eDirectory Field Guide

Rick Killpack

Apress®

eDirectory Field Guide

Copyright © 2006 by Rick Killpack

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN (pbk): 1-59059-553-X

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jim Sumser
Technical Reviewer: Kevin Fenn
Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, Jason Gilmore, Jonathan Hassell, Chris Mills, Dominic Shakeshaft, Jim Sumser
Associate Publisher: Grace Wong
Project Manager: Sofia Marchant
Copy Edit Manager: Nicole LeClerc
Copy Editor: Bill McManus
Assistant Production Director: Kari Brooks-Copony
Compositor: Dina Quan
Proofreader: Dan Shaw
Indexer: Valerie Perry
Artist: Kari Brooks-Copony
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `http://www.springeronline.com`.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail `info@apress.com`, or visit `http://www.apress.com`.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

Contents at a Glance

About the Author xi
About the Technical Reviewer xiii
Author's Note xv

PART 1 Installation and Migration

CHAPTER 1 Installation 3
CHAPTER 2 Installing into an Existing Tree 25
CHAPTER 3 Migration Methodologies 39

PART 2 Administration

CHAPTER 4 Partition Operations 63
CHAPTER 5 Backup and Restore Operations 79
CHAPTER 6 Schema Administration 99
CHAPTER 7 LDAP 111
CHAPTER 8 Management and Monitoring Tools 131

PART 3 Troubleshooting eDirectory

CHAPTER 9 Troubleshooting with NDS iMonitor 145
CHAPTER 10 Common Command-Line Utilities 181
CHAPTER 11 Troubleshooting Common Issues 225
CHAPTER 12 Large-Scale Considerations 245
CHAPTER 13 Troubleshooting Security 267
APPENDIX Comparison of eDirectory Versions 277

INDEX 285

Contents

About the Author xi
About the Technical Reviewer xiii
Author's Note xv

PART 1 Installation and Migration

CHAPTER 1 Installation 3
Prerequisites 3
Supported Operating Systems 4
Applying Patches 4
Hardware Considerations 4
Server-to-Server Communication 6
NetWare 6
Microsoft Windows 7
Linux, Solaris, HPUX, and AIX 7
General Recommendations 10
Time-Synchronization Considerations 10
Troubleshooting Installation Failures 13
NetWare 14
Microsoft Windows 17
*nix 19
Capturing a DSTRACE Log 21

CHAPTER 2 Installing into an Existing Tree 25
Protocol Considerations 25
Security Considerations 26
eDirectory Security Infrastructure 27
Existing Tree Considerations for the Security Components 33
NDS and eDirectory Patch Levels 35
Loss of Trustee Assignments 35
Unknown Objects 36

CHAPTER 3 Migration Methodologies 39
Updating the Program Files 41
NetWare 41
Microsoft Windows 49
Solaris and Linux 50

Migrating the eDirectory Database to eDirectory 8.7.3.x 51
Migrating the DIB from NDS 6.x or NDS 7.x to eDirectory 8.5 51
Migrating the DIB from NDS 8, eDirectory 8.5, eDirectory 8.6, or eDirectory 8.7 to eDirectory 8.7.3 53
Mixed-Environment Considerations 54
Loss of Trustee Assignments 54
Unknown Objects 55
Administration Options 56
NWAdmin 56
ConsoleOne 56
iManager 56
Protocol Considerations When Introducing Multiple Platforms 58

PART 2 Administration

CHAPTER 4 Partition Operations 63
Partition Splits 64
Partition Split Best Practices 65
Troubleshooting Failed Partition Splits 67
Partition Merges 68
Partition Merge Best Practices 68
Troubleshooting Failed Partition Merges 71
Move SubTree Operations 72
Move SubTree Best Practices 73
Troubleshooting Failed Move SubTree Operations 74
Tree Merge 75
NetWare 77
Windows 77
Solaris, Linux, AIX, HPUX 78

CHAPTER 5 Backup and Restore Operations 79
Types of Backup Options 80
Hot Continuous Backup (Backup eMTool) 80
Directory Backup and Restore in NWCONFIG 81
DIB Backup Through DSREPAIR 82
NDSBackup 82
TSA Backup 83
File Copy 83
DIBClone 84
Backup and Restore Strategies 85
Automated Backup 85
No Data Loss 86
Remote Capabilities 87
No Additional Configuration Requirements After Restore 87

Size of the DIB in eDirectory . . . 87
Partitioning Considerations . . . 88
Selective Restore Requirements . . . 88
File System Considerations . . . 88
Multiple-Server Restore Strategies . . . 89
Best Practice Recommendations . . . 89
Using Hot Continuous Backup . . . 90
The Backup File Header . . . 91
Roll-Forward Logging . . . 94
Using iManager to Configure and Perform Backup and Restore . . . 96
Backing Up the Security Infrastructure . . . 98

CHAPTER 6 Schema Administration . . . 99

Schema Synchronization . . . 99
Monitoring Schema Synchronization . . . 100
Controlling Schema Synchronization . . . 102
Schema Comparison . . . 103
Schema Modification . . . 105
Extending Schema . . . 105
Modifying Existing Schema . . . 108
Using Auxiliary Classes . . . 109

CHAPTER 7 LDAP . . . 111

LDAP Binds . . . 112
DN . . . 113
Password . . . 113
Server Address and LDAP Port . . . 113
Connection Method . . . 113
Understanding LDAP Queries . . . 114
LDAP Filter . . . 114
Scope . . . 115
Base . . . 115
Performance Considerations . . . 115
Persistent Search . . . 121
Managing the LDAP Objects . . . 121
LDAP Server Object . . . 122
LDAP Group Object . . . 123
Creating and Configuring the LDAP Objects . . . 124
Walking the Tree . . . 127
Default Referral . . . 127
Conditions to Use Default Referral . . . 128
Referral Options . . . 128
Access Control . . . 128
Using ICE to Bulk-Load Data . . . 129
Summary . . . 130

CHAPTER 8 Management and Monitoring Tools 131
iManager: Managing Your eDirectory System 131
Roles and Tasks View 132
View Objects View 137
NDS iMonitor: Monitoring Your eDirectory System 138
Agent Summary 139
Agent Synchronization 139
Known Servers 139
Schema 140
Agent Configuration 140
Trace Configuration 140
Agent Health 141
Agent Process Status 141
Agent Activity 141
Connections 142
Error Index 142
SNMP: Monitoring the eDirectory Event System 142

PART 3 Troubleshooting eDirectory

CHAPTER 9 Troubleshooting with NDS iMonitor 145
NDS iMonitor Page Descriptions 146
Agent Summary 146
Agent Synchronization 146
Known Servers 147
Schema 147
Agent Configuration 147
Trace Configuration 148
Agent Health 148
Agent Process Status 149
Agent Activity 149
Connections 149
Error Index 149
Troubleshooting NDS iMonitor 150
Understanding the iMonitor Process 150
Determining the HTTP Ports 151
Understanding the HTTP Server Object 152
Using DSTRACE to Troubleshoot iMonitor Issues 158
Troubleshooting Unknown Objects 158
Identifying the Unknown Objects 160
Determining Why the Object Is Unknown 161
Resolving the Condition That Created the Unknown Object 164
Reassigning the Correct Object Type to the Object 165
Troubleshooting Schema 166
Finding the Schema Issue 166
Deciding Which Server Contains Valid Schema 167

Using NDS iMonitor to Remedy Schema Issues . . . 170
Troubleshooting Obituaries . . . 172
Processing Obituaries . . . 173
Using NDS iMonitor to Identify Obituaries . . . 175
Using NDS iMonitor to Resolve Obituary Issues . . . 176
Troubleshooting Processor High Utilization . . . 177
Using Agent Activity . . . 178
Using Trace . . . 179
Using Agent Configuration . . . 179
Summary . . . 180

CHAPTER 10 Common Command-Line Utilities . . . 181

DSREPAIR . . . 182
Launching DSREPAIR . . . 182
DSREPAIR Command-Line Options . . . 184
DSTRACE . . . 198
Understanding the Different DSTRACE Modules . . . 198
Monitoring the DSTRACE Operations . . . 203
NDSConfig . . . 218
LDAPConfig . . . 219
NDSStat . . . 220
NDSLogin . . . 220
NDSSch . . . 221
EDIRUTIL . . . 221
ICE . . . 222
Summary . . . 223

CHAPTER 11 Troubleshooting Common Issues . . . 225

High Processor Utilization . . . 226
Detecting the Offending Process . . . 226
Bindery Issues . . . 228
Looping Requests on Connections . . . 229
Synchronization Issues . . . 231
Schema Synchronization Issues . . . 233
Offending Functions . . . 233
Trends . . . 234
High Memory Consumption . . . 235
Identifying the Process That Is Consuming Most of the Memory . . . 235
Identifying the Process Within eDirectory That Is Consuming the Memory . . . 237
Identifying Memory Fragmentation Issues . . . 239
Slow Logins Using Client 32 . . . 240
Eliminating Workstation and Network Issues . . . 240
Troubleshooting eDirectory Bottlenecks . . . 241
Troubleshooting Tree-Walking Issues . . . 242
Summary . . . 244

CHAPTER 12 Large-Scale Considerations 245
Database Cache 246
Configuring Dynamic Cache Settings 246
Configuring Static Cache Settings 247
Using NDS iMonitor to Fine-Tune Database Settings 248
Memory Management 249
NetWare 250
Windows 250
Linux, Solaris, AIX, and HP-UX 250
LDAP Considerations 251
Indexes 251
Tree Design 254
Processor Considerations 256
Speed of the Processor 256
Number of Processors 256
Disk I/O 257
Disk Cache 257
Direct Attached Storage 257
Checkpoint Thread 258
DIBClone 261
DSREPAIR 262
Repairing a Single Object 262
Disabling Reference Checks 263
Repairing a Replica 263
Management Utilities 264
NDS iMonitor 264
iManager 265
Summary 266

CHAPTER 13 Troubleshooting Security 267
Troubleshooting NICI 268
Deleting Corrupt NICI Files 269
Creating New NICI Keys 269
Troubleshooting Server Certificates 270
Troubleshooting User Certificates 271
Troubleshooting the CA 271
Troubleshooting the Tree Key 272
Summary 275

APPENDIX Comparison of eDirectory Versions 277
Changes in eDirectory 8.6.x 278
Changes in eDirectory 8.7.0 279
Changes in eDirectory 8.7.1 281
Changes in eDirectory 8.7.3 282
Changes in eDirectory 8.8 283

INDEX 285

About the Author

Rick Killpack is currently the eDirectory product manager for Novell, Inc. He started at Novell in 1991 and has been involved in the technology business ever since that time. He spent seven years as a third-tier eDirectory technical support engineer for Novell. Rick contributes once a month to Novell's eDirectory LogicSource, which is a document that describes at a pseudo-code level all processes within eDirectory. With his in-depth knowledge of how eDirectory works from reviewing the code, supporting the product, and helping customers implement the product, Rick is considered one of the world's authorities on Novell eDirectory.

About the Technical Reviewer

Kevin Fenn, a native of the San Diego, California area, has worked in the support industry since September 1997 and has been with Novell since May of 2000. He is currently a World Wide Support Escalation Engineer at Novell supporting NMAS, eDirectory, Security Components (PKI, NICI, etc.), and iManager. He is a member of the iManager Core Team representing Novell Technical Services (NTS) and works tightly with iManager product developers and product managers. He graduated with a master's degree in Information Systems Management from Brigham Young University in December 2000. Kevin is considered one of the lead support engineers for iManager. His hobbies include rock climbing, camping, and geocaching. He currently resides in Spanish Fork, Utah with his wife and two children.

Author's Note

Toward the goal of making this guide as easy as possible to use in the field, where relevant, I have provided the same material in more than one chapter, so you don't have to flip back and forth between chapters to get the full picture on a topic.

PART 1

Installation and Migration

Part 1 of the *eDirectory Field Guide* emphasizes things you need to know while installing or upgrading eDirectory. It is comprehensive insofar as it deals with the nuances of all the eDirectory-supported platforms, but it does not give step-by-step instructions on how to install or upgrade eDirectory. The purpose of Part 1 is to complement the *Novell eDirectory Administration Guide* to ensure that you have a successful experience while installing or migrating to eDirectory. However, it does include tips and tricks that are not contained in the *Novell eDirectory Administration Guide*.

CHAPTER 1

Installation

The following topics are covered in this chapter:

- Prerequisites
  - Supported operating systems
  - Applying patches
  - Hardware considerations
- Server-to-server communication
  - NetWare
  - Microsoft Windows
  - Linux, Solaris, HPUX, and AIX
  - General recommendations
- Time-synchronization considerations
- Troubleshooting installation failures
  - NetWare
  - Microsoft Windows
  - *nix
  - Capturing a DSTRACE log

Prerequisites

This chapter does not go into detailed eDirectory installation procedures, but rather discusses tips on how you can prevent failed installations and how you can troubleshoot various issues that may arise during the installation and configuration of eDirectory. For general information about installing Novell eDirectory, please see the *Novell eDirectory Administration Guide* for your version of eDirectory at `http://www.novell.com/documentation`.

It is beyond the scope of this chapter to discuss in detail all prerequisites for the installation of eDirectory, but I will discuss in this section the specific issues for you to pay special attention to before you install eDirectory.

Supported Operating Systems

As new releases of eDirectory are shipped, it is important to read the new README files and current documentation. Most releases of eDirectory, including Interim Releases (IRs), often drop certain operating systems and architectures and consistently add others. A good example of this can be seen with eDirectory 8.7.3 IR3. eDirectory 8.7.3 IR2 supported Red Hat Linux Advanced Server (AS) 2.1. eDirectory 8.7.3 IR3 added support for Red Hat AS 3.0.

Decisions made by Novell to drop support for a particular operating system (OS) or platform are often driven by the OS vendor's support position. As the OS vendor drops support for a particular OS version, eDirectory often drops support for that OS version as well.

Applying Patches

Another point of consideration is to keep your current eDirectory environment updated with the latest patches. As eDirectory IRs or support packs are released, recommendations of associated security component versions (NICI, NMAS, PKI, and NTLS) are listed in the IR patch README files. In the latest eDirectory IRs (IR4 or greater), the recommended security component patches are bundled with the eDirectory patch. To ensure quality and reliability, it is important to apply all patches together. Novell tests the security components and eDirectory patches together as a suite.

Hardware Considerations

Novell's documentation for eDirectory (`http://www.novell.com/documentation`) lists the minimum versions of the supported operating system as well as the minimum support packs that need to be in place to install eDirectory. These requirements change often. Make sure that you review the prerequisites listed in the eDirectory documentation before you install eDirectory.

An important note to keep in mind is that the prerequisites listed in the eDirectory documentation are *minimum* prerequisites. Most of the minimums are based on an average system, which is somewhere around 500 users. It is critical that you determine how eDirectory will be used in your environment. Determining what operating system or what platform should be used for each business solution is out of the scope of this book. However, Novell has published good documents on how to determine what resources

are needed for each business solution. (See eDirectory LogicSource ➤ eDirectory Best Practices at Novell's subscription page, `http://support.novell.com/subscriptions/`, for more information on selecting operating systems and platforms that are right for your environment.)

If the hardware and operating system that you have selected do not have the resources required for how you want to implement eDirectory, failure and dissatisfaction will certainly follow. When determining what hardware to use, you first need to identify the biggest potential bottlenecks. Next, make that bottleneck large enough to handle the maximum amount of information that you need out of eDirectory. The major bottlenecks for eDirectory are described in the following sections.

Memory

Large numbers of objects and a lot of search requests will require more memory than other operations. According to Novell testing, allocating more than 1 GB of memory toward eDirectory database cache may actually decrease performance.

Number of Processors (CPUs)

If a large number of concurrent users are on the eDirectory servers, more CPUs will show performance increases.

Speed of Processors (CPUs)

The faster the processor, the more transactions per second that will be achieved. Remember that this statement is true only if the processor is maxed out (seeing high utilization). If the processor is not maxed out, there is another bottleneck and increasing processor speed will not help.

I/O Channel

If the database is too large to fit all objects into memory, the I/O channels will be a factor for all types of transactions. Typically, with large databases, the I/O channel is the biggest bottleneck. The following are some general recommendations:

- Increasing disk cache usually improves search performance. The I/O channel to memory is much faster than the I/O channel to the physical disk.
- Increasing the maximum dirty cache can improve systems that have a large number of writes.
- Increasing free disk space may help reduce high utilization, which can occur if there is not enough available local disk space.

■ **Note** The preceding recommendations may vary depending on your system and how the database is utilized.

Server-to-Server Communication

When an eDirectory server is added into an existing tree, the eDirectory Directory Agent (DA) needs a way to locate the server address of a server that holds a copy of the root partition of the tree. The DA on the new server must contact a copy of root for the following reasons:

- The DA needs to request the schema from the server holding a copy of root.
- The DA needs to make a request to add a new NCP server object into the existing eDirectory tree.

For all of this to occur, a connection must be established between the new server's DA and the DA on the server that holds a copy of the root partition. The root server's address must be obtained in order for a connection to be made. The methodology used to obtain the root server's address depends on the operating system that resides on the server that is being added to the eDirectory tree. Each address discovery method for each operating system is briefly discussed in the following sections.

NetWare

NetWare uses a proprietary version of Windows Sockets (Winsock) to perform the tree name resolution. NetWare's registry lists the namespaces that are available for service resolution. By default, Winsock is configured on NetWare 6.5 to try the following namespaces in the listed order:

- Domain Name Service (DNS)
- SYS:\ETC\HOSTS
- Service Location Protocol (SLP) (used by the TCP protocol)
- Service Advertising Protocol (SAP) (used by the IPX protocol)

Because SLP and SAP are the only namespace providers that store eDirectory tree names, DNS and the static HOSTS file cannot be used during the installation.

If the tree is not registered in SLP or SAP, or the name lookup fails for some other reason, eDirectory will allow you to manually specify the IP address at installation time.

Microsoft Windows

With eDirectory 8.7.1 and greater running on Microsoft Windows, eDirectory has three ways of discovering the tree name:

- *SLP provided by Novell Client32*: Novell Client32 ships with an SLP User Agent (UA). The UA communicates with a DA to query for service information. In order for this to work properly, Client32 needs to be configured to query the DA and the scope in which the server holding a copy of the root partition is registered.

■ **Note** For more information on how to configure SLP for Novell Client32, see the Novell Client32 documentation at `http://www.novell.com/documentation`.

- *SLP provided through OpenSLP*: When installing eDirectory 8.7.3 or greater onto Microsoft Windows, the installation checks to see if Novell Client32 is installed on the Windows server. If it is installed, eDirectory uses the UA from Client32. If Client32 is not installed, eDirectory installs and uses OpenSLP for tree name resolution.

  By default, the eDirectory installation configures OpenSLP to run as a UA and Server Agent (SA) only. OpenSLP is also set to auto-discover the DA. If multicasting and broadcasting are not allowed in the environment, configure OpenSLP to point to the specific DA and the specific scope in which the server that holds a copy of the root partition is registered.
- *Manual specification*: If, for whatever reason, the tree name lookup fails through SLP, the eDirectory installation prompts you to manually specify the IP address of the server that holds a copy of the root partition. If you are unsure of the SLP configuration in the tree, this option is recommended.

Linux, Solaris, HPUX, and AIX

The Linux, Solaris, HPUX, and AIX (all UNIX and Linux platforms collectively hereafter are referred to as *nix) operating systems function slightly differently from the other platforms. There are two distinct steps involved in installing eDirectory and adding the server into an existing tree:

1. Install the binaries onto the server.
2. Configure an instance of eDirectory on the server.

The address of the server that holds a copy of the root partition of the existing tree is required during the configuration stage. Like Microsoft Windows, the *nix operating systems use SLP for tree name discovery. There are four methods of finding the tree name, described in the following sections.

/etc/hosts.nds

The DA first looks for the presence of a static text file called /etc/hosts.nds. The tree name can be specified in the hosts.nds file along with an IP address of the server that holds a copy of the root partition.

If this file exists, it must have correct information about the tree name. If the address specified in the hosts.nds file is incorrect, or the tree name is specified incorrectly, the installation will not try to use other discovery methodologies. It will simply fail, with an error stating that the tree could not found.

By default, with the exception of a Novell Open Enterprise Server (OES), an /etc/hosts.nds file is not created. To create one, simply create a text file called hosts.nds in the /etc/ directory. Add to the text file the tree name with the following syntax:

```
Treename.      <server address>
e.g. MyEdirTree.      192.68.1.4
```

For more information about the /etc/hosts.nds file, see the man pages for hosts.nds on a *nix server where eDirectory is installed.

slpuasa

Starting with eDirectory 8.5 (and ending with eDirectory 8.7.3 IR5, as discussed in the next section), a Novell proprietary module called slpuasa was included with the default eDirectory installation. By default, this module is used while adding a server to an existing tree if the /etc/hosts.nds file is not present. This module acted as a UA as well as an SA. It could not act as a DA. This module performed a DA discovery and looked for the tree name. If the DA could not be discovered or the server that held a copy of the root partition of the existing tree was not registered to the DA that was found, the installation would fail.

■ **Note** There is a not a specific call to the slpuasa binary. The slpuasa binary loads in the ndsd process space by default. If it is loaded, any SLP request will be handled by the slpuasa daemon.

OpenSLP

Starting with eDirectory 8.7.3 IR5 (included with OES), Novell discontinued shipping or supporting the proprietary slpuasa on Linux. Also, the slpuasa daemon will not run on HP-UX. In both stated cases, Novell's supported SLP solution is OpenSLP.

Novell also recommends that OpenSLP be used instead of the slpuasa daemon on all *nix platforms, because the slpuasa module was based off of SLP version 1 specifications and has many limitations.

To disable the slpuasa daemon and enable the OpenSLP daemon, perform Task 1-1.

Task 1-1. Disabling slpuasa and Enabling OpenSLP

1. If the slpuasa daemon is running, stop the slpuasa daemon (/etc/init.d/slpuasa stop).
2. Remove the slpuasa script from the run levels:
   a. By default, the slpuasa script is configured to run in runlevel 3 and runlevel 5.
   b. Check the local operating system documentation on how to remove a script from a run level.
3. Make sure that the OpenSLP package has been installed.
4. Modify the /etc/slp.conf file and add applicable information to enable SLP to discover a DA.
5. Start the OpenSLP daemon (/etc/init.d/slpd start).
6. Modify runlevel 3 and runlevel 5 startup scripts and add the slpd script to the list of modules that load on startup.

■ **Note** For more information on how to configure run levels, see the specific operating system's documentation.

Manual Specification

If all other tree name discovery methodologies fail, configure the instance of eDirectory with the command-line tool `ndsconfig`, using the `-p` <*server address*> parameter. Specify the server IP address of a server that holds a replica of the root partition of the tree in the <*server address*> field; for example:

```
ndsconfig -p 192.65.1.2
```

assuming that 192.65.1.2 is a server that holds a replica of the root partition.

General Recommendations

Although each operating system allows you to manually specify a server address to establish communication when adding a server into an existing tree, it is highly recommended that SLP be configured correctly.

There are certain tools and features within eDirectory that require a tree name lookup and will always use SLP (or the static hosts.nds file on the *.nix platforms) to find the tree name. If SLP is not configured correctly, these tools will fail. The following are several examples of tools and features that may fail:

- `ndsconfig add`: This option allows you to add to eDirectory other eDirectory components on the *nix operating systems such as SAS, SNMP, LDAP, and HTTP.
- `ndsstat -s`: This option allows you to see all servers known to the database on the *nix operating system.
- *DSRepair* ➤ *Repair server addresses*: This is a cross-platform option that discovers the server address of any server in the tree and updates the information on the corresponding NCP server object in the tree as well as any replica ring of the replicas that the NCP server holds.

On the *nix platforms, the hosts.nds file or SLP is exclusively used. On NetWare, DNS or the SYS:\ETC\HOSTS file can also be used for this feature.

Time-Synchronization Considerations

NDS and eDirectory use time stamps extensively. Time stamps are used to verify the version of a specific object within the database. If an object has a time stamp newer than the time since the last synchronization cycle to a specific server, the object is sent to the remote server. For all of this to work properly, the local server and the remote server must have synchronized time.

NetWare ships a time-synchronization tool called TIMESYNC.NLM. This tool uses the Novell proprietary NCP protocol. It can communicate with other servers over IPX as well as IP. TIMESYNC.NLM has a built-in algorithm that ensures that the time is synchronized for all the servers within the defined time-synchronization environment.

As eDirectory added support for non-NetWare platforms, alternative time-synchronization methods became a necessity. Time-synchronization modules themselves are independent of eDirectory. As long as all servers within a tree have their time set the same, the method used to get time synchronized is irrelevant to eDirectory.

To make TIMESYNC.NLM compatible with other time-synchronization applications residing on non-NetWare platforms, it was enhanced to be able to send and receive NTP (an open-source time standard protocol) formatted packets. This is not to say that TIMESYNC.NLM follows the NTP-defined algorithm for keeping servers synchronized. TIMESYNC.NLM is simply able to send and receive NTP packets. TIMESYNC.NLM processes the NTP packet as if it came from another NetWare server running TIMESYNC.NLM and negotiates time with the proprietary TIMESYNC algorithm. To enable this functionality, you must perform the steps in Task 1-2 on the NetWare server that is running TIMESYNC.NLM if you wish to point the server to an NTP time source.

■ **Note** You can configure a server that is a SECONDARY, PRIMARY, or REFERENCE time-sync type to send packets in the NTP format.

Task 1-2. Enabling TIMESYNC

1. Type **monitor** at the NetWare console prompt.
2. Choose Server Parameters ➤ Time.
3. Make sure that the TIMESYNC ➤ Configured Sources is set to On.
4. Modify the TIMESYNC Time Sources by pressing Enter.
5. Add the server address of the NTP server by adding **:123** to the end of the address; for example (don't forget the semicolon at the end of the line):

```
192.68.2.34:123;
```

The server address specified in Task 1-2 may be one of the following:

- An external NTP time source
- A local server running the xntp daemon
- A local server running TIMESYNC.NLM also configured to communicate via NTP

If *all* servers within your time-synchronization environment are configured to communicate via IP and are configured to send time-synchronization packets with the NTP packet structure, it is advised that you disable NCP on TIMESYNC.NLM to reduce redundant traffic. This can be accomplished by performing Task 1-3.

Task 1-3. Disabling NCP on TIMESYNC.NLM

1. Edit the SYS:\SYSTEM\TIMESERV.NCF file.
2. Find the line that reads LOAD TIMESYNC.
3. Add **-T noncp** to the end of the line; for example:

```
LOAD TIMESYNC -T noncp
```

4. Reboot the server. (You can also just unload TIMESYNC.NLM and manually load it with the switch specified in Step 3).

To make time synchronization even more seamless, NetWare 6.5 implemented the open-source NTP daemon. This daemon is identical to the NTP daemon that ships on SLES 8 and 9 as well as on Red Hat 2.1 and 3.0 (identical because it came from the same open-source project, not because the versions are all exactly the same).

It is recommended, whenever possible, to use the NTP daemon on NetWare instead of TIMESYNC.NLM when introducing eDirectory into a mixed-platform environment. This ensures that all platforms use the same synchronization model, thus increasing the probability that all servers stay synchronized. If NTP is used as the time-synchronization method, it will also be easier to administer. Remember that on NetWare 6.5, you must use either TIMESYNC.NLM or the NTP daemon. They cannot run simultaneously.

If the eDirectory servers in the environment are running versions of NetWare other than NetWare 6.5, you still need to use TIMESYNC.NLM on the older NetWare versions. The NTP daemon is supported only on NetWare 6.5. In these scenarios, there are several ways to integrate time-synchronization methods across disparate platforms. Figure 1-1 shows one example of how this could be accomplished.

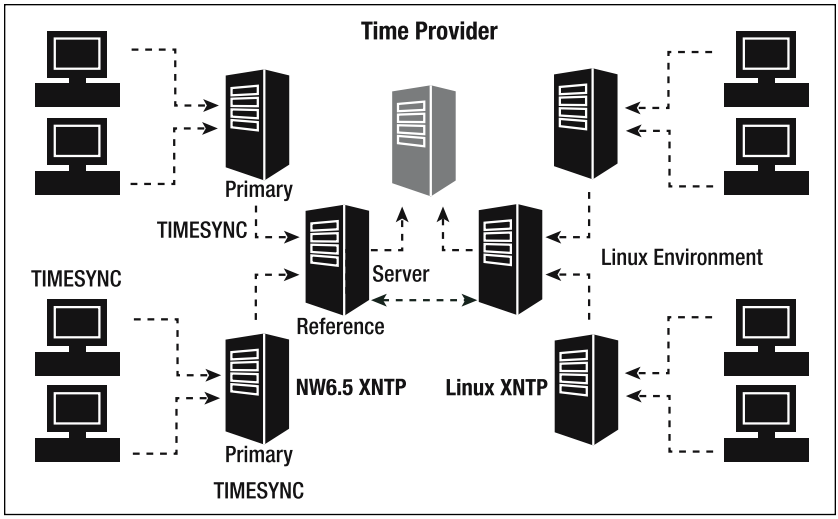

Figure 1-1. *Mixed Timesync environment*

The bottom line is that eDirectory requires all servers within the tree to be synchronized to within a few seconds of each other. It is really up to you to choose the time-synchronization method that makes the most sense for your specific environment.

Troubleshooting Installation Failures

eDirectory environments can be very complex. Adding to that complexity, many eDirectory trees have been around for a long time and carry a lot of baggage or old data that is no longer relevant. Because of these variables, there are many areas that could potentially cause you to fail to install a new server into an existing environment.

The purpose of this section is to discuss some of the most likely scenarios that you may encounter while installing eDirectory. Hopefully, this section will help you to avoid known pitfalls. However, if you run into an issue, this section should be an invaluable tool for you.

The eDirectory installation can be broken down into two basic parts: file copy and configuration.

During the configuration stage, the server is introduced into the eDirectory tree. A local database is created on the local server. All associated services are configured and started. All required objects for the services are also created. These services and objects are as follows:

- Security components
  - Tree key configuration
  - SAS object
  - KMO objects (server certificates)
  - Trusted root certificates
  - A file located in the SYS:\PUBLIC directory (NetWare only)
- LDAP
- SNMP
- HTTPSTK
  - NDS iMonitor
  - eMBox
- Volume objects
  - NetWare volume objects
  - SLES 9 SP1 running OES volume objects (volume objects on SLES 9 are created only if the NCP server or NSS is installed during the OES installation)

Troubleshooting methods for both the binary copy procedure and the configuration procedure during an eDirectory installation will vary from operating system to operating system. Therefore, troubleshooting on each eDirectory-supported operating system is discussed separately in the following sections.

NetWare

NetWare combines the file copy portion and the configuration portion into one process. However, for purposes of explaining what occurs, it is beneficial to break the troubleshooting procedures into two separate processes.

File Copy

All files required for eDirectory are copied to the SYS volume. The file locations are hard coded and cannot be altered. Most of the programs are written to the SYS:\SYSTEM directory. The eDirectory database files are created in the SYS:_NETWARE directory. The installation log files are created in the SYS:\NI\DATA directory.

eDirectory can be installed onto NetWare's legacy file system as well as onto NetWare's NSS file system. The only issue typically encountered with the eDirectory file copy stage is insufficient disk space. Make sure there is sufficient disk space before you start the installation (see `http://www.novell.com/documentation` for more information on the prerequisites).

If you are installing eDirectory 8.7.x on NetWare 5.1 (or Netware 6.0 where the SYS volume is the legacy file system), sometimes, the file copy portion of the installation can be a little bit slow. This can usually be remedied with two file system configuration changes:

- Set the Dirty Disk Cache Delay Time to 0.1 second. This can be set in MONITOR.NLM ➤ Server Parameters ➤ File Caching (the default is 3.3 seconds). This setting allows the file system to be more aggressive about allocating disk cache for data that needs to be written to disk.
- Set Directory Cache Allocation Wait Time to 0.1 second in MONITOR.NLM ➤ Server Parameters ➤ Directory Caching (the default is 2.2 seconds).

Other possible issues that may slow down the file copy process are the following:

- *Compression*: File compression decreases the file copy performance.
- *Antivirus software*: It is recommended that you disable antivirus software if performance during the file copy portion is unacceptable. With most antivirus software programs, each file must be scanned as it is copied to disk.

Configuration

During the configuration phase, a database is created and objects for the server are created. The following is the process of configuring an eDirectory server. References to where to find troubleshooting tips for each step of the process are provided in the next section in case a step does not complete successfully.

- An NCP server object is created in the tree.
- An instance of the DIB is created in the SYS:\NETWARE directory (a hidden directory) on the local file system of the server being installed.
- The schema is extended.
    - The schema necessary to bring the current DIB to the latest version of eDirectory is installed.
    - A reboot must occur.
    - The rest of the schema is installed.
- Any applicable replicas of the tree are synchronized to the local database.
- The SAS object and KMO object are created for the server being installed.

- If this is the first server installed into the tree, the Security container and all components underneath are created.
- The SNMP object is created for the server being installed.
- The NMAS objects are created.
- The LDAP objects are created for the server being installed.

Troubleshooting Tips

There are five basic areas that you can refer to if something goes wrong during the installation or configuration phase of eDirectory on NetWare:

- *NetWare server console*: This screen shows errors.
- *NetWare Logger screen*: Only on NetWare 6.x.
- *SYS:\SYSTEM\NI\DATA*.LOG*: Has information about the file copy as well as the configuration stages.
- *SYS:\SYSTEM\DSMISC.LOG*: Captures information about the schema extension process.
- *SYS:\SYSTEM\DSTRACE.DBG*: See the section "Capturing a DSTRACE Log" at the end of this chapter to get detailed steps.

Disaster Recovery

If an unrecoverable error occurs during installation, perform Task 1-4.

■ **Note** Some of these steps may not apply, depending on where the installation failed.

Task 1-4. Removing eDirectory After a Failed Installation

1. Run **nwconfig –dsremove**. Choose Directory Options ➤ Remove Directory Services from this server to remove the database from the local server.
2. Through iManager or ConsoleOne, delete the NCP server object of the failed server and all associated objects (e.g., LDAP server and group objects, SNMP object, Volume Objects, etc.).
3. At a console prompt of the failed server, type **uinstall edir**. This removes the entry in the products.dat file so that you can reinstall eDirectory.
4. Reinstall eDirectory.

■ **Note** If the first steps of adding the DIB were successful and the failure was with one or all of the components, you can skip removing the DIB and deleting the objects. Simply remove edir from the products.dat file and reinstall eDirectory. The installation will leave the DIB intact and just configure the missing components.

Microsoft Windows

As with NetWare, the eDirectory installation on Microsoft Windows performs the file copy and configuration in one integrated step. However, they are discussed separately here for clarity.

File Copy

All files required for eDirectory are copied to the drive that Windows is installed on (usually C:\). Most of the binaries are copied to \Novell\NDS (e.g., C:\Novell\NDS). The file locations are hard coded and cannot be altered.

The eDirectory database files are created in the \Novell\NDS\DIBFiles directory (e.g., c:\novell\nds\DIBFiles).

The installation log files are created in the %SystemDrive%:\Program Files\Common Files\Novell\ni\data directory. The files are ni.log, nierrors.log, and nioutput.log.

The file copy section is mostly handled by the Microsoft Windows operating system. Use the default Windows operating system logs as well as the NI logs just listed for any file copy errors.

Configuration

During the configuration phase, a DIB is created and objects for the server are created. The following is the process of configuring an eDirectory server. References to where you can find troubleshooting tips for each step of the process are provided in the next section in case a step does not complete successfully.

- An NCP server object is created in the tree.
- An instance of the DIB is created in the %systemrootdrive:\Novell\NDS\DIBFiles directory on the local file system of the server being installed.
- The schema is extended.
    - The schema necessary to bring the current DIB to the latest version of eDirectory is installed.

  - A reboot must occur.
  - The rest of the schema is installed.
- Any applicable replicas of the tree are synchronized to the local database.
- The SAS object and KMO object are created for the server being installed.
- If this is the first server installed into the tree, the Security container and all components underneath are created.
- The SNMP object is created for the server being installed.
- The HTTP server object is created; this is used for NDS iMonitor.
- The NMAS objects are created.
- The LDAP objects are created for the server being installed.

Troubleshooting Tips

The Microsoft event viewer and the %SystemDrive%:\Program Files\Common Files\Novell\ni\data log files are the primary troubleshooting tools for eDirectory installation issues on the Microsoft Windows operating system.

DSTRACE logs can also be evaluated to capture errors. For information on how to capture DSTRACE logs, see the "Capturing a DSTRACE Log" section at the end of the chapter.

Disaster Recovery

If an unrecoverable error occurs during installation, perform Task 1-5.

■ **Note** Some of these steps may not apply, depending on where the installation failed.

Task 1-5. Removing eDirectory on Windows After a Failed Installation

1. Run Add/Remove Programs from Control Panel. Select eDirectory and remove the product.

■ **Note** If Add/Remove Programs fails, stop the dhost service in the Windows services program and then manually delete the files in the following directories: %SystemDrive%:\Novell\NDS and SystemDrive%:\Program Files\Common Files\Novell\ni. Other applications use the latter directory, so if you do delete it, the uninstall procedure through Add/Remove Programs will be broken for those other applications.

---

2. Reinstall eDirectory.
3. Through iManager or ConsoleOne, delete the NCP server object of the failed server and all associated objects (e.g., LDAP server and group objects, SNMP object, Volume Objects, etc.).

*nix

The eDirectory installation on Linux, Solaris, HPUX, and AIX (*.nix) has two completely separate processes. The file copy and configuration are completely separated.

File Copy

To verify that the packages are installed, run the native operating system package database query commands. Most of the packages for eDirectory start with either NDS or NOVL. The following are the commands to query the installed packages:

- Linux
  - rpm –qa | grep NDS*
  - rpm –qa | grep NOVL*
- Solaris
  - pkginfo | grep NDS*
  - pkginfo | grep NOVL*
- AIX
  - lslpp –l | grep NDS*
  - lslpp –l | grep NOVL*
- HPUX
  - swlist –v | grep NDS*
  - swlist –v | grep NOVL*

Configuration

To configure an instance of eDirectory, launch the `ndsconfig` utility. For more information on `ndsconfig`, see the *Novell eDirectory Administration Guide* at `http://www.novell.com/documentation`.

During the configuration phase, a DIB is created and objects for the server are created. The following is the process of configuring an eDirectory server. References to where you can find troubleshooting tips for each step of