 Transport Failure/ Unknown Error" on page 98
- "Error: 30 Retry Entries to Get the Replica Status in the Log File" on page 98

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, Section 8.9, “Executing Provisioning Tasks Manually,” on page 101.

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 98
- “Error: 625 Transport Failure/ Unknown Error” on page 98
- “Error: 30 Retry Entries to Get the Replica Status in the Log File” on page 99

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, Section 8.9, “Executing Provisioning Tasks Manually,” on page 101.

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 99
- "Entry already Exists" on page 99
- "ldapmodify Failed" on page 99

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 100
- "Entry already Exists" on page 100
- "ldapmodify Failed" on page 100

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.

8.9 Executing Provisioning Tasks Manually

This section details the method of Provisioning DSfW server by using command line scripts.

- Section 8.9.1, “Exporting Passwords,” on page 101
- Section 8.9.2, “Provisioning Tasks,” on page 102

8.9.1 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 8-6 *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
Additional Domain Controller	export ADM_PASSWD=current domain password
	export NDSEXISTINGADMINPASSWD=tree domain password

8.9.2 Provisioning Tasks

NOTE: To know about the provisioning tasks associated with each installation scenario, see Section 8.6, “Provisioning Tasks for Name-Mapped and Non-Name-Mapped Scenarios,” on page 89.

- “Provisioning Precheck” on page 102
- “Configure DNS” on page 102
- “Configure DNS and WINS” on page 103
- “Create Domain Partition” on page 103
- “Add Domain Replica” on page 104
- “Configure SLAPI Plug-ins” on page 104
- “Add Domain Objects” on page 104
- “Create Configuration Partition” on page 104
- “Create Schema Partition” on page 105
- “Add Configuration Objects” on page 105
- “Add Domain Controller” on page 105
- “Assign Rights” on page 105
- “Samify Objects” on page 105
- “Configure Site” on page 106
- “Restart DSfW Services” on page 106
- “Set Credential for Accounts” on page 106
- “Enable Kerberos” on page 106
- “Establish Trust” on page 106
- “Cleanup” on page 107

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 passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_precheck.pl
```

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 passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_dns.pl
```

Configure DNS and WINS

This task configures DNS and WINS on the DSfW server. DSfW uses DNS as its location service, enabling computers to find the location of domain controllers. You can also configure a DSfW server as a WINS server. WINS is a name server and service for NetBIOS computer names. It provides NetBIOS name to IP address mapping for the client workstations in different subnets.

As part of DNS configuration, 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 OES DNS and needs at least one DNS server to run on a domain controller, but there are future plans to provide support for any DNS server capable of supporting secure DNS updates.

By default, the DNS server is configured on the first domain controller in a forest. For any additional domain controller in the forest, you can either use the existing DNS server in the forest or configure this server as a DNS server. Before configuring any additional domain controller in the domain, ensure that the nameserver entry in `/etc/resolv.conf` points to the DNS server that the first domain controller of the domain is using.

As part of WINS configuration, the following actions are performed:

- The DNS entry in the corresponding zone object is created.
- The `/etc/samba/smb.conf file` is updated with the parameters required for Samba services to act as a WINS server.
- The nmb process is restarted.

The post-check operation for the task checks if the DNS entry and data files corresponding to WINS are created.

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
```

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
```

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 passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_config_slapi.pl
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

Configure Site

This task partitions the domain controller object (mSDS:Server), which is represented as a container object in eDirectory. This domain controller object is located under `cn=Servers,cn=<sitename>,cn=Sites,cn=Configuration,dc=<domain name>`

This task performs the following actions:

- Pre-checks the DSfW environment before partitioning of the object.
- Partitions the domain controller object.
- Post-checks the DSfW environment after partitioning of the object.

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
```

Set Credential for Accounts

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

After you have exported the passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_set_cred_foraccounts.pl
```

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
```

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 passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_trusts_crossref.pl
```

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 passwords, execute the following script:

```
/opt/novell/xad/share/dcinit/provision/provision_cleanup.pl
```

9 Types of Accounts in DSfW

The DSfW environment includes different types of user accounts and group accounts. Some of the accounts are created during installation and the rest by administrators. The administrators create accounts related to the persons in the organization.

- Default User Accounts

  The user accounts created by default are krbtgt, guest, and administrator.

  Each time a domain controller is added to the domain, it creates a machine account for that domain controller and a corresponding proxy user account. The domain controller account names are suffixed with $. For example, if the hostname of the domain controller is *dsfw-dc1*, then the machine account for that domain controller is *dsfw-dc1$* and the proxy user account is *oescommonproxy_dsfw-dc1*.

  An account is created for every workstation or member server that joins the domain. These account names are also suffixed with $. For example, if the name of the workstation is *Desktop-AEIOU*, then the workstation account created is *Desktop-AEIOU$*.

- Default Group Accounts

  The group accounts created by default are Group Policy Creator Owners, Domain Guests, Domain Admins, Cert Publishers, Domain Controllers, Domain Computers, Domain User, dnsupdateproxy, dhcp administrators, dhcp users, telnet clients, help services dns-dhcp group, enterprise admins, schema admins.

10 Activities After DSfW Installation or Provisioning

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

- Section 10.1, “Verifying the Installation,” on page 111
- Section 10.2, “Renaming Administrator Details Using MMC,” on page 113
- Section 10.3, “Extending the Domain Post Provisioning,” on page 113
- Section 10.4, “Updating the Domain Functional Level and Forest Functional Level,” on page 116
- Section 10.5, “Validating the Schema Update,” on page 116
- Section 10.6, “Validating Domain and Forest Functional Level,” on page 117

10.1 Verifying the Installation

Perform these tasks to verify that eDirectory and DSfW have been installed and configured correctly. These tasks might require certain environment variable settings to be updated. You must either restart the OES server or logout of the OES server and login again to update the necessary environment variables.

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

```
systemctl-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
  ```

- ❒ If you reconfigure the LAN settings using YaST, ensure that the loopback IP address. .(except 127.0.0.1) is not active in `/etc/hosts`.
- ❒ 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:

```
frd:~ # xadcntrl validate
Validating dependent services
Checking for novell-xregd daemon
running
Checking for micasad daemon
running
Checking for service sshd
running
Checking for rsync daemon
running

Validating DSfW
Checking for eDirectory Server
running
Checking for nameserver BIND
running
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
```

- ❒ Execute the following commands:

```
kinit administrator@domainname

KRB5CCNAME=/tmp/krb5cc_<UID> rpcclient -k <hostname> –c dsroledominfo
```

  Entering `KRB5CCNAME=/tmp/krb5cc_<UID>` manually ensures that the rpcclient looks for the kerberos credential cache, which is required for the kerberos authentication, in the correct location.

  <*UID*> is the UNIX user ID of the current user in the decimal format. For example, the UID for the root user is 0. The <*hostname*> is the system hostname and not IP address or localhost.

  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.
```

10.2 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 25.1.30, “iManager Fails to Create Samba Shares if the Administrator Name is Changed using MMC,” on page 207.

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**.

10.3 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.
--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.

Operation	Description
--preps	Prepares the server with the following sequence of activities: **Schema version check:** Checks the Schema version to determine if the version on the server is OES 2 SP3 or later. If the schema version is lesser than OES 2 SP3, an error message is displayed suggesting the user to extend the schema on the server and abort the operation. **uniqueDomainID attribute check:** Searches for `uniqueDomainID` attribute on the domain root. If attribute is not found, the attribute is updated on the domain root. **Samification:** Samifies all the objects in the eDirectory partition that is mapped to the DSfW domain. **NOTE:** This option must be used only if the server is migrated from OES 2 SP2.
--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.

10.3.1 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.

10.4 Updating the Domain Functional Level and Forest Functional Level

To update the Domain Functional Level to AD 2012: Re-run the script `/opt/novell/xad/sbin/domainUpgrade.pl -D` on the Primary Domain Controller of each domain.

To update the Forest Functional Level to AD 2012: Re-run the script `/opt/novell/xad/sbin/domainUpgrade.pl -F` on the Primary Domain Controller of Forest Root Domain.

10.5 Validating the Schema Update

When the schema level is updated from AD 2003 to AD 2012, of new objects and attribute definitions are added. In the following example, a sample attribute `msds-SupportedEncryptionTypes` is used for validating the schema update. For comparison you can use another DSfW server as a reference server which is at AD2003 level.

1. On updating to AD 2012, the attribute `msds-SupportedEncryptionTypes` is available in the `/var/opt/novell/eDirectory/schema.log` file.
2. Verify all the services are running by using the command `#xadcntrl status`.
3. Log in to iManager using the domain or eDirectory credential.
4. Click **Roles & Tasks** > **Schema** > **Attribute Information**.

   The following new attributes are added in the domain:

   - `msds-SupportedEncryptionTypes`
   - `msds-PasswordComplexityEnabled`
   - `msds-PasswordHistoryLength`
   - `msds-PasswordRevEncEnabled`
   - `msds-PasswordSettingsPrecedence`

   These attributes are not available in the schema of AD 2003 server.
5. Export the schema on the server by using the command:

   `# ldapsearch -b cn=schema -s base -x -o ldif-wrap=200 >/tmp/after-schema-upgrade`.
6. Verify the dump file `after-schema-upgrade` for new attributes. These attributes are not available in the schema dump of the reference server.

10.6 Validating Domain and Forest Functional Level

Domain Functional Level refers to a set of attribute values that help applications to determine the functional level of the domain. That is, to determine whether it is at the schema level AD 2003 or AD 2012.

To Validate the Domain functional Level: In the MMC, click **Active Directory Domains and Trusts**, right-click **Domain**, then select **Raise Domain Functional Level**.

A message appears stating the Domain functional level. AD 2012 for the updated server and AD 2003 for the reference server used for validation.

To Validate the Forest Functional Level: In the MMC, right-click **Active Directory Domains and Trusts**, right-click **Domain**, then select **Raise Forest Functional Level**.

A message appears stating the Forest functional level. AD 2012 for the updated server and AD 2003 for the reference server used for validation.

11 Upgrading DSfW

This section provides information and links for upgrading DSfW to OES 24.4.

- Section 11.1, “Upgrading DSfW to OES 24.4,” on page 119
- Section 11.2, “Migrating Data to a Domain Services for Windows Server,” on page 121

11.1 Upgrading DSfW to OES 24.4

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

- Section 11.1.1, “Upgrade Scenario,” on page 119
- Section 11.1.2, “Prerequisite,” on page 119
- Section 11.1.3, “Media Upgrade,” on page 120
- Section 11.1.4, “AutoYaST Upgrade,” on page 120
- Section 11.1.5, “Configuring WINS and Sites in an Upgrade Scenario,” on page 120
- Section 11.1.6, “Troubleshooting,” on page 121

Before upgrading to OES 2018 SP1, if the file `smb.conf.oes2018-upgrade-save` exists, ensure that it contains the DSfW Samba configuration. If it does not contain the DSfW Samba configuration, copy the configuration information from the `smb.conf` file by using the following command:

```
cp /etc/samba/smb.conf{,.oes2018-upgrade-save}
```

11.1.1 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.

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.

11.1.2 Prerequisite

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

- If you are upgrading a CDC or an ADC to OES 24.4, you must also upgrade all the other domain controllers (FRD, ADC, and CDC) in the DSfW forest to OES 24.4. Mixed mode configuration is not supported in OES 24.4.

  If such a configuration is attempted, a message is displayed warning you to upgrade all the domain controllers to the same version of OES for the domain to become operational.

11.1.3 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" in the *Installation Guide*.

11.1.4 AutoYaST Upgrade

AutoYaST upgrade enables you to upgrade to an OES server without user intervention. For more information, see "Using AutoYaST for OES Upgrade" in the *Installation Guide*.

11.1.5 Configuring WINS and Sites in an Upgrade Scenario

After you upgrade your server to OES 24.4, the server reboots and you are prompted to configure additional features like WINS and Sites. This can be done using the DSfW Configuration Wizard. If you are configuring DSfW at runlevel 3, you will not be prompted to configure additional features like WINS and Sites. In this case, you must start the X server and launch the DSfW Configuration Wizard manually using the command: `/opt/novell/xad/sbin/provision_dsfw.sh`

IMPORTANT: You are prompted to configure these features only once. If you fail to configure these features during the first instance, you will not be able to configure these features later.

1 Enter the authentication details in the login dialog box, depending on the scenario in which you are provisioning, then click **OK.**

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

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

2 Select the feature that you want to configure, then click **Next**.

3 On the task list page, click **Run** to manually execute a task or click **Run All** to execute all the tasks sequentially without any manual intervention.

11.1.6 Troubleshooting

- "Samba cache File Corruption" on page 121
- "Upgrade Fails" on page 121

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 211 to resolve the error.

Upgrade Fails

If upgrade to OES 24.4 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.

Upgrade to OES 24.4: 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 <Administrator Name>
```

11.2 Migrating Data to a Domain Services for Windows Server

The migration of data to an OES 24.4 server running DSfW is similar to any other data migration to OES 24.4:

- You should use the OES 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 migration tools for migrating data, see the *Migration Tool Administration Guide*.

12 Activities After Upgrade or Migration

Beginning with OES 2023, DSfW supports schema level and features equivalent to AD 2019. After the domain upgrade, the schema level gets updated to AD 2019 level. This section describes the process to upgrade the domain and schema to AD2019 level.

- Section 12.1, “Updating the Domain Functional Level and Forest Functional Level,” on page 123
- Section 12.2, “Validating the Schema Update,” on page 123
- Section 12.3, “Validating Domain and Forest Functional Level,” on page 124

12.1 Updating the Domain Functional Level and Forest Functional Level

If the upgrade is being performed from OES 2018SP1 or below:

To update the Domain Functional Level: Re-run the script `/opt/novell/xad/sbin/domainUpgrade.pl -D` on the Primary Domain Controller of each domain.

To update the Forest Functional Level: Re-run the script `/opt/novell/xad/sbin/domainUpgrade.pl -F` on the Primary Domain Controller of Forest Root Domain.

If the upgrade is being done from OES 2018SP2 level, there is no need to run `domainUpgrade.pl` with above mentioned options as there is no functional level change in OES 2018SP2 and OES 2018SP3. The DS-Behavior-Version remains same as 7.

12.2 Validating the Schema Update

When the schema level is updated to AD 2019, new objects and attribute definitions are added. In the following example, a sample attribute `msds-preferredDataLocation` is used for validating the schema update. For comparison you can use another DSfW server as a reference server which is at AD2019 level.

1. On updating to AD 2019, the attribute `msds-preferredDataLocation` is available in the `/var/opt/novell/eDirectory/schema.log` file.
2. Verify all the services are running by using the command `#xadcntrl status`.
3. Log in to iManager using the domain or eDirectory credential.
4. Click **Roles & Tasks** > **Schema** > **Attribute Information**.

   The following new attributes are added in the domain from AD 2019:

   - `msds-preferredDataLocation`

   The following new attributes are added in the domain from AD 2016:

   - `msds-DeviceLocation`
   - `msds-KeyCredentialLink-BL`

- `msds-RegistrationQuota`
- `msds-CloudsEnabled`

5 Export the schema on the server by using the command:

```
# ldapsearch -b cn=schema -s base -x -o ldif-wrap=200 >/tmp/after-schema-upgrade
```

6 Verify the dump file `after-schema-upgrade` for new attributes. These attributes are not available in the schema dump of the reference server.

7 Verify the attribute `msds-preferredDataLocation` associated with the new user.

In iManager, click **View Objects** > **Tree** > **Domain Partition** > **Users** > ***Any sample user created using mmc*** > **Other**. The attribute **msds-preferredDataLocation** is available.

12.3 Validating Domain and Forest Functional Level

Domain Functional Level refers to a set of attribute values that help applications to determine the DS-BEHAVIOR-VERSION, also called as functional level of the domain.

To Validate the Domain functional Level: In the MMC, click **Active Directory Domains and Trusts**, right-click **Domain**, then select **Raise Domain Functional Level**.

A message appears stating the Domain functional level Windows Server 2016 for the updated server.

To Validate the Forest Functional Level: In the MMC, right-click **Active Directory Domains and Trusts**, right-click **Domain**, then select **Raise Forest Functional Level**.

A message appears stating the Forest functional level Windows Server 2016 for the updated server.

NOTE: Windows Server 2016 functional level has DS-BEHAVIOR-VERSION value as 7. With AD 2019 schema, there is no change in Functional level from past release AD 2016.

---

13 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) server and requires no special configuration or other changes.

To get started with KVM virtualization, see the Introduction to KVM Virtualization (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-kvm-intro.html) in the SLES Virtualization Guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html) guide.

To get started with XEN virtualization, see Introduction to Xen Virtualization (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-xen-basics.html) in the SLES Virtualization Guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html) guide.

For information on setting up virtualized OES, see “Installing OES on a VM” in the *Installation Guide*.

To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product that you are using.

14 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 14.1, “Joining a Windows Workstation to a DSfW Domain,” on page 127
- Section 14.2, “Logging In to a DSfW Domain,” on page 130
- Section 14.3, “Logging Out,” on page 130
- Section 14.4, “Support for SASL NTLMSSP Bind in LDAP,” on page 131

14.1 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: Joining a Windows workstation to DSfW domain using the NetBIOS name fails.

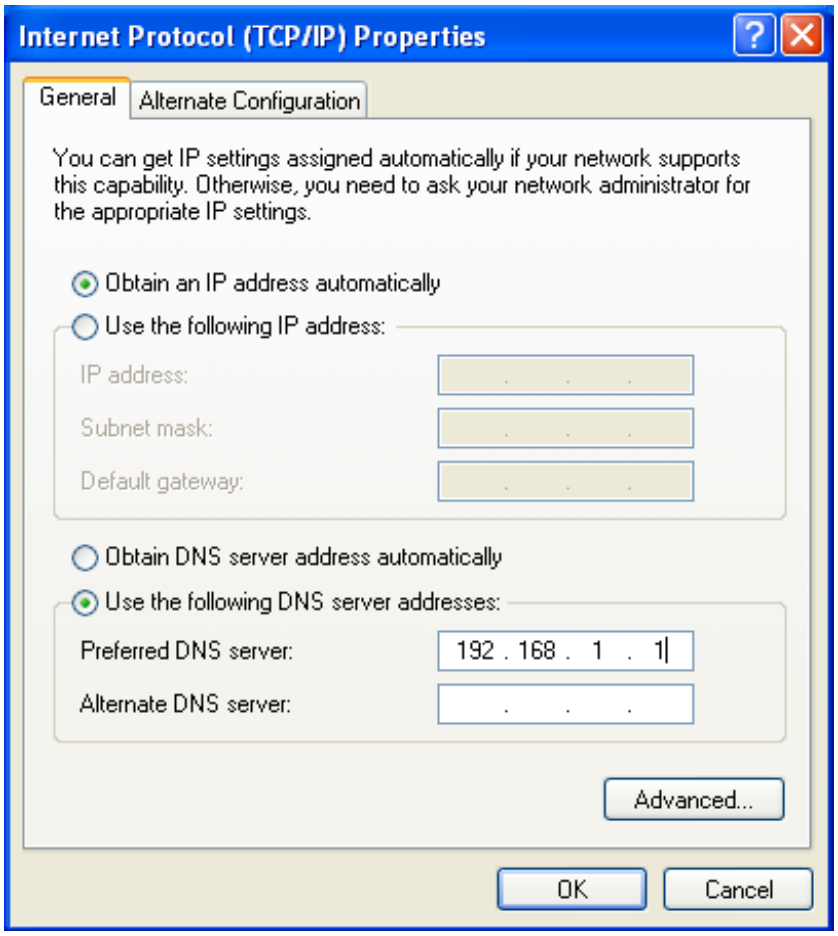
NOTE: A duplicate machine name may get assigned due to reuse of the machine name or re imaging the machines in a virtualized environment.

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.

---

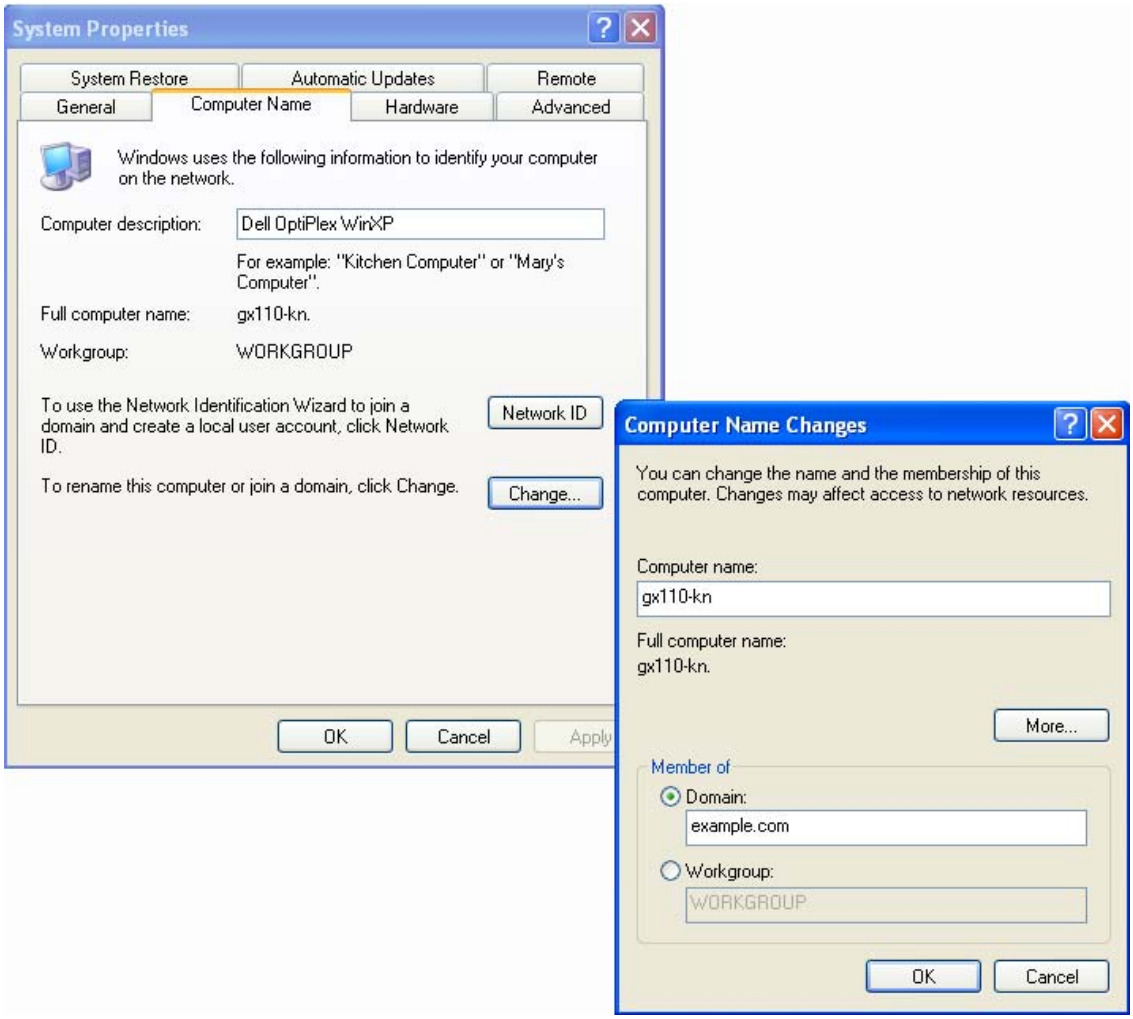
1. From a Windows computer on the same network as the DSfW server, go to Network Connections in the Control Panel, select Local Area Connection, and click **Properties**.
2. Select Internet Protocol (TCP/IP) and click **Properties**.
3. Select **Use the following DNS server addresses**. For the Preferred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

Assume that you join a workstation to the example.com domain. After you join a workstation to the domain, a computer object is created in the default container `cn=computers,dc=example,dc=com`. This default container is by default associated with the default password policy `cn=Default Password Policy,cn=Password Policies,cn=System,dc=example,dc=com`.

The `wellKnownObjects` attribute on the domain container (dc=example,dc=com for the domain example.com) contains a list of well-known object containers by GUID and distinguished name. The well-known objects are system containers. If you want to place all the computer objects under a non-default custom container, you must modify the computers container entry of the `wellKnownObjects` attribute to include the desired container.

1. Launch iManager and connect to a DSfW server.
2. In Roles and Tasks, select **Directory Administration > Modify Object**.
3. Specify the domain container object in the **Object name** field or browse and select the domain container object and click **OK**.
4. Click **General > Other** tab.
5. Select wellKnownObjects from the Valued Attributes list and click **Edit**.
6. Select the entry that contains the GUID AA312825768811D1ADED00C04FD and specify the desired container in the **Volume** field.

After you modify the `wellKnownObjects` attribute entry, ensure that you associate the `cn=Default Password Policy,cn=Password Policies,cn=System,dc=example,dc=com` to the new Computer container. This password policy association is required for all such containers that will hold computer objects.

14.2 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 14.1, “Joining a Windows Workstation to a DSfW Domain,” on page 127), 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**.

14.3 Logging Out

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

14.4 Support for SASL NTLMSSP Bind in LDAP

This feature enables support for LDAP-based applications to authenticate (bind) to a Domain Controller over SASL layer via GSSAPI/GSS-SPNEGO employing NTLM. As part of this feature, DSfW introduces support for NTLM in case Kerberos is down or where a legacy third party application is limited with NTLM support alone. However, applications employing NTLM outside SASL layer will remain unsupported. It is recommended that you avoid NTLM-based authentication, because it is susceptible to attacks. For more information, see NTLM Authentication Protocol.

- Section 14.4.1, “Planning for Support of SASL NTLMSSP Bind in LDAP,” on page 131
- Section 14.4.2, “Troubleshooting,” on page 131

14.4.1 Planning for Support of SASL NTLMSSP Bind in LDAP

To use this feature on Windows XP SP3 or later, you must change the local policy as follows:

1. On a Windows system, click **Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options > Network Security: LAN Manager Authentication Level**
2. Modify the value of the LAN Manager Authentication Level to **Send LM and NTLM -use NTLM2 session security if negotiated**.

14.4.2 Troubleshooting

Use the information in this section to resolve SASL NTLMSSP-based bind issues.

SASL NTLMSSP-Based Bind Over LDAP is Not Working

If there are pre-existing domain controllers prior to OES 11 SP2 in your environment, perform the following steps on these domain controllers:

1. Start the ndstrace process by issuing the `ndstrace -l>log&` command. This runs the process in the background.
2. Force the backlink to run by issuing the `ndstrace -c set ndstrace=*B` command from the ndstrace command prompt.
3. Unload the ndstrace process by issuing the `ndstrace -u` command. Running the backlink process is especially important on servers that do not contain a replica.
4. Restart the ndsd sever by using the `ndsd restart` command.
5. Verify that the size or hash of the `/var/opt/novell/eDirectory/data/nmas-methods/SPNEGOLSMLIN_X64.SO` library matches to that of an OES 2018 or later server.

15 Creating Users

After Domain Services for Windows (DSfW) is properly installed and provisioned, you can create users with either 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.

NOTE: OpenText recommends you to use either iManager or MMC for DSfW user and group management. If you use iManager or MMC interchangeably for DSfW user or group management, then some of the attributes of DSfW users or groups created using MMC will not match with those created using iManager.

- Section 15.1, “Creating Users in iManager,” on page 133
- Section 15.2, “Creating Users in MMC,” on page 134
- Section 15.3, “Creating Filr LDAP Proxy Users,” on page 135
- Section 15.4, “Moving Users Associated with Password Policies,” on page 136
- Section 15.5, “Limitations,” on page 136

15.1 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. For more information about Contextless logins, see “**Contextless Login Using Alternate Object Classes and/or Alternate Attributes**” in the iManager Admin guide (https://www.netiq.com/documentation/imanager-32/imanager_admin/data/bookinfo.html).

   ---

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.

15.2 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 (https://support.microsoft.com/en-in/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems).

1 At a Windows workstation, click **Start** > **Run** and enter `mmc`.

2 When the Console opens, select **File** > **Add/Remove Snap-ins**.

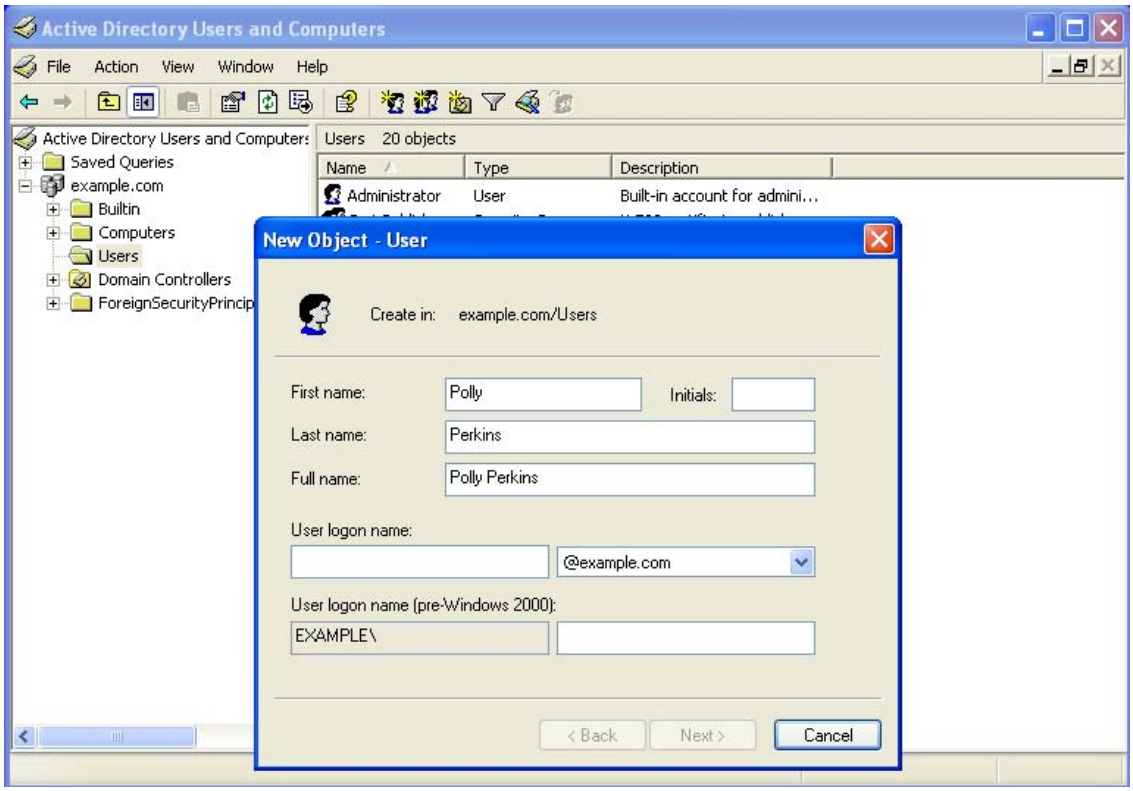
3 Select **Active Directory Users and Computers** and click **Add**.

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.

NOTE: Ensure that the user logon name and the full name that you specify are the same. This is because for an eDirectory user, the full name is the configuration name (cn).

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.

15.3 Creating Filr LDAP Proxy Users

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 Under Roles and Tasks, select **Rights** > **Modify Trustees**.

4 Select the Container object and click **OK**.

5 Click **Add Trustee**.

6 Select a User from any Container.

7 Click **Assigned Rights** for added trustee user.

8 Select **Compare and Read** rights for **All Attribute Rights** entry.

By performing the above mentioned steps, a Domain user gets the rights to read all the attributes of users and groups under particular container, and can be used as LDAP sync proxy user in Filr.

15.4 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.

15.5 Limitations

- Section 15.5.1, “User Samification Fails On Moving Users into a DSfW Domain,” on page 136
- Section 15.5.2, “Moving User Objects Across Containers,” on page 136
- Section 15.5.3, “Primary Group Appears Twice in the memberOf Properties Page,” on page 137
- Section 15.5.4, “Adding Newly Created Users to a Group gives Error Message,” on page 137
- Section 15.5.5, “Dynamic Groups Is Not Supported in DSfW,” on page 137

15.5.1 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.

15.5.2 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.

15.5.3 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.

15.5.4 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.

15.5.5 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.

16 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 OES 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.

OES DNS Services in Open Enterprise Server (OES) 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 the Java Management Console. The OES DNS configuration information is replicated just like any other data in eDirectory.

NOTE: A OES DNS server can only be managed by using the Java Management Console utility. The DNS YaST plug-in or the DNS plug-in of Microsoft Management Console (MMC) do not support managing a OES DNS server.

16.1 DSfW and DNS

DSfW uses the OES 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 *DNS/DHCP Services for Linux 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 16.4, “Migrating DNS to Another Domain Controller,” on page 142

16.1.1 Limitations

- It is not possible to use an existing OES 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 16.2.3, “Configuring a Domain Controller by Using an Existing DNS Server,” on page 141.
- 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

16.2 Understanding DNS Settings in the DSfW Environment

This section explains the configuration changes that happen while DNS is configured for DSfW.

- Section 16.2.1, “General DNS Settings,” on page 140
- Section 16.2.2, “Configuring a Domain Controller as a Primary DNS Server,” on page 141
- Section 16.2.3, “Configuring a Domain Controller by Using an Existing DNS Server,” on page 141

16.2.1 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 Java Management Console uses 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, and the Microsoft Management Console must have access to these objects.

16.2.2 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=0ESSystemObjects,<DomainDN>`.

For a name-mapped setup, the fields are blank and the user can enter any context in the tree.For an additional 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 OES DNS services, see "Installing and Configuring DNS " in the *DNS/DHCP Services for Linux Administration Guide*

16.2.3 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 additional 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.

16.3 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 Java 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 OES DNS server for the changes to take effect by using the `systemctl-named restart` command.

16.4 Migrating DNS to Another Domain Controller

In a typical DSfW deployment, 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 additional 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 additional domain controller execute the following steps:

1 Using the `oescredstore` utility, set the credentials on the additional domain controller with the following command.

```
oescredstore -s -n dns-ldap -u <username> -p <password>
```

To retrieve the common proxy user DN, use the following command:

```
/opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred username
```

To retrieve the common proxy user password, use the following command:

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

2 Using Java Management Console, execute the following steps:

2a Create a DNS server object. For more information, see "Creating a DNS Server Object" in the "*DNS/DHCP Services for Linux Administration Guide*".

While creating the DNS server object you must specify the NCP server name of the additional domain controller, hostname and the domain name for the server object.

2b Select the DNS zones in Java Management Console.

Associate the zone with the DNS server. For details on associating zone with a DNS server, see "Zone Management"in the *DNS/DHCP Services for Linux Administration Guide*

3 Restart novell-named on the additional domain controller using the following command:

```
systemctl-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 `systemctl-named restart` command.

16.5 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:

```
systemctl-named restart
```

For information on updating records, refer to "Understanding DNS and DHCP Services" in the *DNS/DHCP Services for Linux Administration Guide*

17 Understanding AES Encryption for Communication

The AD 2003 level in DSfW used ARCFOUR encryption for communication between Workstations and domain controllers. After the domain upgrade, the encryption also gets upgraded to AES. AES encryption is more secure when compared with ARCFOUR based encryption. The following communications are based on AES in the upgraded server:

- Kerberos AS and TGS requests
- SMB setup connection
- LDAP SASL bind and other requests
- Dcerpc bind and other requests

For information on how to create AES 256-Bit Tree key, see Creating an AES 256-Bit Tree Key in the NICI Administration Guide.

18 Configuring DSfW Server as a WINS Server

This section describes how to configure a DSfW server as a WINS server.

Windows Internet Name Service (WINS) is a service that resolves NetBIOS computer names. It provides NetBIOS name to IP address mapping for the client workstations in different subnets. Without WINS, the NetBIOS to IP address mapping is limited to a single subnet. For example, if you ping a NetBIOS name, the corresponding IP address is returned. Without WINS, this mapping is done only for workstations within a subnet. However, with WINS, this mapping can be done for clients to WINS servers across subnets.

- Section 18.1, “Using WINS in DSfW Environment,” on page 147
- Section 18.2, “Rectifying Duplicate Workstation Names,” on page 150
- Section 18.3, “Verifying Duplicate Workstation Names Prior to WINS Configuration,” on page 152
- Section 18.4, “Troubleshooting,” on page 152

18.1 Using WINS in DSfW Environment

Beginning with OES 11 SP2, you can configure a DSfW server as a WINS server. Configuring a DSfW server as a WINS server helps to prevent having two workstations with the same name in a domain. If a workstation client is configured to use a WINS server, before joining a domain, the administrator is alerted if a workstation with the same name already exists in the domain.

Duplicate workstation names in a domain can lead to several problems. If your domain has duplicate workstations, users might experience slow logins to the domain. Logins might take several minutes instead of seconds. You will also require substantial recovery effort to bring back configuration to a unique workstation name across a domain.

Configuring a DSfW server as a WINS server also changes the NetBIOS join functionality. Without WINS server, a NetBIOS join will not work if there is no domain controller in the subnet. However, with WINS support, the join will work if the workstation's WINS configuration points to a domain controller that is configured as a WINS server.

- Section 18.1.1, “Planning for WINS Support,” on page 148
- Section 18.1.2, “Configuring WINS Server and Client,” on page 148
- Section 18.1.3, “Migrating WINS Server,” on page 149
- Section 18.1.4, “Caveats,” on page 149

18.1.1 Planning for WINS Support

Use the following guidelines to configure a WINS server:

- You can configure only one DSfW domain controller as a WINS server in a domain. All the workstations in the domain must be configured to use this domain controller as the WINS server.
- Microsoft or any other OES server should not be configured as a WINS or a WINS proxy server for the workstations in the domain.
- DSfW server cannot be configured as a WINS proxy server.
- DSfW WINS server helps in detecting workstations with duplicate names. Any other WINS functionality is not supported.
- Ensure that the client workstation's firewall for UDP port 137 is disabled.
- Ensure that the gateways between DSfW server and Windows clients have the UDP port 137 disabled for messages originating from server to workstation.
- If you have a significant number of workstations that are part of the domain, then DHCP service can be used for configuring these workstations as WINS clients.

18.1.2 Configuring WINS Server and Client

- "Configuring WINS Server" on page 148
- "Configuring WINS Client" on page 148

Configuring WINS Server

You can configure WINS server by selecting the **Configure this machine to be a WINS server** check box while installing and configuring DSfW using YaST. For information, see "Configure this machine to be a WINS server:" on page 59.

Configuring WINS Client

1. On a Windows system, click **Start** and point to **Control Panel**.
2. Click **Network and Dial-up Connections > Local Area Connections > Properties**.
3. Select the **Internet Protocol (TCP/IP)** Properties entry in the list and then click **Properties> Advanced > WINS Address** tab.
4. Select the **Disable NetBIOS over TCP/IP** option.
5. Click **Add**.
6. Specify the IP address or the domain name of the WINS server.

18.1.3 Migrating WINS Server

This section describes how to migrate a DSfW WINS server from one domain controller to another.

Before you migrate WINS, ensure that you stop the nmb service on the server where WINS is configured and take a backup of the `wins.dat` and `wins.tdb` files (`/var/lib/samba`). Follow the steps given below to migrate WINS:

1. Verify if WINS is configured on the server by running the following command:

   ```
   /opt/novell/xad/share/dcinit/configure_dsfw_wins.pl --isconfigured-upgrade
   ```

2. Unconfigure WINS on the source server.

   ```
   /opt/novell/xad/share/dcinit/unconfigure_dsfw_wins.pl
   ```

3. Verify if WINS is configured on the server by running the following command:

   ```
   /opt/novell/xad/share/dcinit/configure_dsfw_wins.pl --isconfigured-upgrade
   ```

4. Configure WINS on the target server.

   ```
   /opt/novell/xad/share/dcinit/configure_dsfw_wins.pl
   ```

5. Stop the nmb process in the target server.

   ```
   rcnmb stop
   ```

6. Copy the `wins.dat` and `wins.tdb` files (`/var/lib/samba`) from the source server to the target server.
7. Start the nmb process.

   ```
   rcnmb start
   ```

8. Reconfigure WINS clients to point to the target server. For more information on configuring WINS clients, see “Configuring WINS Client” on page 148.

18.1.4 Caveats

- If you have workstations joined to the domain prior to the WINS configuration, you must ensure that you configure those workstations as WINS clients after the WINS server configuration and reboot those clients. This will add workstation names to the WINS database and ensure that their duplicate names are detected.
- You can configure only one DSfW domain controller as a WINS server in a domain. Therefore, if the WINS service goes down, any workstation join with a duplicate name will not be reported. Also, if a workstation is down, a duplicate workstation join will not be reported. To identify workstations with duplicate names during such scenarios, follow the steps below:

1. Run the following command:

   ```
   /opt/novell/xad/share/dcinit/checkdupws.pl --current
   ```

2. Ensure that you have unique workstation names.
3. Run the following command:

```
/opt/novell/xad/share/dcinit/checkdupws.pl --clear-cache
```

This will clear the duplicate workstation name cache and display the list of duplicate workstation names that are cleared.

You can also schedule this script to be run after a specified interval. To schedule the script, run the following command:

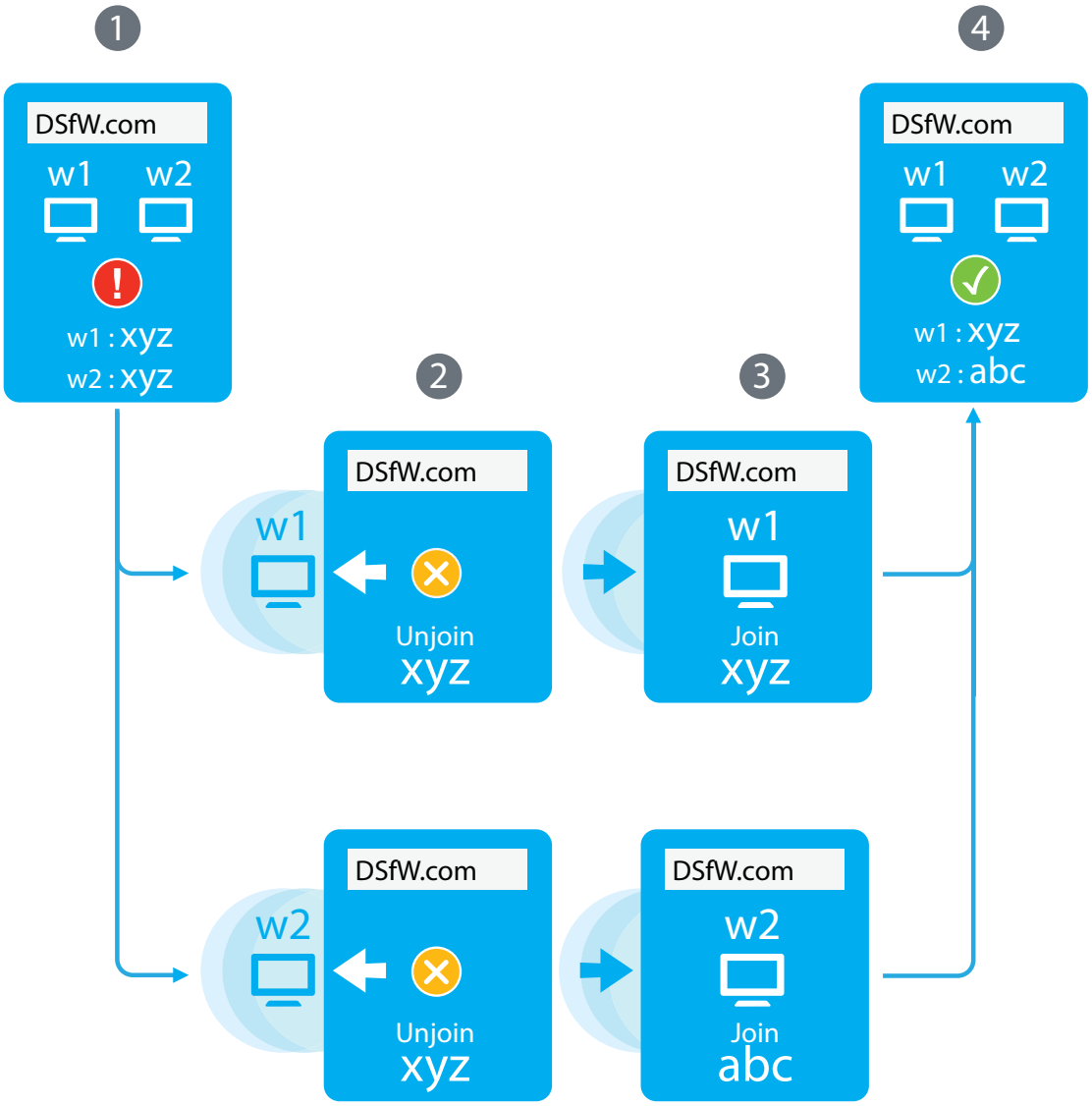
```
/opt/novell/xad/share/dcinit/checkdupws.pl --schedule=<interval in hours>
```

This schedules the script to be run periodically in the specified interval. The script is run with the --clear-cache option in the scheduled interval. The `/var/opt/novell/xad/log/wins_duplicate_check.log` will list the duplicate workstation names.

18.2 Rectifying Duplicate Workstation Names

If you have workstations with duplicate names in a domain, you might not be able to log in to one of these workstations. To rectify this, do the following:

Figure 18-1 *Rectifying Duplicate Workstation Names*



1. Log in to the workstation that you are unable to log in to, using the local workstation administrator credentials.
2. Rejoin the second workstation to the domain using a unique name. You must first unjoin the workstation from the domain and then join the workstation with a unique name.
3. Rejoin the first workstation, using the same name. You must first unjoin the workstation from the domain and then join the workstation with a unique name.

18.3 Verifying Duplicate Workstation Names Prior to WINS Configuration

If workstations with duplicate names exist in a domain prior to WINS configuration, you can use the workstation check script `/opt/novell/xad/share/dcinit/checkdupws.pl` to identify workstations with duplicate names and take appropriate action.

1. Run the following command:

   ```
   checkdupws.pl --history
   ```

2. Ensure that you have unique workstation names.
3. Run the following command:

   ```
   checkdupws.pl --clear-cache
   ```

   This will clear the duplicate workstation name cache.

18.4 Troubleshooting

This section describes known issues and frequently asked questions for configuring DSfW server as a WINS server.

18.4.1 WINS Server Does not Report Duplicate Workstation Name

If a workstation is down when another workstation with the same name joins the domain, the WINS server will not report the duplicate workstation name. This could lead to issues such as slow logins when the first workstation is up and running. To rectify this, schedule the duplicate workstation script to run periodically every few hours.

```
checkdupws.pl –-schedule=<interval in hours>
```

This script will log duplicate workstation names in `/var/opt/novell/xad/log/checkdupws.log`. For more information on rectifying duplicate workstation names, see Section 18.2, “Rectifying Duplicate Workstation Names,” on page 150.

19 Managing Group Policy and Fine-Grained Password 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. The Password Policies for DSfW users are applied through NMAS/Universal Password settings. For information on password policy management, refer to Section 19.3.1, “GPO Account Policies,” on page 158.

NOTE: Group Policy settings that apply to Domain Controllers are not supported in the OES environment since here it is an OES server and not a Windows Server.

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.

- Section 19.1, “Configuring Group Policies,” on page 153
- Section 19.2, “Configuring Fine-Grained Password Policy,” on page 156
- Section 19.3, “Group Policy Objects,” on page 158
- Section 19.4, “Sysvol,” on page 161
- Section 19.5, “Limitations with Group Policy Management,” on page 162

19.1 Configuring Group Policies

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

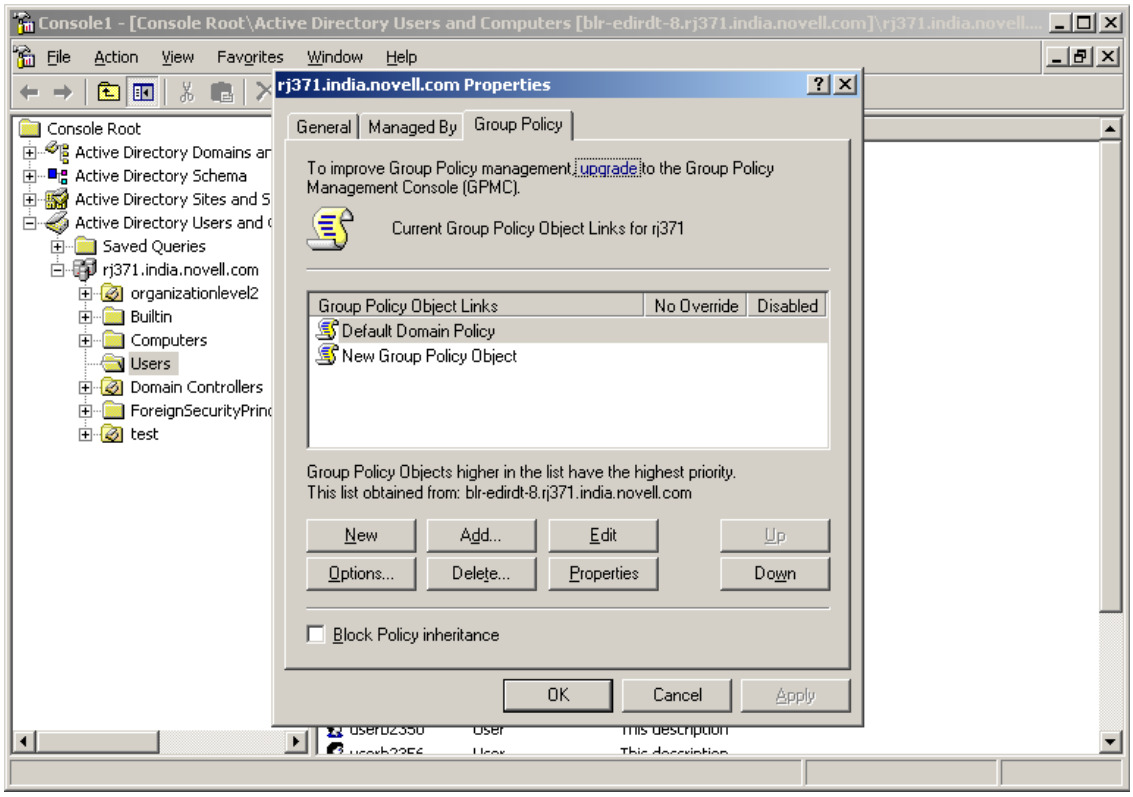
NOTE: If you have installed the Group Policy Management Console from Microsoft, the **Group Policy** tab options described below are no longer accessible. Refer to the Microsoft Windows Server 2003 documentation for instructions on how to use the Group Policy Management Console to manage Group Policies.

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 an 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)

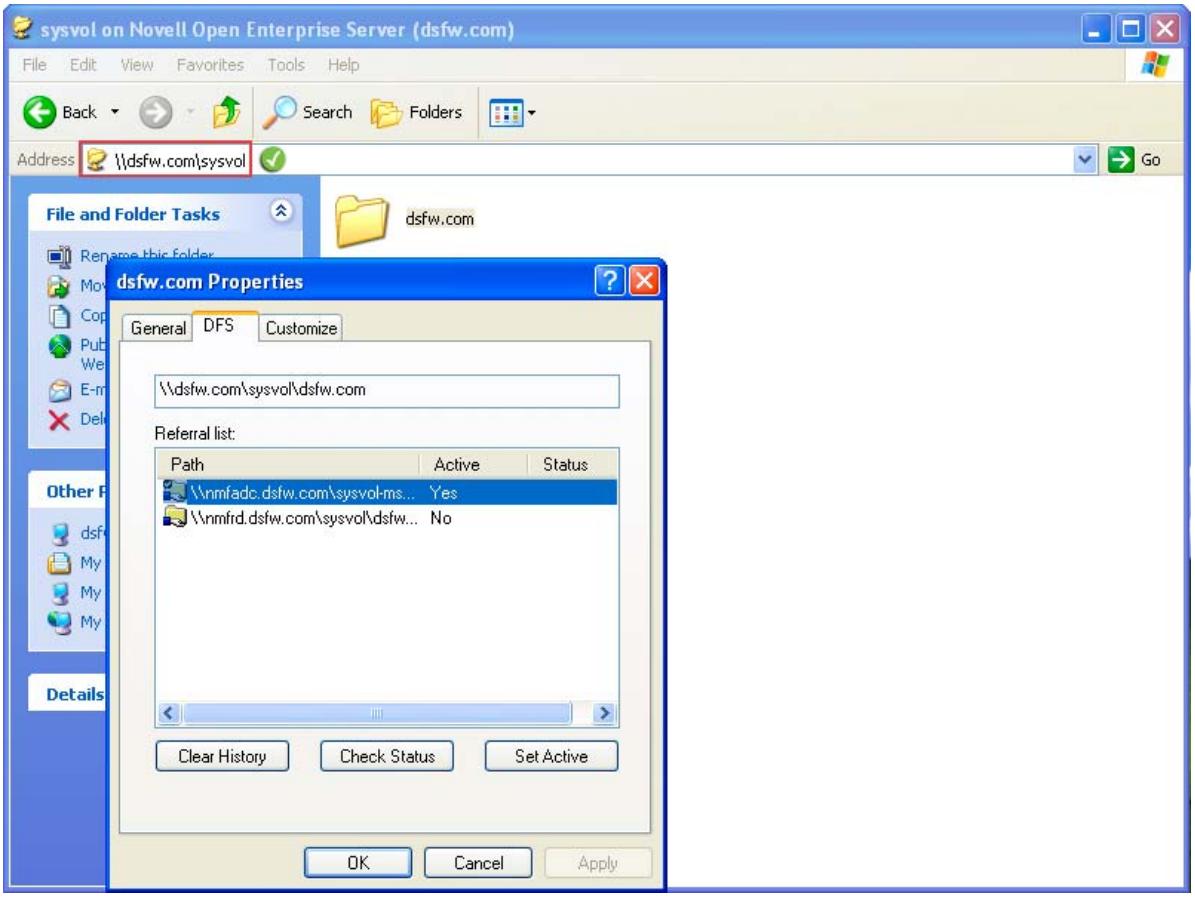
NOTE: If you are not able to edit the Group Policy, it is because the DFS cache is pointing to a server that is not holding the PDC Emulator role. To set the DFS link to point to the server holding the PDC Emulator role, execute the steps in Setting the DFS Referral of the Server Holding the PDC Emulator Role as Active on the Workstation.

Setting the DFS Referral of the Server Holding the PDC Emulator Role as Active on the Workstation

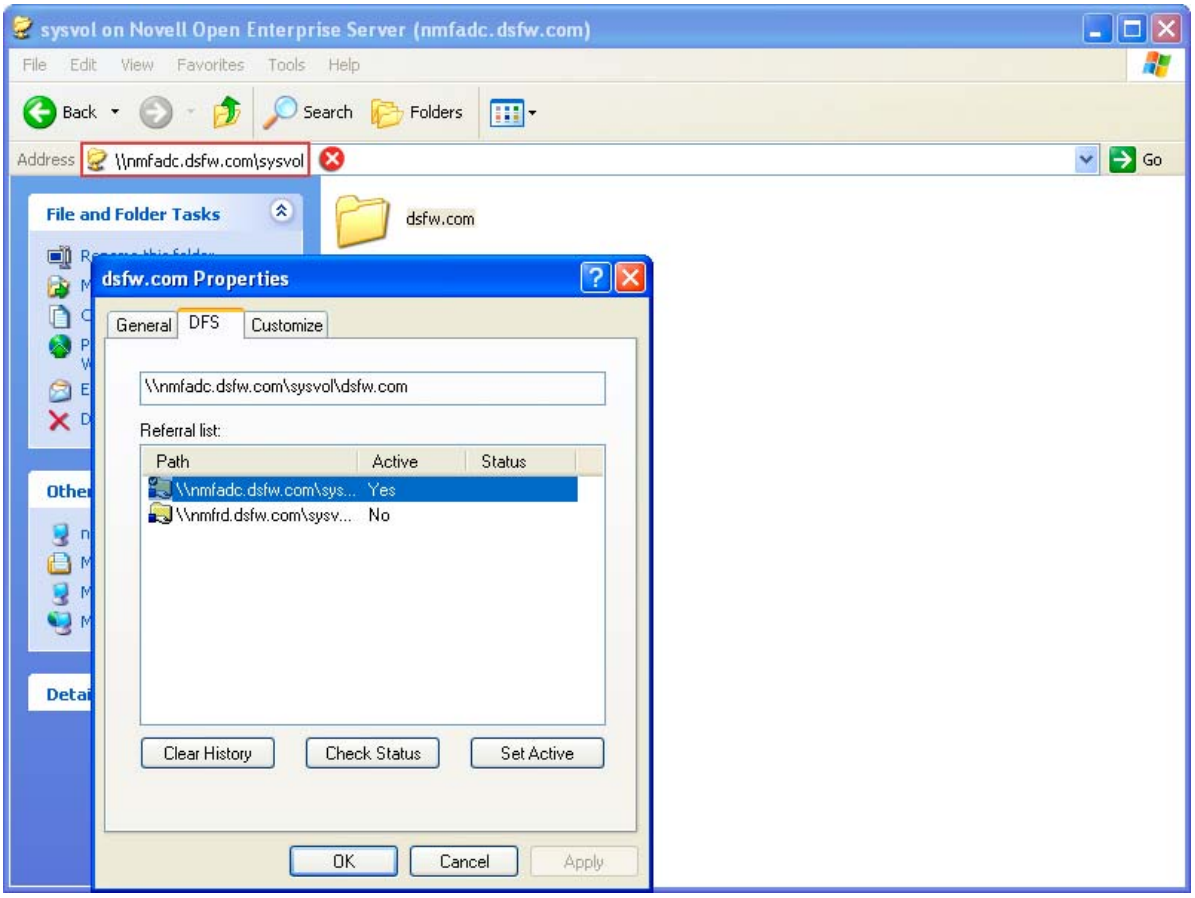
To set the DFS link of the server holding the PDC Emulator role as active, execute the following procedure:

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. For more information about NMAS and Universal Password settings, refer to the eDirectory documentation (https://www.netiq.com/documentation/edirectory-92/).

19.2 Configuring Fine-Grained Password Policy

Fine-grained password policy feature is available with schema 2012 level. It enables user level configuration of password policies. For fine-grained password policy to work in a domain, all domain controllers must be upgraded to OES 2018 or later.

You can use the fine-grained password policy feature to:

- Set multiple password policies within a single domain for a particular user.
- Apply password restrictions and account lockout policies to set of users in a domain.

19.2.1 Restrictions

- Policy can be applied only to user objects (or inetOrgPerson objects if they are used instead of user objects).
- By default, only members of the Domain Admins group can set fine-grained password policies.

- Fine-grained password policy cannot be applied to an organizational unit (OU) directly.
- Fine-grained password policies do not interfere with custom password filters that you might use in the same domain.

19.2.2 Creating the Fine-Grained Password Policy

During the schema extension to AD 2012 level, the script creates the Password Setting Container under the System container in the domain. The fine-grained password policy or Password Setting Object (PSO) can be created in the Password Setting Container.

1. Log in to one of your domain controllers, click **Start** > **Run**, and enter `mmc`.
2. In the **File** menu, select **Add/Remove Snap-ins**.
3. Select **ADSI Edit** from the list, click **Add** > **OK**.
4. Right-click **ADSI Edit** and click **Connect to**.
5. Expand the tree view, right-click **Password Setting Container**, then select **New** > **object**.
6. In the Create Object dialog box, select the class **msDS-PasswordSettings** and click **Next**.
7. Specify the name of the Password Setting Object in the **Value** field and click **Next**.
8. Specify the value for each of the following attributes and click **Next** after setting the value for each attribute.
   - **msDS-PasswordSettingsPrecedence** - represents the priority of the policy over other policies. The value of the precedence must be set between 1 and 10. When multiple policies are applied on a single user, the policy with lower precedence value takes the highest priority. It is recommended to create policies with different precedence value. If there are two different policies with the same precedence value, then the GUID of the object validates the effectiveness of the policy. The smaller the GUID, higher the effectiveness.
   - **msDS-PasswordReversibleEncryptionEnabled** - set the value to false, unless you want to save the eDirectory passwords in a reversible format.
   - **msDS-PasswordHistoryLength** - set the number of passwords to be remembered for the user account.
   - **msDS-PasswordComplexityEnabled** - set the value to True, if you want the password to be complex for the user account, else set it to False.
   - **msDS-MinimumPasswordLength** - set the minimum length of the password for the user account.
   - **msDS-MinimumPasswordAge** - set the duration (DD:HH:MM:SS) within which the password cannot be changed. For example, 1:00:00:00 for one day. If you want to allow changing of password soon after it is set, set the value of this attribute to its default value (none).
   - **msDS-MaximumPasswordAge** - set the duration (DD:HH:MM:SS) you want the password to be valid before expiring. For example, 14:00:00:00 for 14 days.
   - **msDS-LockoutThreshold** - set the number of trials a wrong password is allowed before the account gets locked. Setting this attribute to a low value may result to an account lockout storm. Any existing users with wrongly cached passwords might lockout quickly.

- **msDS-LockoutObservationWindow** - set the duration to be passed before the locked user account gets automatically unlocked.
- **msDS-LockoutDuration** - set the duration that the account should be in locked state after it gets locked.

9 Click **Finish**.

19.2.3 Setting the Password Policy on the User

1 Right-click the fine-grained password policy or Password Setting Object (PSO) created in the console tree and click **Properties**.

2 Select the attribute **msDS-PSOAppliesTo**, then click **Edit**.

3 Click **Add Windows Account**.

4 To apply the PSO on users, specify the users and click **OK** > **OK** > **Apply**.

You can verify that the **msDS-PSOAppliesTo** attribute contains an SID value.

19.3 Group Policy Objects

- Section 19.3.1, “GPO Account Policies,” on page 158
- Section 19.3.2, “gposync,” on page 160
- Section 19.3.3, “Enforcing Computer Configuration and User Configuration,” on page 160
- Section 19.3.4, “Troubleshooting,” on page 160

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 SYSV0L SMB volume.

The default configuration of SYSV0L resides in the `/etc/samba/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 SYSV0L SMB volume.

19.3.1 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

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

Table 19-1 *GPO and eDirectory Parameter Mapping for Password Policies*

GPO Parameter	eDirectory Parameter
Enforce Password History	pwdInHistory
Maximum Password Age	passwordExpirationInterval
Minimum Password Age	nspmMinPasswordLifetime
Minimum Password Length	passwordMinimumLength

Account Lockout Policy

Table 19-2 *GPO and eDirectory Parameter Mapping for Account Lockout Policies*

GPO Parameter	eDirectory Parameter
Account Lockout Duration	intruderLockoutResetInterval
Account Lockout Threshold	loginIntruderLimit
Reset Account Lockout Counter After	intruderAttemptResetInterval

Kerberos Policy

Table 19-3 *GPO and eDirectory Parameter Mapping for Kerberos Policies*

GPO Parameter	eDirectory Parameter
Maximum Lifetime for User Ticket	maxTicketAge
Maximum Lifetime for User Ticket Renewal	maxRenewAge

19.3.2 gposync

The gposync tool synchronizes the policies stored in eDirectory with those in SYSV0L.

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 SYSV0L, gposync updates the Account Policies. Similarly, it updates the policies in eDirectory if they are older than Account Policies maintained in SYSV0L.When you modify the Account Policies in SYSV0L by using Group Policy Management Console (GPMC), gposync makes the relevant changes to the policies in eDirectory when it runs the next time.

The gposync utility parses all the applied GPO policies and synchronizes appropriately to containers it is associated with. A typical output gposync utility on success will be as follows:

```
The list of Group Policies present in the domain dc=multizone,dc=com are:
        {31B2F340-016D-11D2-945F-00C04FB984F9}

Syncing {31B2F340-016D-11D2-945F-00C04FB984F9} Group Policy
Update NMAS Password Policy Links
Link present at : dc=multizone,dc=com
Group Policy Template is older than NMAS login policy <cn=Domain Password
Policy,cn=Password Policies,cn=System,dc=multizone,dc=com>.
DOMAIN\intruderLockoutResetInterval[1800] => System
Access\LockoutDuration[30]
DOMAIN\intruderAttemptResetInterval[1800] => System
Access\ResetLockoutCount[30]
DOMAIN\loginIntruderLimit[0] => System Access\LockoutBadCount[0]
NMAS\passwordExpirationInterval[3628800] => System
Access\MaximumPasswordAge[42]
NMAS->GPO synchronization OK.
```

19.3.3 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.

19.3.4 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.

19.4 Sysvol

- Section 19.4.1, “sysvolsync Utility,” on page 161

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.

The SYSV0L 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 SYSV0L volume only on the first domain controller.

Following are the benefits of having the SYSV0L 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 SYSV0L.
- 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 19.4.1, “sysvolsync Utility,” on page 161

19.4.1 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.

19.5 Limitations with Group Policy Management

- Section 19.5.1, “Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition,” on page 162
- Section 19.5.2, “Members of GroupPolicy Creator Owner group cannot change the active DFS Referral,” on page 162
- Section 19.5.3, “Ignore Warnings while Backing up Group Policies,” on page 162
- Section 19.5.4, “WMI Filters Cannot be Applied for Processing GPOs,” on page 162

19.5.1 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.

19.5.2 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

19.5.3 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.

19.5.4 WMI Filters Cannot be Applied for Processing GPOs

WMI filters are not supported in this release.

20 Managing Trust Relationships in Domain Services for Windows

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

- Section 20.1, “What is a Trust?,” on page 163
- Section 20.2, “Cross-Forest Trust Relationships,” on page 164
- Section 20.3, “Limitations with Cross-Forest Trust,” on page 173

20.1 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.

20.2 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 20.2.1, “Creating a Cross-forest Trust between Active Directory and Domain Services for Windows Forests,” on page 164
- Section 20.2.2, “Creating a Cross-forest Trust between two Domain Services for Windows Forests,” on page 170
- Section 20.2.3, “Shortcut Trusts,” on page 172

20.2.1 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 164
- “Configuring the Reverse Lookup Zone Forwarder” on page 165
- “Configuring the DNS Forward Lookup Zone on the Active Directory Server” on page 166
- “Creating the Trust” on page 167
- “Verifying the Trust” on page 169

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. In the DNS Service window of the DNS/DHCP Java-based Management Console utility, click Create on the tool bar.
2. Select **Zone** from the Create New DNS Object dialog box, then click **OK**.

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

- Specify the eDirectory context for the zone or browse to select it; that is, the container containing the DNS related objects.
- Specify a name for the zone; that is, the domain name of the Active Directory forest.
- Select the Zone Type as Forward.
- Select a DNS server from the **Assign Authoritative DNS Server** drop-down list. This is the name of the DNS server object.
- Click **Create**. A message indicates that the new forward zone has been created.

4 Select the zone that is created.

5 Click the Forwarding List tab. This tab displays a list of all forwarding IP addresses. To add an address to the list, click **Add**, select the **Forwarder Address** option and specify the IP address of the Active Directory forest's DNS server. Click **OK**.

6 Restart DNS by using the `systemctl-named start` command.

7 To save the changes done to the nds, click the **Save** button.

Configuring the Reverse Lookup Zone Forwarder

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

1 In the DNS Service window of the DNS/DHCP Java-based Management Console utility, select **All Zones** click **Create**.

2 Select Zone from the Create New DNS Object dialog box, then click **OK**.

3 Specify the DNS configuration parameters:

- Select **Create IN-ADDR.ARPA**.
- Specify the network address. This is the IP address of the Active Directory forest's DNS server.
- Select **Forward** as the Zone Type.
- Select a DNS server from the **Assign Authoritative DNS Server** drop-down list. This is the name of the DNS server object.
- Click **Create**. A message indicates that the zone has been created.

4 Select the zone that is created.

5 Click the Forwarding List tab. This tab displays a list of all forwarding IP addresses. To add an address to the list, click **Add**, select the **Forwarder Address** option and specify the IP address of the Active Directory forest's DNS server. Click **OK**.

6 To save the changes done to the nds, click the **Save** button.

7 Verify the DNS configuration by trying to resolve the Active Directory domain and its DNSSRV 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**.

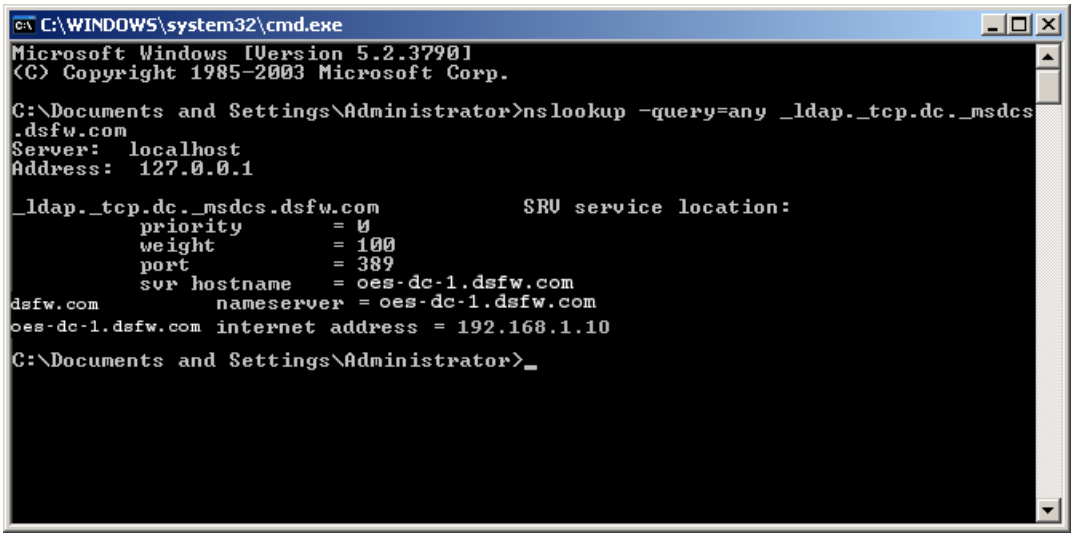
1a Click **File>Add/Remove** snap-in, click **Add** and select DNS snap-in, then click **Add**. Click **Close** to close the window and then click **OK**.

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 Level** 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 Forest 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*.

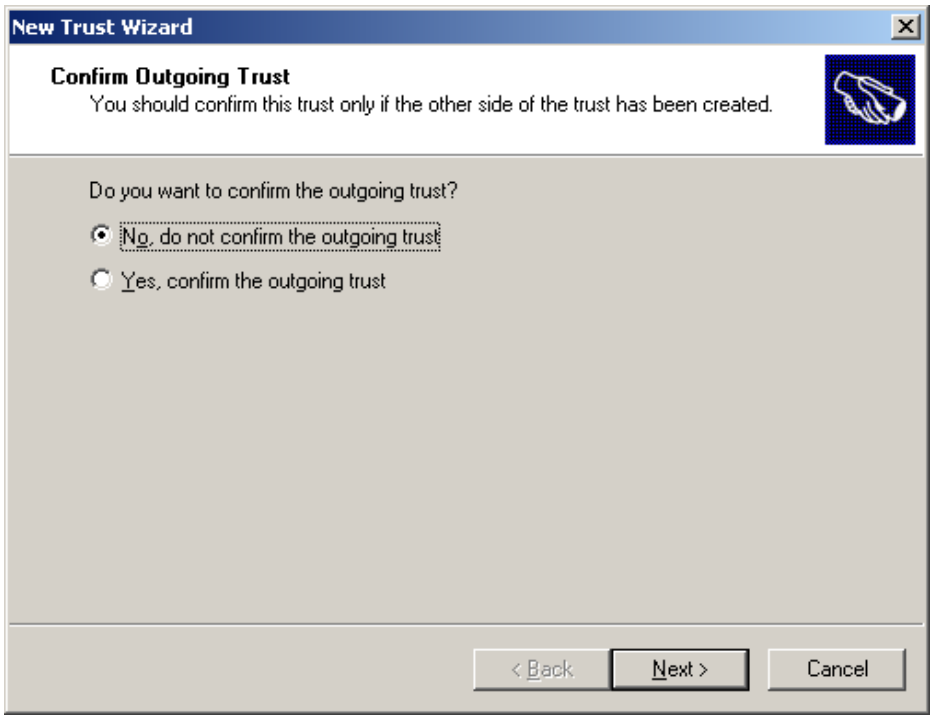
12 Specify the user name and password of the Active Directory domain administrator, then click *Next*.

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

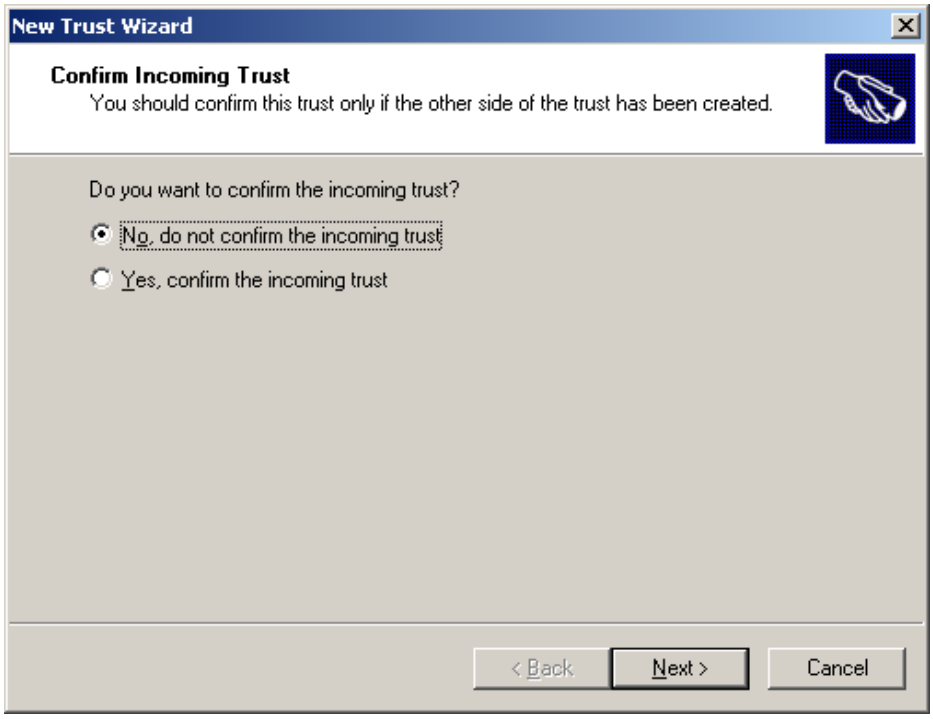
14 Select **Forest-wide authentication** to authenticate Active Directory forest users to use resources in the dsfw.com forest or those identified by the administrator, then click *Next*.

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 XP machine that is joined to the Domain Services for Windows domain has an entry for the Active Directory domain. For other higher versions of Windows like Windows 8, follow the instructions in Step 2.

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 XP machine that is joined to the Active Directory domain has an entry for the Domain Services for Windows domain. For other higher versions of Windows like Windows 8, follow Step 4.

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.

20.2.2 Creating a Cross-forest Trust between two Domain Services for Windows Forests

This section describes how to create a cross-forest trust between two DSfW forests.

- "Configuring the DNS Forwarders on the Domain Services for Windows Server" on page 170
- "Configuring the Reverse Lookup Zone Forwarder" on page 171
- "Creating the Trust" on page 171
- "Verifying the Trust" on page 172

In this example, there are two DSfW forests: dsfw1.com and dsfw2.com.

Configuring the DNS Forwarders on the Domain Services for Windows Server

You need to configure a DNS forwarder on the first DSfW DNS server (dsfw1.com) to forward any DNS queries for the second DSfW domain(dsfw2.com). The queries are forwarded to the DNS server of the second domain.

1. In the DNS Service window of the DNS/DHCP Java-based Management Console utility, click Create on the tool bar.
2. Select **Zone** from the Create New DNS Object dialog box, then click **OK**.
3. Select **Create New Zone** and specify the DNS configuration parameters as follows:
   - Specify the eDirectory context for the zone or browse to select it; that is, the container containing the DNS related objects.
   - Specify a name for the zone; that is, the DSfW domain name with which you want to create trust (second domain).
   - Select the Zone Type as Forward.
   - Select a DNS server from the **Assign Authoritative DNS Server** drop-down list. This is the name of the DNS server object.
   - Click **Create**. A message indicates that the new forward zone has been created.
4. Select the zone that is created.
5. Click the Forwarding List tab. This tab displays a list of all forwarding IP addresses. To add an address to the list, click **Add**, select the **Forwarder Address** option and specify the IP address of the DNS server of the DSfW domain with which you want to create trust (second domain). Click **OK**.
6. Restart DNS by using the `systemctl-named start` command.
7. To save the changes done to the nds, click the **Save** button.

Repeat steps Step 1 to Step 7 to create forwarder for the first DSfW domain (dsfw1.com) in the DNS server of the second DSfW domain (dsfw2.com).

Configuring the Reverse Lookup Zone Forwarder

You need to configure a reverse lookup zone for the second DSfW domain on the DNS server of the first DSfW domain.

1. In the DNS Service window of the DNS/DHCP Java-based Management Console utility, select **All Zones** click **Create**.
2. Select Zone from the Create New DNS Object dialog box, then click **OK**.
3. Specify the DNS configuration parameters:
   - Select **Create IN-ADDR.ARPA**.
   - Specify the network address. This is the IP address of the DNS server of the DSfW domain with which you want to create a trust.
   - Select **Forward** as the Zone Type.
   - Select a DNS server from the **Assign Authoritative DNS Server** drop-down list. This is the name of the DNS server object.
   - Click **Create**. A message indicates that the zone has been created.
4. Select the zone that is created.
5. Click the Forwarding List tab. This tab displays a list of all forwarding IP addresses. To add an address to the list, click **Add**, select the **Forwarder Address** option and specify the IP address of the Active Directory forest's DNS server. Click **OK**.
6. To save the changes done to the nds, click the **Save** button.
7. Verify the DNS configuration by trying to resolve the DSfW domain with which you want to create trust 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.dsfw2.com
Server: 192.168.1.10
Address: 192.168.1.10#53
Non-authoritative answer:
ldap._tcp.dc._msdcs.dsfw2.com service = 0 100 389 osg-dtsrv22.
dsfw2.com.
Authoritative answers can be found from:
osg-dt-srv22.dsfw2.com internet address = 192.168.1.20
```

Repeat steps Step 1 to Step 7 to create forwarder for the reverse lookup zone of the first DSfW domain (dsfw1.com) in the DNS server of the second DSfW domain (dsfw2.com).

Creating the Trust

1. At your Windows management workstation which is joined to the first DSfW domain, 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 first DSfW domain(dsfw1.com), 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 domain name (or NetBIOS name) of the second DSfW forest(dsfw2.com), 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 second DSfW 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 the second DSfW forest users to use resources in the first DSfW 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 for confirming outgoing trust, then click **Next**.

17 Click any option depending on your choice for confirming incoming trust, 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 trust creation 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 first DSfW domain has an entry for the second DSfW domain.

2 Try to log on to the Windows machine that is joined to the first DSfW domain with the second DSfW domain's user principal name.

3 Verify that the **Log on to** field in the Login window of a Windows machine that is joined to the second DSfW domain has an entry for the first DSfW domain.

4 Try to log on to the Windows machine that is joined to the second DSfW domain with the first DSfW domain's user principal name.

20.2.3 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.

20.3 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.

21 NSS Volume Access by DSfW and Active Directory Users

Prior to OES 2015, Active Directory users were unable to access files in NSS volumes. Therefore, DSfW users could not share files in NSS volumes with Active Directory users. However, beginning with OES 2015, Active Directory users can also natively access the NSS resources, administer them, and provision rights for Active Directory trustees. This is achieved by using the OES Storage Services (NSS) Active Directory (AD) support feature. With NSS AD support enabling Active Directory users to access NSS volumes, DSfW users can now share their files with AD users in NSS volumes.

This chapter is designed to help you understand how DSfW works with the NSS AD support feature. For detailed information about the NSS AD support, see the NSS AD Administration Guide.

- Section 21.1, “Configuring NSS AD and DSfW in the same tree,” on page 175

21.1 Configuring NSS AD and DSfW in the same tree

You cannot install NSS AD and DSfW in the same server. However, you can install NSS AD and DSfW in the same tree but separate servers. If you configure NSS AD and DSfW in the same tree and join the NSS AD server to the Active Directory domain, you can enable Active Directory users to access the same NSS volumes that the DSfW users have access to. Follow the instructions given below to enable Active Directory users to access NSS volumes that DSfW users have access to.

1. Install (or upgrade) and configure NSS AD and CIFS server in the same tree that DSfW server is configured. Join the NSS AD server to the Active Directory domain during the NSS AD configuration. For information on configuring NSS AD and, see NSS AD Administration Guide.
2. After installing and configuring NSS AD, upgrade the local pools and volumes to support AD users. For information, see NSS Media Upgrade Commands in the Storage Services File System (NSS) Administration Guide for Linux.
3. To enable Active Directory users to access NSS resources, you must AD-enable the volumes. For information on AD-enabling NSS volumes, see Volume AD-enabling in the Storage Services File System (NSS) Administration Guide for Linux.
4. Using iManager, add the DSfW users context to CIFS contexts.
5. Using iManager, assign rights to the DSfW users on the NSS-AD volumes.
6. Add the DNS HOST/PTR entries of OES NSS AD server in Active Directory DNS.
7. Using the NURM tool, map the users having same name in DSfW and Active Directory and the rights of the users. For information on the NURM tool, see NURM (OES User Rights Map) in the NSS AD Administration Guide.
8. Join a Windows workstation to the Active Directory Domain.
9. Log in to the Windows workstation using the Active Directory user credentials of a mapped user.
10. Map the network drive using the FQDN of the NSS AD server. For example:

```
\\<NSS-ADServer.ADDomain.com>\<ADEnabledVolume>
```

The Active Directory user will now be able to access the NSS volumes.

22 Providing Access to Server Data

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

- Section 22.1, “Accessing Files by Using Native Windows Methods,” on page 177
- Section 22.2, “Accessing Files by Using the Client for Open Enterprise Server,” on page 183
- Section 22.3, “Accessing Files in Another Domain,” on page 183

22.1 Accessing Files by Using Native Windows Methods

This section discusses the following topics:

- Section 22.1.1, “Prerequisites,” on page 177
- Section 22.1.2, “Samba: A Key Component of DSfW,” on page 177
- Section 22.1.3, “Samba in the DSfW Environment,” on page 178
- Section 22.1.4, “Creating Samba Shares in iManager,” on page 178
- Section 22.1.5, “Creating Samba Shares in the smb.conf File,” on page 179
- Section 22.1.6, “Assigning Rights to Samba Shares,” on page 180
- Section 22.1.7, “Adding a Network Place,” on page 181
- Section 22.1.8, “Adding a Web Folder,” on page 182
- Section 22.1.9, “Mapping Drives to Shares,” on page 182

22.1.1 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 14.1, “Joining a Windows Workstation to a DSfW Domain,” on page 127
- Section 14.2, “Logging In to a DSfW Domain,” on page 130
- Chapter 15, “Creating Users,” on page 133

22.1.2 Samba: A Key Component of DSfW

One of the primary benefits of DSfW is that users can access files on OES servers without having any Client for Open Enterprise Server software installed. This is accomplished through Samba software that is installed on every DSfW server.

Samba 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 customers have the DSfW configuration of Samba

The Section 22.1.3, “Samba in the DSfW Environment,” on page 178 explains the Samba configuration that is included with DSfW.

22.1.3 Samba in the DSfW Environment

When you install a DSfW server, Samba software is automatically installed on that server. This is configured as outlined in Table 22-1.

Table 22-1 *Samba in DSfW*

Item	Samba in DSfW
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 server.
Samba enablement	eDirectory users in the domain (eDirectory partition) are automatically Samba users and are enabled to access Samba shares. See Chapter 15, “Creating Users,” on page 133. Domain users are set up with the necessary UID and default group (DomainUsers) membership. Every additional eDirectory group created within the domain is automatically Linux-enabled.
Username and password	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.

22.1.4 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 Documentation (https://www.netiq.com/documentation/imanager-32/)

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 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 22.1.6, "Assigning Rights to Samba Shares," on page 180 to assign users rights to access the new share.

22.1.5 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 Section 22.1.6, "Assigning Rights to Samba Shares," on page 180 to assign users rights to access the new share.

22.1.6 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 22-2 lists the management tools available for assigning rights to Samba shares created on various file systems.

Table 22-2 *Tools for Managing File System Rights*

File System	Rights Management Tools	Notes
OES Storage Services (NSS)	**iManager > Files and Folders > Properties > Rights** `rights` command	The `rights` command available at the terminal prompt is for working with NSS volumes only. For online help, enter `rights` with no options.
NCP Volume on Linux POSIX file systems (no NSS)	iManager > Flies and Folders > Properties > **Rights** `ncpcon` > `rights`	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`.
Linux POSIX file systems (no NSS or NCP)	`chmod chown chgrp`	For information on assigning POSIX rights, see the SLES 12 Administration Guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-administration.html).

Example: Assigning Rights to Folders on an NSS Volume

The example below continues the steps described in Section 22.1.4, “Creating Samba Shares in iManager,” on page 178 and Section 22.1.5, “Creating Samba Shares in the smb.conf File,” on page 179.

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/code -r rf trustee user1.full_edir_context
   rights -f /projects/code -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 OES 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.

22.1.7 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 server. For more information and setting up shares, see Section 22.1.4, “Creating Samba Shares in iManager,” on page 178 and Section 22.1.5, “Creating Samba Shares in the smb.conf File,” on page 179.

---

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 server. For more information and for instructions on setting up shares, see Section 22.1.4, “Creating Samba Shares in iManager,” on page 178.
   - **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 server. For more information and for instructions on setting up shares, see Section 22.1.4, “Creating Samba Shares in iManager,” on page 178.

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.

22.1.8 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 server. For more information and setting up shares, see Section 22.1.4, “Creating Samba Shares in iManager,” on page 178 and Section 22.1.5, “Creating Samba Shares in the smb.conf File,” on page 179.

---

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**.

22.1.9 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.

22.2 Accessing Files by Using the Client for Open Enterprise Server

Organizations that have the Client for Open Enterprise Server installed on Windows workstations can continue to use the standard NCP methods, such as drive mappings, to access data that is located on NSS or NCP volumes on DSfW servers.

22.3 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. After the trust is established, users in one domain can access shares in another domain. For more information, refer to "OES Domain Services for Windows" in the *Storage Services File System (NSS) Administration Guide for Linux*.

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 20, “Managing Trust Relationships in Domain Services for Windows,” on page 163.

23 Printing in the Domain Services for Windows Environment

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

- Section 23.1, “Setting Up iPrint,” on page 185
- Section 23.2, “Special Handling for iPrint on DSfW,” on page 185
- Section 23.3, “iPrint Clustering in a DSfW Environment,” on page 186

23.1 Setting Up iPrint

With Domain Services for Windows, you set up iPrint in the same way as for any OES Linux installation.

For instructions on how to install and configure iPrint on OES servers, see OES iPrint Advanced Administration Guide.

23.2 Special Handling for iPrint on DSfW

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

- Section 23.2.1, “Secure and Non-Secure Printing,” on page 185
- Section 23.2.2, “Using a Common Driver Store in a DSfW partition,” on page 186

23.2.1 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>`"

23.2.2 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.

23.3 iPrint Clustering in a DSfW Environment

- Section 23.3.1, “iPrint Clustering on NSS Clusters,” on page 186

23.3.1 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.

24 Flexible Single Master Operation (FSMO) Roles

This section provides details on the various FSMO roles and provides details on transferring and seizing FSMO roles.

- Section 24.1, “FSMO Roles and Limitations,” on page 187
- Section 24.2, “Transferring and Seizing FSMO Roles,” on page 188

24.1 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

24.1.1 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.

24.1.2 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.

24.1.3 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.

24.1.4 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.

24.1.5 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.

24.2 Transferring and Seizing FSMO Roles

The domain controller playing the role of PDC emulator hold the writable copy of SYSV0L while all other domain controllers host a read-only copy of SYSV0L. 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 24.2.1, “To Transfer the PDC Emulator Role from the First Domain Controller to an additional domain controller,” on page 189
- Section 24.2.2, “To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Functional),” on page 189
- Section 24.2.3, “To Seize PDC Emulator Role from First Domain Controller to an Another Domain Controller (DNS is Not Functional),” on page 190
- Section 24.2.4, “Transferring the ADPH Master Role to Other Domain Controllers,” on page 190

IMPORTANT: If during installation of the additional 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 in the NetIQ eDirectory Administration Guide.

24.2.1 To Transfer the PDC Emulator Role from the First Domain Controller to an additional 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 (https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/view-transfer-fsmo-roles).
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
   ```

24.2.2 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 `ntdsutil` utility. For more information on how to seize FSMO roles using `ntdsutil`, see Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller (https://support.microsoft.com/en-us/help/255504/using-ntdsutil-exe-to-transfer-or-seize-fsmo-roles-to-a-domain-control).
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
   ```

24.2.3 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 `ntdsutil` utility. For more information on how to seize FSMO roles using `ntdsutil`, see Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller (https://support.microsoft.com/en-us/help/255504/using-ntdsutil-exe-to-transfer-or-seize-fsmo-roles-to-a-domain-control).
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
   ```

24.2.4 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 190
- “Using LDIF File” on page 191

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
```

25 Troubleshooting

Use the information in this section to resolve DSfW issues.

- Section 25.1, “Troubleshooting DSfW,” on page 193
- Section 25.2, “Error Messages in Log Files,” on page 212
- Section 25.3, “Novell SecureLogin Issues,” on page 213
- Section 25.4, “Known Issues,” on page 213

25.1 Troubleshooting DSfW

- Section 25.1.1, “Logging In from a Workstation - Issues,” on page 195
- Section 25.1.2, “Unable to Add msDs-PrincipalName and Create Password Settings Container During Upgrade,” on page 197
- Section 25.1.3, “No Immediate Effect of the Applied Fine-Grained Password Policy,” on page 197
- Section 25.1.4, “MMC Fails to Display the “Properties” Option for Multiple Selected Users,” on page 198
- Section 25.1.5, “Remote Desktop License Server Cannot Update the License Attributes,” on page 198
- Section 25.1.6, “Editing GPO for Windows Server 2012 R2 Member Server Might Result in an Error,” on page 199
- Section 25.1.7, “The wbinfo Operation for winbind Daemon Fails if two IP Interfaces are Present in a Domain Controller,” on page 199
- Section 25.1.8, “DSfW Provisioning Fails When you Configure an Additional Domain Controller to an Existing Child Domain,” on page 199
- Section 25.1.9, “Error During DSfW Provisioning,” on page 200
- Section 25.1.10, “User Moved out of DSfW Domain is able to Access to DSfW Service,” on page 200
- Section 25.1.11, “Rename of User Object Using iManager Fails to Update the samAccountName and userPrincipalName,” on page 201
- Section 25.1.12, “Windows Password Synchronization Fails With DSfW Domain Users for Windows XP Clients,” on page 201
- Section 25.1.13, “Workstation Login Fails With Samba Error,” on page 201
- Section 25.1.14, “On a Non-DSfW Server, eDirectory Restart Results in an Error Message,” on page 202
- Section 25.1.15, “ADC Install Enters Wrong Context for Server,” on page 202
- Section 25.1.16, “DSfW Fails to Set Up Signed NTP for Clients to Trust,” on page 202
- Section 25.1.17, “Unable to Proceed with Installation of an Additional Domain Controller,” on page 203

- Section 25.1.18, “Unable to Access Sysvol,” on page 203
- Section 25.1.19, “Reverse Zone Record for Workstations Joined to CDC and ADC is Not Getting Updated,” on page 203
- Section 25.1.20, “DSfW Provisioning Wizard Might Hang During the Restart DSfW Services Phase,” on page 204
- Section 25.1.21, “Citrix Xenserver Fails to Join a DSfW Domain,” on page 204
- Section 25.1.22, “Changing the User Password Requires Reimport of Third-Party Application Certificates,” on page 204
- Section 25.1.23, “Administrative Templates in the Computer Configuration and User Configuration Are Empty,” on page 204
- Section 25.1.24, “SLED or SLES Workstation Join to DSfW Triggers Traces in the log.smbd File,” on page 205
- Section 25.1.25, “Extending the DSfW Object Classes with Mandatory Attributes Leads to Object Creation Failure in MMC,” on page 205
- Section 25.1.26, “Kinit Not Working for Users,” on page 206
- Section 25.1.27, “Cleanup Task Fails in Name Mapped Scenarios,” on page 206
- Section 25.1.28, “MMC Fails to Create Users,” on page 206
- Section 25.1.29, “Using DSfW Server as a WINS Server Results in an Error,” on page 206
- Section 25.1.30, “iManager Fails to Create Samba Shares if the Administrator Name is Changed using MMC,” on page 207
- Section 25.1.31, “If Administrator and Default Group Objects are Accidentally Deleted,” on page 207
- Section 25.1.32, “Tree Admin is Not Automatically Granted Rights for DSfW Administration,” on page 208
- Section 25.1.33, “DSfW Services Stop Working if the Concurrent LDAP Bind Limit is Set to 1,” on page 208
- Section 25.1.34, “The Provision Utility Succeeds Only With the *--locate-dc Option,” on page 208*
- Section 25.1.35, “Users Are Not Samified When the RID Master Role is Seized,” on page 208
- Section 25.1.36, “Shared Volumes Are Not Accessible,” on page 209
- Section 25.1.37, “Requirements for Samba/CIFS Access to NSS volumes via DSfW,” on page 209
- Section 25.1.38, “Identifying novell-named Error,” on page 210
- Section 25.1.39, “Login Failure,” on page 210
- Section 25.1.40, “Unable to Connect to Legacy Applications,” on page 210
- Section 25.1.41, “User in a Domain Can Access Resources from Another Domain by Using the UID of the Foreign User,” on page 211
- Section 25.1.42, “Users Cannot Log In if They Are Moved From a Non-Domain Partition to a DSfW Domain Partition,” on page 211
- Section 25.1.43, “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,” on page 211
- Section 25.1.44, “Child Domains Slow Down When the First Domain Controller is Not Functional,” on page 211

- Section 25.1.45, “Error Mapping SID to UID,” on page 211
- Section 25.1.46, “After DSfW Installation, the Services are Not Working,” on page 212
- Section 25.1.47, “Configuring eDirectory on a Non-Default Port Affects the Installation of DSfW in a Name-Mapped Scenario,” on page 212
- Section 25.1.48, “Issues in Using iManager and MMC Interchangeably to Add Users in a Mixed OES (non-DSfW) and DSfW Environment,” on page 212

25.1.1 Logging In from a Workstation - Issues

- “Rejoining an Existing Windows Workstation or Server to a DSfW Domain Fails” on page 195
- “Workstation Join or Login Fails if the tdb Files are Corrupted” on page 195
- “Joining a Workstation to a Domain Fails if Password Policy Requirements is not met” on page 196
- “Joining a Workstation to a Domain Fails if Time is Not Synchronized” on page 196
- “Join a Workstation to a Domain Fails if Services are Down” on page 196
- “Workstation Join Fails due to Missing Serviceprincipalname Attribute Value” on page 196
- “Joining Multiple Workstations to the Domain at the Same Time Results in an Error” on page 197

Rejoining an Existing Windows Workstation or Server to a DSfW Domain Fails

If you attempt to rejoin an existing Windows workstation or server to a DSfW domain, an error message, `"The trust relationship between this workstation and the primary domain failed"` might appear.

To resolve this issue, perform the following steps:

1. Click **Start > Administrative Tools > Active Directory Users and Computers**.
2. In the console tree, open the Domain Services for Windows domain, and click **Computers** container.
3. In the right pane, browse to the corresponding Windows workstation object.
4. Right-click on the object and select **Delete**.
5. Click **Yes** to confirm.
6. Complete the steps mentioned in Section 14.1, “Joining a Windows Workstation to a DSfW Domain,” on page 127 to rejoin the Windows workstation to a DSfW Domain.

Workstation Join or Login Fails if the tdb Files are Corrupted

If the tdb files at `/var/lib/samba` are corrupted, then the workstation join or login fails. The tdb files are used by Samba services (smbd, winbindd, and nmbd). The workstation join or login failure is indicated by the following message in the Samba logs:

```
rec_free_read bad magic
```

NOTE: Samba logs are located at `/var/log/messages`.

To resolve this issue, you must first delete all the tdb files at `/var/lib/samba`, then restart the Samba services.

Joining a Workstation to a Domain Fails if Password Policy Requirements is not met

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).

Joining a Workstation to a Domain Fails 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
```

Join a Workstation to a Domain Fails if Services are Down

For joining domains, ensure that SLES11 SP4 is installed first, updated with Samba 3.0.36 patch, and then OES is 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
```

Workstation Join Fails due to Missing Serviceprincipalname Attribute Value

If the DSfW domain has multiple domain controllers and certain values of the attribute `servicePrincipalName` are missing from the domain controller object, then the workstation join to the domain might fail. In this case, the following message is logged in the `/var/opt/novell/xad/log/kdc.log` file:

```
<servicePrincipalName>, Server not found in Kerberos database.
```

To update the servicePrincipalName attribute with the missing values, you must create an LDIF file with the list of service principals. The list of service principals can be obtained from the `/var/opt/novell/xad/ds/domain/domain-bl.ldif` file. You must then upload the LDIF file by using the following command:

```
LDAPCONF=/etc/opt/novell/xad/openldap/ldap.conf ldapmodify -Y EXTERNAL -f
<path-to-your-ldif-file>
```

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.

25.1.2 Unable to Add msDs-PrincipalName and Create Password Settings Container During Upgrade

After upgrade to OES 2018 or later, it is advisable to review the `/var/opt/novell/xad/log/ndsdcinit.log file`.

If the following errors are seen in the `ndsdcinit` log file, you must execute the commands that are suggested in the log file after each of the errors:

```
2017-08-28 15:04:48 Executing...(principal) LDAPCONF=/etc/opt/novell/xad/
openldap/ldap.conf /usr/bin/ldapmodify -Q -Y EXTERNAL -Z -f /var/opt/
novell/xad/ds/domain/principal-domain-acls.ldif
2017-08-28 15:04:48 /opt/novell/xad/lib64/perl/util_update.pm:1099 Failed
to add msDS-PrincipalName to the objects: 17: [modifying entry
"ou=dsfwfrd,o=novell"] at /opt/novell/xad/lib64/perl/util_update.pm line
1094.
```

and

```
2017-08-28 15:05:10 /opt/novell/xad/lib64/perl/util_update.pm:1202 Failed
to create Password Settings Container: 65: [ldap_add: Object class
violation (65)       additional info: NDS error: no such class (-604)adding
new entry "CN=Password Settings Container,CN=System,ou=dsfwfrd,o=novell"]
at /opt/novell/xad/lib64/perl/util_update.pm line 1199.
```

25.1.3 No Immediate Effect of the Applied Fine-Grained Password Policy

The fine-grained password policy might not be effective immediately.

To resolve this issue, change the sync time to a lower value in crontab for `fgsync.sh`. Alternatively, you can manually run the binary `/opt/novell/xad/sbin/fgpsync.sh` on the DSfW server.

25.1.4 MMC Fails to Display the “Properties” Option for Multiple Selected Users

For a workstation joined to a DSfW domain, on the MMC console, if you select multiple users and right-click, the **Properties** option is not displayed. This is because the `nTSecurityDescriptor` attribute is not fully supported by DSfW. Therefore, you cannot change settings for multiple users using the **Properties** option.

You can change the settings for multiple users by adding a GPO in the DSfW domain and applying the same settings on GPO. For example, if you need to add `\\servername\profiles\%username%` to the profile path attribute of multiple users at the same time, follow the steps given below:

1. Login as Administrator to the DSfW server from a workstation.
2. Open the Group Policy Management Console.
3. Right-click the servername and select **"Create a GPO in this domain, and Link it here..." .**
4. Go to **Policies > Administrative Templates Policy > System > User Profiles** and click the **"Set roaming Profile paths for all users logging onto this ...."** option.
5. Select the **Enabled** check box and in the **Options** field add `\\servername\profiles\%username%` , then click **OK**.
6. In the Group Policy Management Console, select the new group policy created and click **Add** to add all users that require `\\servername\profiles\%username%` in the profile path attribute.

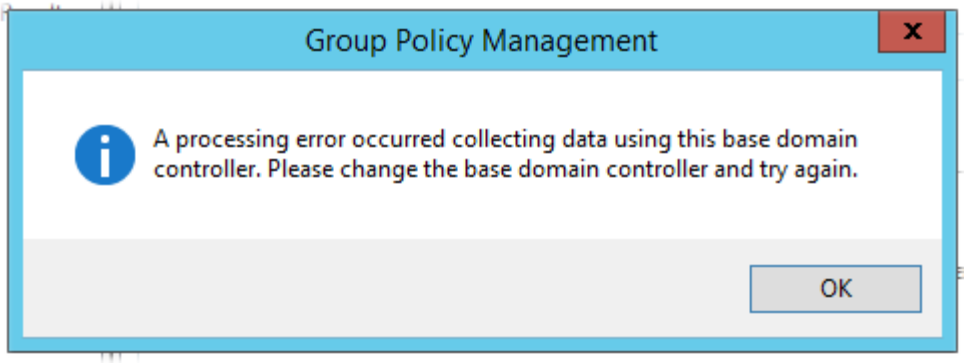
25.1.5 Remote Desktop License Server Cannot Update the License Attributes

Remote Desktop license server cannot update the license attributes because the `terminalServer` attribute has insufficient rights. You must provide sufficient rights to `terminalServer` attribute to resolve this issue. To provide sufficient rights to the `terminalServer` attribute, follow the steps given below.

1. In iManager, select **Roles and Tasks > Rights > Modify Trustees**.
2. Select the domain root partition.
3. Click **Assigned Rights for Public Trustee**.
4. Add the `terminalServer` attribute to the Public Trustee.
   - **4a** Click **Add Property**.
   - **4b** Select the `terminalServer` attribute from the Property Name list and click **OK**.
5. Select the **Inherit** check box for the `terminalServer` attribute.
6. Restart the DSfW services.

25.1.6 Editing GPO for Windows Server 2012 R2 Member Server Might Result in an Error

After joining a Windows server 2012 R2 to a DSfW domain, editing the GPO might result in the following error:



You can ignore this error since the editing of GPO works fine.

25.1.7 The wbinfo Operation for winbind Daemon Fails if two IP Interfaces are Present in a Domain Controller

If WINS is enabled, winbind will try to resolve a domain controller name with WINS, which might return the secondary IP address in some cases, resulting in a winbind request failure with a timeout error. This is because the domain controller is configured using the primary IP and it will not be able to resolve the domain controller name with a secondary IP. To resolve this, remove the secondary IP address entry from the `/etc/hosts` file.

25.1.8 DSfW Provisioning Fails When you Configure an Additional Domain Controller to an Existing Child Domain

DSfW provisioning fails during the Configure DNS task when the child domain controller is OES 11 SP1 or previous version or the child domain controller is upgraded to OES 11 SP2 or later. When you add a domain controller to an existing child domain, follow the steps below before provisioning:

1. Click the **DNS Service** tab of the DNS/DHCP Java Management Console.
2. Select the parent domain zone.
3. Click **Create** on the toolbar.
4. In the Create New DNS Record Window, select the resource record, then click **OK**.
5. In the Create Resource Record Window, select **Others > NS**.
6. Specify the child domain's name in the **DNS Server Domain Name** field and click **Create** . A new sub-zone is created under the parent zone.
7. Select the new sub-zone created for the child domain and click **Create** on the toolbar.
8. In the Create New DNS Object Window, select **Resource Record**, then click **OK**.
9. In the Create Resource Record Window, add an A record and specify the IP address, then click **Create**.

25.1.9 Error During DSfW Provisioning

You might receive the following error during DSfW provisioning if the LDAP certificates are not created correctly:

```
Can't contact LDAP server (-1)
```

Verify if the LDAP server is running by executing the following command:

```
$rcndsd status
```

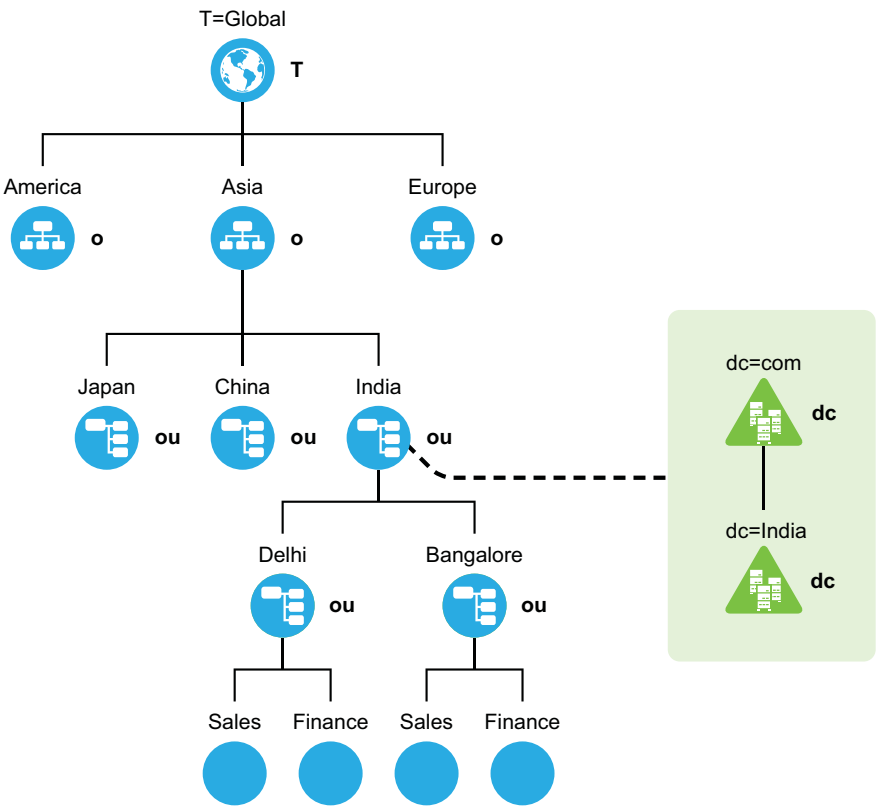
If this error is displayed and the LDAP daemon is running on the DSfW server that is contacted over secure port 636, you must execute the following command to rectify this issue:

```
ndsconfig upgrade
```

25.1.10 User Moved out of DSfW Domain is able to Access to DSfW Service

Assume that the container ou=India is mapped to a DSfW domain. A user which is part of this domain will be able to access all DSfW services such as domain login.

Figure 25-1 *Access to DSfW Service*



If you move the user to a partition above the mapped container (for example o=asia), the user will not be able to access DSfW services. However, if you move this user outside this domain boundary to another eDirectory partition which is below the mapped container(for example ou=Bangalore), and if this partition has a local replica on the DSfW server, the user will still continue to access the DSfW service. To resolve this issue, you must remove the local replica of the partition (ou=Bangalore).

25.1.11 Rename of User Object Using iManager Fails to Update the samAccountName and userPrincipalName

If you rename a user object using iManager, the respective samAccountName and userPrincipalName will not be updated. You must manually update the respective samAccountName and userPrincipalName in iManager.

1. Launch iManager and connect to a DSfW server.
2. In Roles and Tasks, select **Directory Administration > Modify Object**.
3. Specify the user object in the **Object name** field and click **OK**.
4. Click the **Other** tab.
5. Select **samAccountName** from the **Valued Attributes** list and click **Edit**.
6. Specify the appropriate value and click **OK**.

Repeat Step 5 and Step 6 to change the value of userPrincipalName.

NOTE: Optionally, you can also use MMC Users and Computers snap-in and set appropriate logon name to rectify this issue.

25.1.12 Windows Password Synchronization Fails With DSfW Domain Users for Windows XP Clients

If you have enabled the Windows Password Synchronization feature on a workstation with Client for Open Enterprise Server installed and then attempt to login to eDirectory and the DSfW domain with a different password for the same user, password synchronization fails with the following error message:

```
Failed to change windows password to match Novell. Your windows password
was not changed.
```

This issue is observed only on windows workstations with Windows XP installed.

25.1.13 Workstation Login Fails With Samba Error

When you attempt to login to workstation it fails with the following samba error message in the `/var/log/samba/log.smbd` file:

```
Failed to verify incoming ticket with error NT_STATUS_LOGON_FAILURE!
```

This might be because the keytab file is corrupted and it is unable to verify the service ticket. To rectify this issue, you must regenerate the keytab file and set the necessary permissions for the keytab file.

1 Generate the keytab file for the domain controller.

```
/opt/novell/xad/sbin/setpassword -DNOSf -r -k /var/opt/novell/xad/ds/
krb5kdc/krb5.keytab -u <DC_HOSTNAME>$
```

2 Set the necessary permission on the keytab file.

```
chmod 0640 "/var/opt/novell/xad/ds/krb5kdc/krb5.keytab"
```

3 Change the group ownership on the keytab file to named.

```
chgrp named /var/opt/novell/xad/ds/krb5kdc/krb5.keytab
```

25.1.14 On a Non-DSfW Server, eDirectory Restart Results in an Error Message

On a non- DSfW Server, if you restart eDirectory, the following error message is received:

```
Method load failed: libxadnds.so.2: cannot open shared object file: No such
file or directory
```

This is because 3 NMAS methods (IPCExternal, Kerberos, and Negotiate) fail to load on the server. These NMAS methods that are specific to DSfW are part of the `novell-xad-nmas-methods rpm` and depend on the libraries from the `novell-xad-framework rpm`. Since the `novell-xad-framework rpm` is part of the DSfW pattern and is installed only on a DSfW server, you receive this error message on a non-DSfW server.

If you receive this error message, you can ignore this message as these DSfW NMAS methods do not function in a non-DSfW server and do not impact any eDirectory functionality.

25.1.15 ADC Install Enters Wrong Context for Server

During the Additional domain controller install, the server is installed in the `cn=users` container and the field is grayed out. Any attempt to modify the context in `nds.conf` fails.

To resolve this problem, you must recreate the Certificate Authority. For information, see TID 7012509.

25.1.16 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 Scheduled Maintenance patch for OES 11 SP1.
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 `xadsd.service, rpcd.service, /etc/samba/smb.conf`, and `/etc/profile.d/novell-xad.sh.`
   - /opt/novell/xad/bin/xadcntrl reload
   - /usr/sbin/rcntp restart

25.1.17 Unable to Proceed with Installation of an Additional Domain Controller

During installation of an ADC, if the **Existing Domain Administrator Name** field is empty and grayed out, you will be unable to proceed with the installation. This issue may be due to the missing 'A' record in DNS. To confirm if this issue is due to the missing 'A' record, do the following:

1. Verify if the DNS server is running on the remote server

   `systemctl-named status`
2. Run the command `/usr/bin/dig <server name>.<domain name> +short`

   If this command displays no results, proceed to Step 3.
3. Run the command `/usr/bin/dig -t SRV _ldap._tcp.pdc._msdcs.<domain name> +short`

   If this command displays the corresponding SRV record, then this confirms the missing 'A' record in DNS.

To proceed with the installation, you must add the missing A record using Java Console. For information on how to add the record, see "Creating Resource Records" in the *DNS/DHCP Services for Linux Administration Guide*.

25.1.18 Unable to Access Sysvol

If you are unable to access sysvol refer Section 6.16, "Ensuring Filesystem ACL Support," on page 55 and TID 7009748.

25.1.19 Reverse Zone Record for Workstations Joined to CDC and ADC is Not Getting Updated

When workstations are joined to the DSfW domain, the *A* record is created in the forward zone and *PTR* record is created in the reverse zone. However, when the workstation is joined to the DSfW domain using CDC or ADC DNS server IP, the *PTR* record does not get created in the reverse zone. This is because the reverse zone DNS master is always the FRD DNS server.

To create a *PTR* record in the reverse zone, specify the FRD DNS server IP in the **Alternate DNS server field** of the TCP/IP Properties dialog box on the workstation that is being joined to the domain.

25.1.20 DSfW Provisioning Wizard Might Hang During the Restart DSfW Services Phase

The DSfW provisioning Wizard might hang during the Restart DSfW Services phase while executing CLDAP Netlogon query. This is an intermittent issue.

If the Provisioning Wizard hangs, do the following:

1. A read-write local replica of Configuration partition should be added to the DSfW server. It is recommended to add a read-write local replica of the Schema partition too. For more information, see Administering Replicas in the NetIQ eDirectory Administration Guide.
2. Restart eDirectory

   ```
   systemctl stop ndsd.service
   systemctl start ndsd.service
   ```
3. Abort the provisioning wizard and relaunch it.

25.1.21 Citrix Xenserver Fails to Join a DSfW Domain

Citrix Xenserver 5.6 fails to join a DSfW domain. This is because when Xenserver attempts to join a DSfW domain, it attempts to read certain password policy related attributes in eDirectory which fails. To enable the attributes to be readable, you need to run a script.

For more information, refer to the TID (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008231&sliceId=2&docTypeID=DT_TID_1_1&dialogID=240165588&stateId=0 0 240163546).

25.1.22 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.

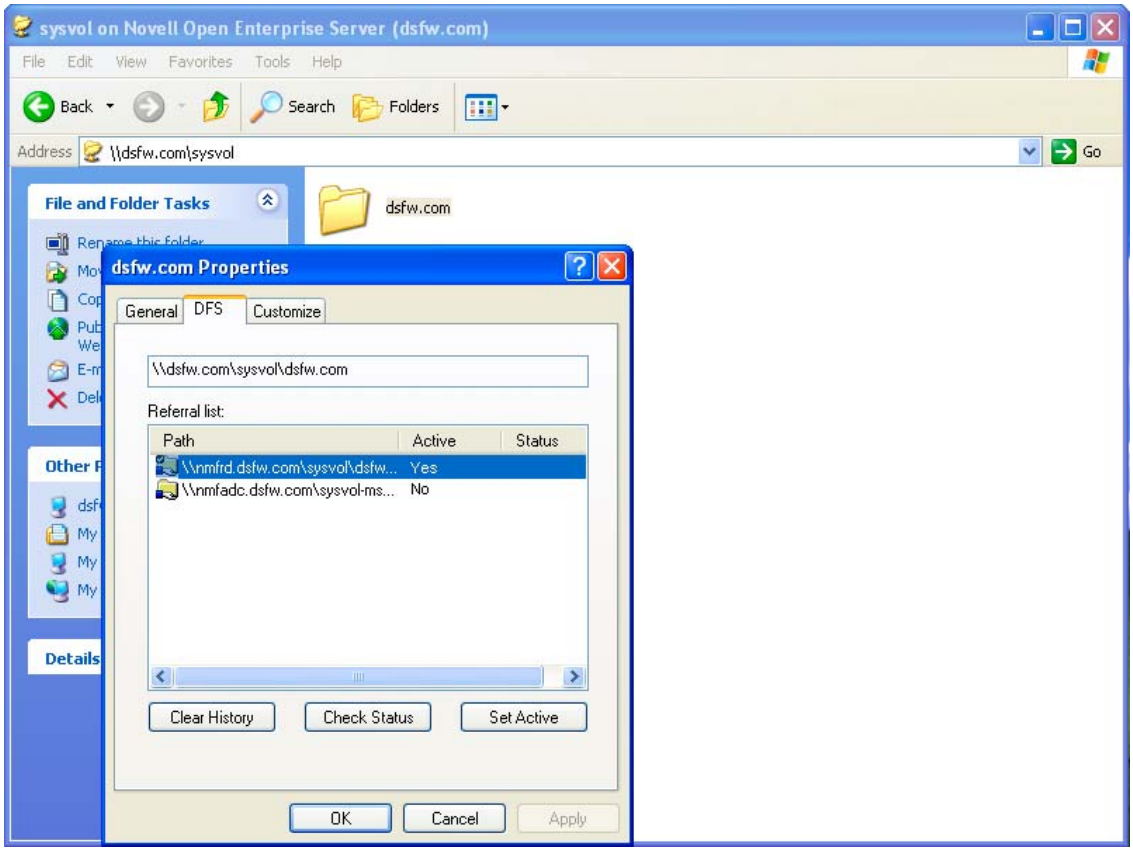
NOTE: This issue occurs only with Windows 8 or later versions.

25.1.23 Administrative Templates in the Computer Configuration and User Configuration Are Empty

While you are editing a group policy object, if the administrative templates in the computer configuration and user configuration screens are empty, it is because the DFS link is pointing to ADC instead of FRD as a PDC emulator. If this happens, you must ensure that the DFS link points to FRD as a PDC emulator by executing the following procedure:

1. Browse to the SYSVOL folder at `\\domain.tld\sysvol\` or `\\ipadress\sysvol`.
2. Right-click the domain.tld folder to view the properties, then click the DFS tab. It lists all the referrals.

3 Select the FRD link, then set it as active.



25.1.24 SLED or SLES Workstation Join to DSfW Triggers Traces in the log.smbd File

When the SLED and SLES workstations are joined to DSfW as member servers, backtraces are observed in the `/var/log/samba/log.smbd` file. This is because after joining, the workstations send periodic requests to the Samba server. The Samba server acts as a proxy and forwards these requests to the RPCD server. However, the connection between the Samba server and the RPCD server times out after 5 minutes. Therefore, periodic requests to the Samba server fail after the connection times out, and the traces are logged in the `log.smbd` file.

25.1.25 Extending the DSfW Object Classes with Mandatory Attributes Leads to Object Creation Failure in MMC

When you extend the schema of the object classes OrganizationalPerson, OrganizationUnit, and group with mandatory attributes, using MMC to create objects for these classes fails with the following error:

```
-609 MISSING MANDATORY
```

The error message can be observed by using the ndstrace utility with the LDAP tag enabled.

25.1.26 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.

25.1.27 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.

25.1.28 MMC Fails to Create Users

If you receive a failure 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.

25.1.29 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.

25.1.30 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.

25.1.31 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
```

25.1.32 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.

25.1.33 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.

25.1.34 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.

25.1.35 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.

25.1.36 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. nmbd (NMB server, NETBIOS lookup)
9. winbindd (winbind)
10. smbd (Samba)
11. sshd (SSH)
12. rsyncd (rsync)

To restart the services use the `xadcntrl reload` command.

25.1.37 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, OES Remote Manager, the Client for Open Enterprise Server, and the command line.

- "Administrator Not Able to Create Samba Shares" on page 210
- "Users Not Able to Access NSS volume/Samba Shares" on page 210

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.

25.1.38 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 `systemctl-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 `systemctl-named start` to restart the `novell-named`.

If the `novell-named` continues hanging, you should restart it to ensure its works properly.

25.1.39 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
```

25.1.40 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.

25.1.41 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.

25.1.42 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.

25.1.43 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.

25.1.44 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)

25.1.45 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(smbd, winbindd, and nmbd) to proceed.

25.1.46 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.

25.1.47 Configuring eDirectory on a Non-Default Port Affects the Installation of DSfW in a Name-Mapped Scenario

If an existing eDirectory is configured on a non-default port, the DSfW installation in a name-mapped scenario fails.

25.1.48 Issues in Using iManager and MMC Interchangeably to Add Users in a Mixed OES (non-DSfW) and DSfW Environment

OpenText recommends that you use only Micro Focus iManager to add users in a mixed OES (non-DSfW) and DSfW environment. If you use iManager or MMC interchangeably to add users, some of the attributes of DSfW users or groups created using MMC will not match with those created using iManager.

25.2 Error Messages in Log Files

- Section 25.2.1, “ndsd Log File Error,” on page 212

25.2.1 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
```

25.3 Novell SecureLogin Issues

- Section 25.3.1, “Novell SecureLogin LDAP Attribute Mappings,” on page 213

25.3.1 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.

25.4 Known Issues

- Section 25.4.1, “Cannot Configure UMC on DSfW Server,” on page 213
- Section 25.4.2, “Cannot Create Samba Shares,” on page 213
- Section 25.4.3, “Warning Message Appears on ADC Installation,” on page 214
- Section 25.4.4, “Limitation for Number of Characters in Login Username,” on page 214
- Section 25.4.5, “Creating Filr LDAP Proxy Users with MMC Fails,” on page 214
- Section 25.4.6, “Domain Join with NetBIOS Name Fails,” on page 214
- Section 25.4.7, “NTLM Authentication Fails Over SSP,” on page 214
- Section 25.4.8, “Provisioning Fails for a New DC in the Forest When PDC is Not a DNS Server after PDC Role Transfer,” on page 214
- Section 25.4.9, “Password Setting Container Might Not Be Visible On Domain Controllers In A Mixed Mode Environment,” on page 215
- Section 25.4.10, “Restriction on Fine-Grained password Policy Attribute Name Length,” on page 215
- Section 25.4.11, “Fine-Grained Password Policy Limitations,” on page 215
- Section 25.4.12, “Copying a User Object from MMC Fails,” on page 215
- Section 25.4.13, “Users Must Change Their Own Passwords,” on page 215

25.4.1 Cannot Configure UMC on DSfW Server

UMC configuration on DSfW Domain Controllers (FRD, ADC, or CDC) fail in Name-Mapped and Non Name-mapped DSfW setup. UMC is unable to detect the existing UMC server in the same tree.

25.4.2 Cannot Create Samba Shares

The Samba shares cannot be created in iManager because the NCP Server object fails to load during the process. However Samba shares can be created in the `smb.conf` file.

25.4.3 Warning Message Appears on ADC Installation

Following warning message appears for ADC installation when there is an empty space in the FRD password.

```
Few of the Domain Controllers are not reachable. Before proceeding with the installation, it is recommended to make the following Domain Controllers available: <FRD hostname>
```

NOTE: The ADC installation can proceed, and there will not be any install failures even after receiving the warning message.

25.4.4 Limitation for Number of Characters in Login Username

If a username contains more than 20 characters, a garbage value is displayed when you run "wbinfo -u" command.

25.4.5 Creating Filr LDAP Proxy Users with MMC Fails

Using Windows MMC, it is not possible to create a proxy user in DSfW domain with sufficient rights to read the user and group information.

25.4.6 Domain Join with NetBIOS Name Fails

Joining a Windows workstation to DSfW domain using the NetBIOS name fails with the following error:

```
The specified domain either does not exist or could not be contacted.
```

25.4.7 NTLM Authentication Fails Over SSP

Unable to bind to DSfW servers using NTLM when kerberos is down. This issue is fixed in the OES 2018 SP1 Update 1 patch release.

25.4.8 Provisioning Fails for a New DC in the Forest When PDC is Not a DNS Server after PDC Role Transfer

After the PDC role is transfered from Forest Root Domain to Additional Domain Controller, which is not a DNS server, adding a Domain Controller with the **Configure this Server as a DNS Server** option selected during installation fails during provisioning.

25.4.9 Password Setting Container Might Not Be Visible On Domain Controllers In A Mixed Mode Environment

In a mixed mode environment (OES 2015 and OES 2018 or later) if any of the domain controllers are updated prior to updating the FRD with 2012 schema, the password setting container might not be visible on domain controllers during object creation with 2012 schema level. Therefore it is recommended to always update the FRD with the latest schema level first and then update the domain controllers.

25.4.10 Restriction on Fine-Grained password Policy Attribute Name Length

The name of the attributes for Fine-grained password policies cannot be longer than 32 characters.

25.4.11 Fine-Grained Password Policy Limitations

- The support for the following three attributes is not available with the current implementation of Fine-Grained Password Policy due to the limitation imposed by eDirectory. Currently, eDirectory supports these attributes only at the container level.
  - `msDS-LockoutThreshold`
  - `msDS-LockoutObservationWindow`
  - `msDS-LockoutDuration`
- The values for the following attributes must be provided in multiples of number of seconds per day (86400 seconds per day).
  - `msDS-MinimumPasswordAge`
  - `msDS-MaximumPasswordAge`
- The current implementation of Fine-Grained Password Policy is limited to individual users and is not applicable for groups. This is because of the limitations imposed by eDirectory.

25.4.12 Copying a User Object from MMC Fails

When you copy a user object from MMC, it fails with an unspecified error. OpenText has no current plans to change this.

25.4.13 Users Must Change Their Own Passwords

After a user is created, the administrator cannot force password changes through MMC because the check box is disabled. Users must change their own passwords. OpenText has no current plans to change this.

A 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.

- Section A.1, “Schema Objects,” on page 217
- Section A.2, “Extending the Third-Party Schema using Traditional Methods,” on page 225
- Section A.3, “Extending the Third-Party Schema using Microsoft Active Directory Standard Methods,” on page 225
- Section A.4, “Adding an Attribute to Partial Attribute Set (PAS),” on page 228

A.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 A-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.

Attribute	Syntax	Description
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.
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.

Attribute	Syntax	Description
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.

- Section A.1.1, “Syntaxes,” on page 220
- Section A.1.2, “Attribute Mappings,” on page 221
- Section A.1.3, “Special Attributes,” on page 222
- Section A.1.4, “Class Mappings,” on page 224

A.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 A.2, “Extending the Third-Party Schema using Traditional Methods,” on page 225 for more information on automating mapping.

Table A-2 *Mapping Valid Syntaxes for Attributes in the DSfW Schema*

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

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

A.1.2 Attribute Mappings

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

Table A-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

A.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 A-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.

Attribute	Syntax	Description
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.
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.

Attribute	Syntax	Description
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.

A.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 A-5 *Attributes for the AttributeSchema Class*

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

A.2 Extending the Third-Party Schema using Traditional Methods

To traditionally 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.

A.3 Extending the Third-Party Schema using Microsoft Active Directory Standard Methods

To extend the schema for a DSfW server, you can use standard Microsoft Active Directory (AD) methods through the following approaches:

- Section A.3.1, “Manual Extension using the LDIFDE Tool,” on page 225
- Section A.3.2, “Programmatic Extension,” on page 227

Things to Consider Before Extending the Schema

- **Backup:** Schema changes are irreversible. Always back up your domain before making any modifications.
- **Test in a staging environment:** Never apply schema changes directly to a production environment. Use a replica or staging domain for testing.
- **Document OIDs and GUIDs:** Each attribute and class must have a unique Object Identifier (OID) and Global Unique Identifier (GUID). Ensure there are no conflicts to avoid potential issues.
- **Be precise:** Errors in LDIF files can result in schema corruption or unexpected behavior.

A.3.1 Manual Extension using the LDIFDE Tool

The LDAP Data Interchange Format (LDIF) is a standard file format used in LDAP implementations. The LDIF Data Exchange (LDIFDE) tool allows you to import and export Active Directory objects using LDIF-formatted files. LDIFDE is useful for batch operations, enabling you to add, create, or modify multiple Active Directory objects.

Prerequisites

- Verify the tree root replica is present on all Domain Controllers (DCs). You can verify or configure using the Identity Console.
- Join a Windows server or workstation to the DSfW domain.
- Prepare an LDIF file based on the attribute or class to be created.

Procedure

1 Run the command to extend the schema.

```
ldifde -i -v -f samplegw.ldf -c
"<SchemaContainerDN>""CN=Schema,CN=Configuration,DC=...,DC=..."
```

For more information, see Using the LDIFDE Tool (https://learn.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2003/ms870068(v=exchg.65)).

2 Verify newly added schema classes and attributes.

```
/usr/bin/ldapsearch -x -b "cn=schema" -s base -LLL -o ldif-wrap=200 |
grep "class-name"
```

3 Verify newly added schema objects.

```
ldapsearch -Y EXTERNAL -b
"cn=schema,cn=configuration,dc=domainName,dc=com" -s sub dn
```

Sample LDIF file for creating a new schema attribute

```
dn: CN=NewAttribute,CN=Schema,CN=Configuration,DC=<domainName>,DC=<com>
cn: NewAtrribute
objectClass: attributeSchema
attributeID: 1.2.840.113556.1.4.2993
attributeSyntax: 2.5.5.11
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: NewAttribute
adminDescription: NewAttribute
oMSyntax: 24
searchFlags: 1
lDAPDisplayName: newAttribute
schemaIDGUID:: 9U4AcMMlakSXyJlq6FZndg==
attributeSecurityGUID:: YrwFWMm9KESl4oVqD0wYXg==
systemOnly: FALSE
systemFlags: 16
```

Sample LDIF file for deleting a schema attribute

```
dn: CN=NewAttribute,CN=Schema,CN=Configuration,DC=<domainName>,DC=<com>
changetype: delete
```

Sample LDIF file for creating a new schema class

```
dn: CN=New-Schema-
Class,CN=Schema,CN=Configuration,DC=<domainName>,DC=<com>
cn: New-Schema-Class
objectClass: classSchema
subClassOf: top
governsID: 1.2.840.113556.1.5.237
rDNAttID: cn
showInAdvancedViewOnly: TRUE
adminDisplayName: New-Schema-Class
adminDescription: New-Schema-Class
objectClassCategory: 1
lDAPDisplayName: newSchemaClass
schemaIDGUID:: iBJWfwFT0RGpxQAA+ANnwQ==
systemOnly: FALSE
systemMayContain: seeAlso
defaultSecurityDescriptor:
D:(A;;RPWPCRCCDCLCLOLORCWOWDSDDTDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;
;SY)(A;;RPLCLORC;;;AU)
systemFlags: 16
defaultHidingValue: TRUE
```

Sample LDIF file for deleting a schema class

```
dn: CN=New-Schema-
Class,CN=Schema,CN=Configuration,DC=<domainName>,DC=<com>
changetype: delete
```

A.3.2 Programmatic Extension

Programmatic schema extension involves modifying the directory schema through code rather than manually using tools like LDIF files. This approach allows administrators to automate schema changes, integrate them into applications, and efficiently manage complex scenarios, offering flexibility and scalability, especially in large or dynamic environments.

Prerequisites

- Verify the tree root replica is present on all Domain Controllers (DCs). You can verify or configure using the Identity Console.
- Join a Windows server or workstation to the DSfW domain.
- Install Visual Studio.

Procedure

1. Create a new project in Visual Studio.
2. Run the script to extend the schema

   For sample script, see Example Code for Extending the Schema Programmatically (https://learn.microsoft.com/en-us/windows/win32/ad/example-code-for-extending-the-schema-programmatically).
3. Verify newly added schema classes and attributes.

```
/usr/bin/ldapsearch -x -b "cn=schema" -s base -LLL -o ldif-wrap=200 |
grep "class-name"
```

4 Verify newly added schema objects.

```
ldapsearch -Y EXTERNAL -b
"cn=schema,cn=configuration,dc=domainName,dc=com" -s sub dn
```

A.4 Adding an Attribute to Partial Attribute Set (PAS)

The Global Catalog server stores the partial representation of every object of the domain. The Partial Attribute Set (PAS) is an attribute set that is returned when a global catalog search is done. When an attribute is included to the Partial Attribute Set, the attribute is returned during global catalog searches.

When the PAS is updated or modified, the schema cache maintained in every domain controller needs a refresh. Execute the below LDIF file on every domain controller as the domain administrator.

```
dn:
changetype:modify
add:schemaupdatenow
schemaUpdateNow:1
```

B Understanding DSfW in Relation to IDM and Samba

This section analyses the features and capabilities of DSfW in relation to Samba and IDM.

- Section B.1, “Understanding DSfW in Relation to Samba,” on page 229
- Section B.2, “Understanding DSfW in Relation to IDM,” on page 231

B.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. DSfW includes novell-oes-samba package 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.

A DSfW server uses the following services in order to provide Active Directory equivalent environment:

- SAMBA
- 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 **OES Domain Services for Windows** pattern is selected, a set of other dependent RPMs also get selected. Provisioning helps in configuring DSfW and the supporting services.

Table B-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 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 and Fine-Grained Password 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 OES 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 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.

B.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 Client for Open Enterprise Server on the desktop.

The following table analyses the features of DSfW and IDM.

Table B-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 and Fine-Grained Password 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

C 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 C-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
RPC 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 10, “Activities After DSfW Installation or Provisioning,” on page 111 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.

D DSfW Password Policy Attributes

This section describes the default attributes that are required for creating the DSfW password policy for DSfW users.

Table D-1 *DSfW Password Policy Attributes*

Attribute	Description	Value
nspmConfigurationOptions	Defines the characteristics of the password policy such as enabling universal password policy. The value specified is an integer value.	832
passwordExpirationInterval	Time interval (in seconds) after which the password will expire.	3628800 (time in seconds)
nspmAdminsDoNotExpirePassword	Specifies that the administrator password cannot expire.	True
nspmSpecialCharactersAllowed	Allows special characters in passwords.	True
nspmNumericCharactersAllowed	Allows numeric characters in passwords.	True
nspmLowerAsLastCharacter	Allows the last character of the password to be in lowercase.	True
nspmLowerAsFirstCharacter	Allows the first character of the password to be in lowercase.	True
nspmExtendedCharactersAllowed	Allows extended characters in passwords.	True
nspmCaseSensitive	Enables passwords to be case sensitiv.e	True
nspmSpecialAsLastCharacter	Allows the last character of the password to be a special character.	True
nspmSpecialAsFirstCharacter	Allows the first character of the password to be a special character.	True
nspmNumericAsLastCharacter	Allows the last character of the password to be a numeric character	True
nspmNumericAsFirstCharacter	Allows the first character of the password to be a numeric character.	True
passwordUniqueRequired	Specifies whether any old passwords can be reused.	False
loginGraceLimit	Specifies the number of grace logins allowed.	6
passwordAllowChange	Specifies whether the eDirectory object can change the password.	True

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. 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 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.

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.

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.

Additional Domain Controller. An added server used to improve the availability and reliability of network services. If you have an additional domain controller, it helps in fault tolerance and balances the load of existing domain controllers. It also provides additional infrastructure support to the sites.

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.

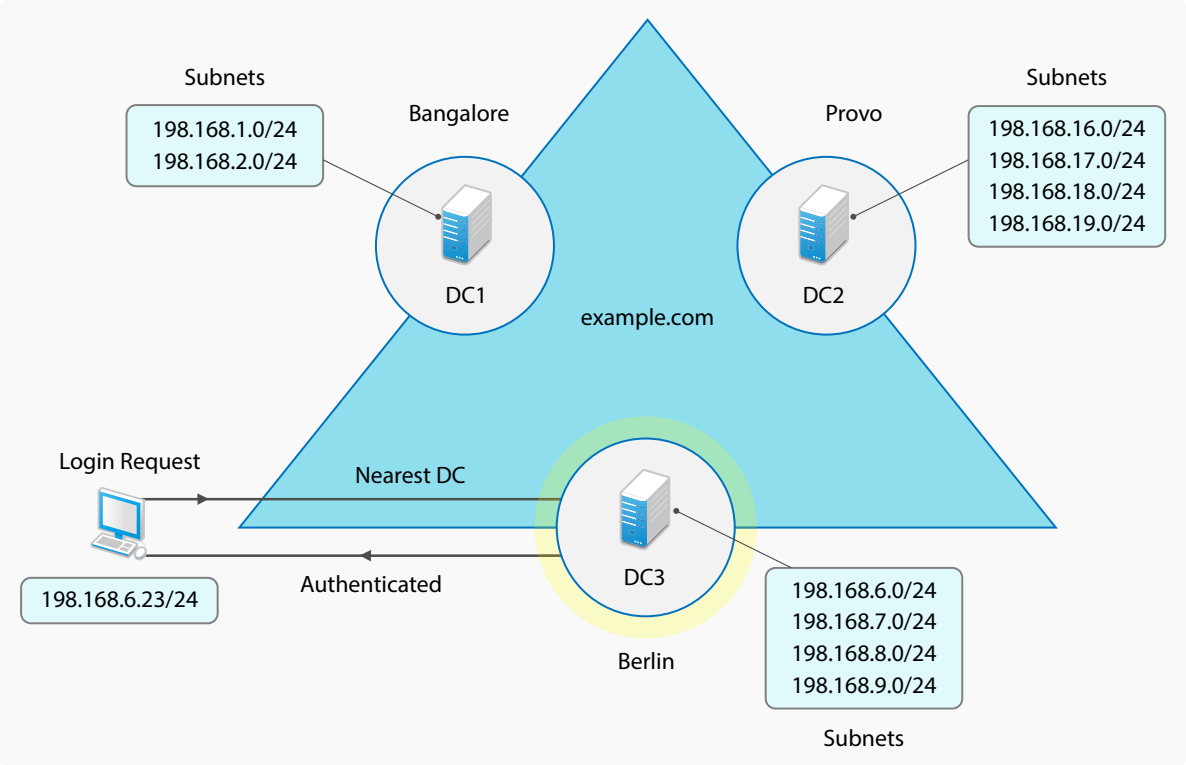
Trust-Posix-Offset Attribute. An offset that the system uses to generate POSIX user and group identifiers that correspond to a given SID. To generate a POSIX identifier, the system adds the RID from the SID to the POSIX offset of the trusted domain identified by the SID.

26 Configuring Sites and Subnets

A site is made up of one or more Internet Protocol (IP) subnets that are linked by high-speed and reliable connections. Sites represent the physical structure or topology of your network, and a domain represents the logical structure where all the domain controllers are logically linked. Subnets are associated to a site. Associating a subnet to a site implies associating an IP address or set of IP addresses to the site.

In a DSfW environment, when you configure the first domain controller, a site named “Default-First-Site-Name” is created. All domain controller objects for all the domains are associated with this site.

Figure 26-1 *Sites and Subnets*



Having multiple domain controllers in different geographical locations associated with the same domain and within a single site is not an ideal scenario. For such environments, the sites and subnets feature enables you to configure multiple sites and distribute domain controllers over different geographical locations.

After you configure the sites and subnets feature, when a client tries to log in to a domain, the request goes to the nearest available domain controller, thus ensuring faster domain login.

- Section 26.1, “Planning for Sites and Subnets Support,” on page 242
- Section 26.2, “Managing Sites and Subnets,” on page 242
- Section 26.3, “Troubleshooting,” on page 242

26.1 Planning for Sites and Subnets Support

Use the following guidelines to configure sites and subnets:

- Ensure that all the domain controllers present in the replica ring are up and running.
- All domain controllers must have replicas of all partitions with objects that belong to the domain.

26.2 Managing Sites and Subnets

Using MMC (Active Directory Sites and Services) snap-in tool, you must first create a new site and subnet. You must then associate the subnet to a site and move the container object from “Default-First-Site-Name” or any other site to the new site.

1. Create a site. For more information, see Creating a Site.
2. Create a subnet. For more information, see Creating a Subnet.
3. Associate a subnet with the site. For more information, see Associating a Subnet with a Site.
4. Move the Active Directory server object of the domain controller from “Default-First-Site-Name” or any other site to the new site.

   NOTE: Although the Active Directory server object is moved from one site to the other, the changes do not get reflected immediately.

The movement of Active Directory server object from one site to the other completes with the help of a crontab job (`sites_dnsupdate.py`) which takes care of creating 6 DNS records for each site. Use the `sites_dnsupdate.py --logging` option in the crontab job to capture the additional logs apart from the error and warnings.

NOTE: Ensure that you use the MMC (Active Directory Sites and Services) snap-in tool on a DSfW server only to move the Active Directory server object from one site to another. OpenText recommends you to not perform any other operation using this tool other than the move operation on the domain controller.

26.3 Troubleshooting

This section describes known issues and frequently asked questions for configuring Sites and Subnets.

26.3.1 Moving a DSfW Server to a Site Results in an Error Message

When you move the DSfW server from one site to another, you might receive the following error message:

```
Windows cannot move object DSFW-SERVER because: There is no such object on
the server.
```

This is because of the latency during the movement operation. You may ignore this message as this does not affect the movement of the DSfW server to the destination site.

NOTE: After you move the DSfW server, the changes might not get reflected in MMC immediately. If the changes do not get reflected immediately, you must manually refresh.