Deploying OpenLDAP

Dear Reader,

If you’re a developer, system administrator, or database administrator considering OpenLDAP, then keep reading! I’ll show you the types of decisions you need to make regarding the OpenLDAP environment before downloading any software.

In Deploying OpenLDAP, I discuss how to evaluate your current environment, consolidate data, plan for data creation and migration, and plan the most useful directory infrastructure possible. I then cover the configuration files and the base set of tools. Finally, I discuss APIs and how to integrate OpenLDAP into your current environment.

With this information, you’ll be able to make essential decisions before installing and configuring your OpenLDAP environment. In fact, properly designing and deploying OpenLDAP from the start will give you access to many of the best features of the technology—features that may otherwise be unusable.

I wrote this book to assist you with practical tasks, not the theory of OpenLDAP. By carefully evaluating your needs and implementing my suggestions, you’ll be able to build a directory that will make your network run much more efficiently.

Tom Jackiewicz
Deploying
OpenLDAP

TOM JACKIEWICZ

Apress®
This book is dedicated to all those who suffered while I grew up from a bright and curious kid to the bitter, stubborn, and outspoken person I've become, especially my dad, Zdzislaw Jackiewicz.
## Contents at a Glance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Author</td>
<td>xiii</td>
</tr>
<tr>
<td>About the Technical Reviewers</td>
<td>xv</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xvii</td>
</tr>
<tr>
<td>Preface</td>
<td>xix</td>
</tr>
<tr>
<td>Introduction</td>
<td>xxi</td>
</tr>
<tr>
<td>CHAPTER 1 Assessing Your Environment</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 2 Understanding Data Definitions</td>
<td>23</td>
</tr>
<tr>
<td>CHAPTER 3 Implementing Deployment, Operations, and Administration Strategies</td>
<td>47</td>
</tr>
<tr>
<td>CHAPTER 4 Installing OpenLDAP</td>
<td>65</td>
</tr>
<tr>
<td>CHAPTER 5 Implementing OpenLDAP</td>
<td>93</td>
</tr>
<tr>
<td>CHAPTER 6 Scripting and Programming LDAP</td>
<td>123</td>
</tr>
<tr>
<td>CHAPTER 7 Integrating at the System Level</td>
<td>199</td>
</tr>
<tr>
<td>CHAPTER 8 Integrating OpenLDAP with Applications, User Systems, and Client Tools</td>
<td>263</td>
</tr>
<tr>
<td>INDEX</td>
<td>289</td>
</tr>
</tbody>
</table>
Contents

About the Author ................................................................. xiii
About the Technical Reviewers ............................................... xv
Acknowledgments .............................................................. xvii
Preface .............................................................................. xix
Introduction ........................................................................ xxi

CHAPTER 1  Assessing Your Environment .............................. 1
Gathering Information ....................................................... 1
   Name ........................................................................ 3
   E-mail .................................................................... 4
   Phone ..................................................................... 4
   PKI Information ....................................................... 5
   Badge ..................................................................... 6
   Customer Data ........................................................ 7
Creating an Ongoing Process ............................................... 8
   Changing Application Sources .................................... 8
   Understanding Meta-Directories ................................. 12
Avoiding Mistakes .............................................................. 15
   LDAP As Oracle ....................................................... 15
   LDAP As a Sync Source ............................................ 18
   Shortsighted Deployment .......................................... 20
Summary ........................................................................ 22

CHAPTER 2  Understanding Data Definitions ....................... 23
Defining Your Schema ....................................................... 23
Understanding Schemas .................................................... 26
   ASN Schema Format ............................................... 26
   Object Identifiers (OIDs) .......................................... 27
   Attributes ................................................................ 29
   Object Classes ....................................................... 34
Other Data Definition Information ................................... 35
Understanding Distinguished Names (DNs) ........................................ 38
Schema Checking ........................................................................ 38
Referential Integrity .................................................................... 39
Structuring the Directory Information Tree (DIT) ....................... 39
Regional Deployment of Information ......................................... 40
Functional Deployment of Information ...................................... 40
Organization by Business Function or Group ......................... 40
Introducing the LDAP Data Interchange Format (LDIF) ............. 41
LDAP Operations ...................................................................... 41
Chaining Operations .................................................................. 43
Indexing Data ........................................................................... 44
Summary ..................................................................................... 45

CHAPTER 3 Implementing Deployment, Operations, and
Administration Strategies .......................................................... 47
Separating Your Environments .................................................. 47
Setting Up Classes of Hosts ...................................................... 50
Using Naming Conventions ...................................................... 52
Using the Creative Convention ................................................ 52
Using the Logical Convention .................................................. 55
Reaching a Compromise ............................................................. 57
Following Standard Procedures .............................................. 57
Using the Standard Host Specifications .................................. 57
Using the Standard Host Installation ....................................... 58
Using the Standard Application Installation ............................. 60
Running the Application ............................................................ 60
Starting the Application ............................................................. 60
Stopping the Application ........................................................... 61
Using Command-Line Options ............................................... 61
Implementing Logs ................................................................... 62
Summary ..................................................................................... 63

CHAPTER 4 Installing OpenLDAP ...................................................... 65
Choosing a Distribution ............................................................ 65
Setting Up Your System ............................................................ 66
Choosing a Special User ............................................................ 66
Obtaining the Distribution ........................................................ 66
Performing the Base Installation ............................................. 68
Compiling OpenLDAP ............................................................... 71
# CONTENTS

Creating a Local Database ............................................. 71
Creating an Offline Database ........................................... 73
Using LDAP Search Filters ............................................. 75
Using OpenLDAP Utilities .............................................. 78
  ldapmodify (1) and ldapadd (1) .................................. 79
  ldapsearch (1) ....................................................... 81
  ldapdelete (1) ...................................................... 84
  ldapmodrdn (1) ...................................................... 87
  slapcat (8C) ......................................................... 89
  slapadd (8C) ......................................................... 90
  slapindex (8C) ....................................................... 91
Summary ................................................................. 91

## CHAPTER 5 Implementing OpenLDAP ........................................ 93

How Much RAM Do You Need? ......................................... 93
How Much Disk Space Do You Need? ................................. 94
Considering Security in Your Implementation .................... 96
  Authentication ..................................................... 96
  SASL ................................................................. 97
  X.509 Certificates .................................................. 103
  Transport Layer Security ......................................... 103
  Access Control .................................................... 104
  Kerberos ........................................................... 104
Understanding Replication ............................................. 105
  changelog/Replication Log ....................................... 106
  slurpd ............................................................ 108
  updateref ........................................................ 109
Importing Databases .................................................... 109
  slapcat ............................................................ 110
Testing .................................................................. 111
Understanding Referrals ................................................ 112
  DNS Resource Records for Service Location ..................... 112
  Localized Scope .................................................... 113
Understanding the Installation Structure ......................... 114
  ldap.conf .......................................................... 114
  slapd.conf .......................................................... 116
  slapd.at.conf ....................................................... 121
  slapd.oc.conf ....................................................... 121
Summary ................................................................. 122
CHAPTER 6 Scripting and Programming LDAP

Utilizing Command-Line Tools ........................................... 123
  LDAP Controls .......................................................... 123
  LDAP API ................................................................. 128
  Obtaining the LDAP Perl API ........................................ 138
  Using the LDAP Perl API ............................................. 139
  Mozilla::LDAP::API .................................................... 145
Performing Operations Against Your OpenLDAP Directory .......... 174
Using Java and JNDI ....................................................... 175
OASIS Standards .......................................................... 189
  Directory Services Markup Language (DSML) .................... 189
  Directory Schema ....................................................... 194
  Conformance ............................................................ 197
Summary ................................................................. 198

CHAPTER 7 Integrating at the System Level ......................... 199

Introducing Network Information Services .......................... 199
Introducing Standard NIS Configurations ............................ 200
  Performing Synchronization with LDAP ......................... 202
  Performing Direct Integration .................................... 203
Configuring the LDAP Client (Host) ................................. 238
  Using the ldapclient Utility ...................................... 244
  Configuring NSS ....................................................... 249
  Configuring PAM ..................................................... 250
  Setting Up Security .................................................. 251
Using Sendmail .......................................................... 252
  Enabling the Software .............................................. 253
  Building the Binaries ............................................... 255
  Migrating Information .............................................. 255
  Setting Up LDAP Routing ......................................... 259
Summary ................................................................. 261

CHAPTER 8 Integrating OpenLDAP with Applications, User Systems, and Client Tools .......... 263

Preparing for Integration .............................................. 263
Integrating Apache ...................................................... 264
Integrating Pine ......................................................... 268
Integrating Samba ....................................................... 274
**About the Author**

TOM JACKIEWICZ is currently responsible for global LDAP and e-mail architecture at a Fortune 100 company. Over the past 12 years, he has worked on the e-mail and LDAP capabilities of Palm VII, helped architect many large-scale ISPs servicing millions of active e-mail users, and audited security for a number of Fortune 500 companies.

Tom has held management, engineering, and consulting positions at Applied Materials, Motorola, TAOS, and WinStar GoodNet. Jackiewicz has also published articles on network security and monitoring, IT infrastructure, Solaris, Linux, DNS, LDAP, and LDAP security. He lives in San Francisco's Mission neighborhood, where he relies on public transportation plus a bicycle to transport himself to the office—fashionably late.
About the Technical Reviewers

Born under Vesuvius in southern Italy, MASSIMO NARDONE moved to Finland more than eight years ago, where he now works and lives. He holds a master’s of science degree in computing science from the University of Salerno, Italy, and has more than nine years of work experience in project management and the mobile, security, and Web technology areas for both national and international projects. Massimo has worked as a technical account manager, project manager, software engineer, research engineer, chief security architect, and software specialist for many different software houses and international telecommunication companies. Massimo is also a visiting lecturer and supervisor at the Networking Laboratory of the Helsinki University of Technology (TKK) for the course “Security of Communication Protocols.” As a software engineer, he mainly develops Internet and mobile applications involving different technologies, such as Java/J2EE/WebLogic, ASP/COM+, WAP, SMS, PKI, and WPKI. As a research engineer, he participated in different research projects involving PKI, WPKI, WAP, sim applications, SMS, SIP, SAML, BS7799, TTS, security, NGN, and mobile applications. In his role as chief security architect, he has been researching security standards and methods, as well as developing a security framework model for different companies. He researches, designs, and implements security methodologies for Java (JAAS, JSSE, JCE, and so on), BEA WebLogic, J2EE, LDAP, Apache, Microsoft SQL Server, XML, and so on. He’s an expert on the security standard BS7799 and the protocols PKI and WPKI, where he holds two international patent applications.

ORIS ORLANDO, born in Naples, Italy, in 1971, has been interested in computer science since the ’80s. His first computer was a Computer Intellivision Module that developed programs written in the limited-edition BASIC language. At the end of the ’80s, he began to use 8086 machines. In 1989 he enrolled at the University of Salerno, in Italy, for computer science. During his university career, he developed many applications for small businesses and used the BBS before the Internet became prominent. He graduated in 1997 from the University of Salerno. In December 1997 he began working for Siemens Nixdorf for two years as an analyst/programmer (Java, C, PL/SQL, CGI, HTML) in the Web environment. In 1999 he came to work for Bull H.N. For two years he worked with the technical team; in the third year he became a project leader in the security department, and this year he’s a project manager. He has had significant experience with Unix, Windows, Linux, DOS, computer programming, security, and databases (Oracle and LDAP), and he’s certified for the BS7799 security standard.
I’d like to thank all those who have helped me go from bitterly screaming about LDAP (among other things) to finally writing it down, including Lane Davis, my mentor; Darin Wayrynen, whose late-night sessions inspired me to get into this systems stuff; Strata Rose, of whom I’m still in awe after working with her on SMTP and LDAP environments; Susan Surapruik, my better half, who, with great patience and understanding, has dealt with my opinionated rantings for so many years; and all those who have helped me in the search for the perfect chopped liver sandwich in the Bay.

And thanks to everyone involved in this project who put this together and dealt with any of the pain usually associated with geeks such as me.