# Table of Contents

**Preface**...........................................................................................................................................1

| Copyright.................................................................1 |
| Scope of this Document..............................................1 |
| Acknowledgments........................................................1 |
| Amendments......................................................................2 |
| About this document....................................................3 |

1. **Introduction to OpenLDAP Directory Services**................................................................. 3
   1.1. What is a directory service?....................................................................................................... 3
   1.2. What is LDAP?............................................................................................................................. 6
   1.3. When should I use LDAP?............................................................................................................ 6
   1.4. When should I not use LDAP?................................................................................................... 6
   1.5. How does LDAP work?.............................................................................................................. 7
   1.6. What about X.500?.................................................................................................................... 7
   1.7. What is the difference between LDAPv2 and LDAPv3?........................................................... 7
   1.8. LDAP vs RDBMS...................................................................................................................... 9
   1.9. What is slapd and what can it do?.............................................................................................. 11

2. **A Quick-Start Guide**.................................................................................................................15

3. **The Big Picture - Configuration Choices**.............................................................................15
   3.1. Local Directory Service..............................................................................................................15
   3.2. Local Directory Service with Referrals....................................................................................15
   3.3. Replicated Directory Service.....................................................................................................16
   3.4. Distributed Local Directory Service........................................................................................17

4. **Building and Installing OpenLDAP Software**........................................................................17
   4.1. Obtaining and Extracting the Software.....................................................................................17
   4.2. Prerequisite software.............................................................................................................. 17
       4.2.1. Transport Layer Security...................................................................................................18
       4.2.2. Simple Authentication and Security Layer........................................................................18
       4.2.3. Kerberos Authentication Service.......................................................................................18
       4.2.4. Database Software............................................................................................................18
       4.2.5. Threads..............................................................................................................................19
       4.2.6. TCP Wrappers....................................................................................................................19
   4.3. Running configure....................................................................................................................20
   4.4. Building the Software.............................................................................................................20
   4.5. Testing the Software..............................................................................................................20
   4.6. Installing the Software............................................................................................................21

5. **Configuring slapd**...................................................................................................................21
   5.1. Configuration Layout...............................................................................................................23
   5.2. Configuration Directives.........................................................................................................23
       5.2.1. cn=config........................................................................................................................25
       5.2.2. cn=module........................................................................................................................25
       5.2.3. cn=schema.......................................................................................................................26
# Table of Contents

5. Configuring slapd
   5.2.4. Backend-specific Directives ................................................................. 27
   5.2.5. Database-specific Directives ................................................................. 31
   5.2.6. BDB and HDB Database Directives ....................................................... 35
5.3. Access Control ......................................................................................... 36
   5.3.1. What to control access to ................................................................. 37
   5.3.2. Who to grant access to ................................................................. 38
   5.3.3. The access to grant ......................................................................... 38
   5.3.4. Access Control Evaluation ............................................................... 38
   5.3.5. Access Control Examples ............................................................... 40
   5.3.6. Access Control Ordering ............................................................... 41
5.4. Configuration Example ......................................................................... 43
5.5. Converting from slapd.conf(8) to a cn=config directory format .......... 45

6. The slapd Configuration File ...................................................................... 45
   6.1. Configuration File Format ...................................................................... 46
   6.2. Configuration File Directives ............................................................... 46
       6.2.1. Global Directives ......................................................................... 48
       6.2.2. General Backend Directives ......................................................... 48
       6.2.3. General Database Directives ......................................................... 52
       6.2.4. BDB and HDB Database Directives ............................................ 52
   6.3. The access Configuration Directive .................................................. 53
       6.3.1. What to control access to .......................................................... 54
       6.3.2. Who to grant access to .................................................................. 55
       6.3.3. The access to grant ..................................................................... 55
       6.3.4. Access Control Evaluation ......................................................... 55
       6.3.5. Access Control Examples .......................................................... 57
   6.4. Configuration File Example ................................................................... 59

7. Running slapd ......................................................................................... 59
   7.1. Command-Line Options ....................................................................... 60
   7.2. Starting slapd ...................................................................................... 60
   7.3. Stopping slapd .................................................................................... 63

8. Database Creation and Maintenance Tools ............................................ 63
   8.1. Creating a database over LDAP ......................................................... 64
   8.2. Creating a database off-line ............................................................... 65
       8.2.1. The slapadd program ............................................................... 66
       8.2.2. The slapindex program ............................................................ 66
       8.2.3. The slapcat program ............................................................... 66
   8.3. The LDIF text entry format .............................................................. 69

9. Backends .............................................................................................. 69
   9.1. Berkeley DB Backends ................................................................. 69
       9.1.1. Overview .................................................................................. 69
       9.1.2. back-bdb/back-hdb Configuration ........................................... 69
       9.1.3. Further Information ............................................................... 69
   9.2. LDAP ............................................................................................... 69
# Table of Contents

## 9. Backends
- 9.2.1. Overview.........................................................................................................................69
- 9.2.2. back-ldap Configuration..................................................................................................70
- 9.2.3. Further Information........................................................................................................70
- 9.3. LDIF.......................................................................................................................................70
  - 9.3.1. Overview.........................................................................................................................70
  - 9.3.2. back-ldif Configuration................................................................................................70
  - 9.3.3. Further Information........................................................................................................70
- 9.4. Metadirectory.......................................................................................................................70
  - 9.4.1. Overview.......................................................................................................................70
  - 9.4.2. back-meta Configuration.............................................................................................70
  - 9.4.3. Further Information........................................................................................................71
- 9.5. Monitor..................................................................................................................................71
  - 9.5.1. Overview.......................................................................................................................71
  - 9.5.2. back-monitor Configuration.......................................................................................71
  - 9.5.3. Further Information........................................................................................................71
- 9.6. Null.......................................................................................................................................71
  - 9.6.1. Overview.......................................................................................................................71
  - 9.6.2. back-null Configuration..............................................................................................71
  - 9.6.3. Further Information........................................................................................................71
- 9.7. Passwd...................................................................................................................................72
  - 9.7.1. Overview.......................................................................................................................72
  - 9.7.2. back-passwd Configuration.......................................................................................72
  - 9.7.3. Further Information........................................................................................................72
- 9.8. Perl/Shell.............................................................................................................................72
  - 9.8.1. Overview.......................................................................................................................72
  - 9.8.2. back-perl/back-shell Configuration............................................................................72
  - 9.8.3. Further Information........................................................................................................72
- 9.9. Relay.....................................................................................................................................72
  - 9.9.1. Overview.......................................................................................................................73
  - 9.9.2. back-relay Configuration............................................................................................73
  - 9.9.3. Further Information........................................................................................................73
- 9.10. SQL.......................................................................................................................................73
  - 9.10.1. Overview.....................................................................................................................73
  - 9.10.2. back-sql Configuration.............................................................................................73
  - 9.10.3. Further Information........................................................................................................75

## 10. Overlays...............................................................................................................................75
- 10.1. Access Logging................................................................................................................75
  - 10.1.1. Overview....................................................................................................................76
  - 10.1.2. Access Logging Configuration....................................................................................76
- 10.2. Audit Logging...................................................................................................................76
  - 10.2.1. Overview....................................................................................................................76
  - 10.2.2. Audit Logging Configuration.......................................................................................76
- 10.3. Chaining.............................................................................................................................76
  - 10.3.1. Overview....................................................................................................................76
  - 10.3.2. Chaining Configuration.............................................................................................77
  - 10.3.3. Handling Chaining Errors.........................................................................................77
Table of Contents

10. Overlays
   10.4. Constraints............................................................................................................................77
       10.4.1. Overview............................................................................................................................77
       10.4.2. Constraint Configuration................................................................................................77
   10.5. Dynamic Directory Services..................................................................................................77
       10.5.1. Overview............................................................................................................................78
       10.5.2. Dynamic Directory Service Configuration.......................................................................78
   10.6. Dynamic Groups......................................................................................................................78
       10.6.1. Overview............................................................................................................................78
       10.6.2. Dynamic Group Configuration.........................................................................................78
   10.7. Dynamic Lists..........................................................................................................................78
       10.7.1. Overview............................................................................................................................78
       10.7.2. Dynamic List Configuration..............................................................................................78
   10.8. Reverse Group Membership Maintenance...........................................................................78
       10.8.1. Overview............................................................................................................................78
       10.8.2. Member Of Configuration.................................................................................................79
   10.9. The Proxy Cache Engine.........................................................................................................79
       10.9.1. Overview............................................................................................................................80
       10.9.2. Proxy Cache Configuration...............................................................................................81
   10.10. Password Policies..................................................................................................................82
        10.10.1. Overview..........................................................................................................................82
        10.10.2. Password Policy Configuration......................................................................................82
   10.11. Referential Integrity................................................................................................................82
        10.11.1. Overview..........................................................................................................................82
        10.11.2. Referential Integrity Configuration................................................................................82
   10.12. Return Code...........................................................................................................................82
        10.12.1. Overview..........................................................................................................................82
        10.12.2. Return Code Configuration..............................................................................................82
   10.13. Rewrite/Remap.......................................................................................................................82
        10.13.1. Overview..........................................................................................................................82
        10.13.2. Rewrite/Remap Configuration.........................................................................................82
   10.14. Sync Provider........................................................................................................................82
        10.14.1. Overview..........................................................................................................................82
        10.14.2. Sync Provider Configuration.........................................................................................82
   10.15. Translucent Proxy................................................................................................................83
        10.15.1. Overview..........................................................................................................................83
        10.15.2. Translucent Proxy Configuration....................................................................................83
   10.16. Attribute Uniqueness..............................................................................................................83
        10.16.1. Overview..........................................................................................................................83
        10.16.2. Attribute Uniqueness Configuration.................................................................................83
   10.17. Value Sorting........................................................................................................................83
        10.17.1. Overview..........................................................................................................................83
        10.17.2. Value Sorting Configuration............................................................................................83
   10.18. Overlay Stacking......................................................................................................................83
        10.18.1. Overview..........................................................................................................................83
        10.18.2. Example Scenarios...........................................................................................................85
# Table of Contents

11. **Schema Specification** ..................................................................................................................85
   11.1. Distributed Schema Files ...........................................................................................................85
   11.2. Extending Schema .......................................................................................................................86
      11.2.1. Object Identifiers ..................................................................................................................87
      11.2.2. Naming Elements ..................................................................................................................87
      11.2.3. Local schema file ..................................................................................................................87
      11.2.4. Attribute Type Specification ...............................................................................................90
      11.2.5. Object Class Specification ..................................................................................................91
      11.2.6. OID Macros ..........................................................................................................................93

12. **Security Considerations** ................................................................................................................93
   12.1. Network Security ........................................................................................................................93
      12.1.1. Selective Listening ...............................................................................................................93
      12.1.2. IP Firewall ..........................................................................................................................93
      12.1.3. TCP Wrappers ......................................................................................................................94
   12.2. Data Integrity and Confidentiality Protection ................................................................................94
      12.2.1. Security Strength Factors ....................................................................................................94
   12.3. Authentication Methods .............................................................................................................94
      12.3.1. "simple" method ...................................................................................................................95
      12.3.2. SASL method .......................................................................................................................97

13. **Using SASL** .................................................................................................................................97
   13.1. SASL Security Considerations ....................................................................................................98
   13.2. SASL Authentication ...................................................................................................................98
      13.2.1. GSS-API ..............................................................................................................................99
      13.2.2. KERBEROS_V4 ....................................................................................................................100
      13.2.3. DIGEST-MD5 ......................................................................................................................101
      13.2.4. Mapping Authentication Identities ....................................................................................102
      13.2.5. Direct Mapping ....................................................................................................................102
      13.2.6. Search-based mappings .......................................................................................................104
   13.3. SASL Proxy Authorization ..........................................................................................................104
      13.3.1. Uses of Proxy Authorization ..............................................................................................105
      13.3.2. SASL Authorization Identities ............................................................................................105
      13.3.3. Proxy Authorization Rules .................................................................................................109

14. **Using TLS** .....................................................................................................................................109
   14.1. TLS Certificates ........................................................................................................................109
      14.1.1. Server Certificates ..............................................................................................................109
      14.1.2. Client Certificates ..............................................................................................................109
   14.2. TLS Configuration .....................................................................................................................109
      14.2.1. Server Configuration ..........................................................................................................111
      14.2.2. Client Configuration ..........................................................................................................113

15. **Constructing a Distributed Directory Service** ...........................................................................113
   15.1. Subordinate Knowledge Information .........................................................................................113
   15.2. Superior Knowledge Information .............................................................................................114
   15.3. The ManageDsaIT Control ........................................................................................................115
# Table of Contents

16. Replication .................................................................................................................................................115
   16.1. Replication Strategies............................................................................................................................115
       16.1.1. Push Based..................................................................................................................................117
       16.1.2. Pull Based..................................................................................................................................117
   16.2. Replication Types....................................................................................................................................117
       16.2.1. syncrepl replication....................................................................................................................117
       16.2.2. delta-syncrepl replication............................................................................................................117
       16.2.3. N-Way Multi-Master....................................................................................................................117
       16.2.4. MirrorMode................................................................................................................................117
   16.3. LDAP Sync Replication..........................................................................................................................118
       16.3.1. The LDAP Content Synchronization Protocol.................................................................................119
       16.3.2. Syncrepl Details............................................................................................................................121
       16.3.3. Configuring Syncrepl....................................................................................................................123
   16.4. N-Way Multi-Master...............................................................................................................................123
   16.5. MirrorMode...........................................................................................................................................123
       16.5.1. Arguments for MirrorMode..........................................................................................................123
       16.5.2. Arguments against MirrorMode....................................................................................................123
       16.5.3. MirrorMode Configuration...........................................................................................................125
       16.5.4. MirrorMode Summary....................................................................................................................127

17. Maintenance................................................................................................................................................127
   17.1. Directory Backups..................................................................................................................................127
   17.2. Berkeley DB Logs..................................................................................................................................128
   17.3. Checkpointing.......................................................................................................................................129
   17.4. Migration...............................................................................................................................................131

18. Monitoring................................................................................................................................................131
   18.1. Monitor configuration via cn=config(5)...............................................................................................131
   18.2. Monitor configuration via slapd.conf(5)..............................................................................................132
   18.3. Accessing Monitoring Information.....................................................................................................133
   18.4. Monitor Information...............................................................................................................................134
       18.4.1. Backends.....................................................................................................................................135
       18.4.2. Connections................................................................................................................................135
       18.4.3. Databases...................................................................................................................................136
       18.4.4. Listener.......................................................................................................................................136
       18.4.5. Log..............................................................................................................................................136
       18.4.6. Operations...................................................................................................................................137
       18.4.7. Overlays.....................................................................................................................................137
       18.4.8. SASL..........................................................................................................................................137
       18.4.9. Statistics....................................................................................................................................137
       18.4.10. Threads..................................................................................................................................138
       18.4.11. Time.........................................................................................................................................138
       18.4.12. TLS..........................................................................................................................................138
       18.4.13. Waiters....................................................................................................................................139

19. Tuning..........................................................................................................................................................139
   19.1. Performance Factors............................................................................................................................139
       19.1.1. Memory......................................................................................................................................139
Table of Contents

19. Tuning
   19.1. Disks........................................................................................................................................139
   19.1.3. Network Topology.................................................................139
   19.1.4. Directory Layout Design.................................................................139
   19.1.5. Expected Usage.............................................................................139
19.2. Indexes............................................................................................................................139
   19.2.1. Understanding how a search works.........................................................140
   19.2.2. What to index..............................................................................140
   19.2.3. Presence indexing........................................................................140
19.3. Logging................................................................................................................................140
   19.3.1. What log level to use.......................................................................141
   19.3.2. What to watch out for........................................................................141
   19.3.3. Improving throughput........................................................................141
19.4. BDB/HDB Database Caching.........................................................................................141
   19.4.1. Berkeley DB Cache..........................................................................143
   19.4.2. slapd(8) Entry Cache.................................................................144
   19.4.3. IDL Cache......................................................................................145

20. Troubleshooting.........................................................................................................................145
   20.1. User or Software errors?..........................................................................145
   20.2. Checklist........................................................................................................145
   20.3. OpenLDAP Bugs..................................................................................146
   20.4. 3rd party software errors.........................................................................146
   20.5. How to contact the OpenLDAP Project..................................................146
   20.6. How to present your problem.................................................................146
   20.7. Debugging slapd(8)................................................................................146
   20.8. Commercial Support...........................................................................147

A. Changes Since Previous Release.........................................................................................147
   A.1. New Guide Sections..............................................................................147
   A.2. New Features and Enhancements in 2.4..............................................147
      A.2.1. Better cn=config functionality.............................................................148
      A.2.2. Better cn= schema functionality..........................................................148
      A.2.3. More sophisticated Syncrepl configurations......................................148
      A.2.4. N-Way Multimaster Replication..........................................................148
      A.2.5. Replicating slapd Configuration (syncrepl and cn=config)...............148
      A.2.6. Push-Mode Replication........................................................................149
      A.2.7. More extensive TLS configuration control......................................149
      A.2.8. Performance enhancements...............................................................149
      A.2.9. New overlays....................................................................................149
      A.2.10. New features in existing Overlays....................................................150
      A.2.11. New features in slapd.................................................................150
      A.2.12. New features in libldap.................................................................150
      A.2.13. New clients, tools and tool enhancements......................................150
      A.2.14. New build options.........................................................................150
   A.3. Obsolete Features Removed From 2.4.........................................................150
      A.3.1. Slurpd.........................................................................................150
      A.3.2. back-ldbm....................................................................................151
B. Upgrading from 2.3.x .................................................................................................................................151
  B.1. Monitor Backend .................................................................................................................................151
  B.2. cn=config olc* attributes ................................................................................................................153

C. Common errors encountered when using OpenLDAP Software ..............................................................153
  C.1. Common causes of LDAP errors .........................................................................................................153
    C.1.1. ldap_*: Can't contact LDAP server ............................................................................................153
    C.1.2. ldap_*: No such object ..............................................................................................................154
    C.1.3. ldap_*: Can't chase referral .......................................................................................................154
    C.1.4. ldap_*: server is unwilling to perform .....................................................................................155
    C.1.5. ldap_*: Insufficient access ........................................................................................................155
    C.1.6. ldap_*: Invalid DN syntax ..........................................................................................................155
    C.1.7. ldap_*: Referral hop limit exceeded ............................................................................................155
    C.1.8. ldap_*: operations error ...........................................................................................................155
    C.1.9. ldap_*: other error .......................................................................................................................155
    C.1.10. ldap_add/modify: Invalid syntax ..............................................................................................156
    C.1.11. ldap_add/modify: Object class violation ..................................................................................157
    C.1.12. ldap_add: No such object ........................................................................................................157
    C.1.13. ldap_add: invalid structural object class chain .......................................................................158
    C.1.14. ldap_add: no structuralObjectClass operational attribute ....................................................158
    C.1.15. ldap_add/modify/modify: Naming violation ............................................................................159
    C.1.16. ldap_add/delete/modify/modify/modify: no global superior knowledge ...............................159
    C.1.17. ldap_bind: Insufficient access ................................................................................................159
    C.1.18. ldap_bind: Invalid credentials ................................................................................................160
    C.1.19. ldap_bind: Protocol error .........................................................................................................160
    C.1.20. ldap_modify: cannot modify object class ................................................................................160
    C.1.21. ldap_sasl_interactive_bind_s: ...............................................................................................160
    C.1.22. ldap_sasl_interactive_bind_s: No such Object .......................................................................160
    C.1.23. ldap_sasl_interactive_bind_s: No such attribute ....................................................................161
    C.1.24. ldap_sasl_interactive_bind_s: Unknown authentication method .............................................161
    C.1.25. ldap_sasl_interactive_bind_s: Local error (82) .....................................................................161
    C.1.26. ldap_search: Partial results and referral received .....................................................................161
    C.1.27. ldap_start_tls: Operations error ...............................................................................................161
  C.2. Other Errors ........................................................................................................................................161
    C.2.1. ber_get_next on fd X failed erro=34 (Numerical result out of range) .......................................161
    C.2.2. ber_get_next on fd X failed erro=11 (Resource temporarily unavailable) ................................162
    C.2.3. daemon: socket() failed erro=97 (Address family not supported) ............................................162
    C.2.4. GSSAPI: gss_acquire_cred: Miscellaneous failure; Permission denied; ..............................162
    C.2.5. access from unknown denied .....................................................................................................163
    C.2.6. ldap_read: want=# error=Resource temporarily unavailable ................................................163
    C.2.7. `make test' fails .........................................................................................................................164
    C.2.8. ldap_*: Internal (implementation specific) error (80) - additional info: entry index delete failed .........................................................................................................................164
    C.2.9. ldap_sasl_interactive_bind_s: Can't contact LDAP server (-1) .............................................165

D. Recommended OpenLDAP Software Dependency Versions ..........................................................................165
  D.1. Dependency Versions ........................................................................................................................167
## Table of Contents

E. Real World OpenLDAP Deployments and Examples.................................................................169

F. OpenLDAP Software Contributions...........................................................................................169
   F.1. Client APIs..............................................................................................................................169
      F.1.1. ldapc++...........................................................................................................................169
      F.1.2. ldaptcl.............................................................................................................................169
   F.2. Overlays.................................................................................................................................169
      F.2.1. acl....................................................................................................................................169
      F.2.2. addpartial.........................................................................................................................169
      F.2.3. allop................................................................................................................................169
      F.2.4. comp_match......................................................................................................................169
      F.2.5. denyop..............................................................................................................................169
      F.2.6. dsaSchema.........................................................................................................................169
      F.2.7. lastmod............................................................................................................................169
      F.2.8. passwd............................................................................................................................169
      F.2.9. proxyOld...........................................................................................................................169
      F.2.10. smb5pwd.........................................................................................................................169
      F.2.11. trace...............................................................................................................................169
   F.3. Tools........................................................................................................................................170
      F.3.1. Statistic Logging..............................................................................................................170
   F.4. SLAPI Plugins.........................................................................................................................170
      F.4.1. addrdnvalues.....................................................................................................................171

G. Configuration File Examples.....................................................................................................171
   G.1. slapd.conf.............................................................................................................................171
   G.2. ldap.conf.............................................................................................................................171
   G.3. a-n-other.conf......................................................................................................................173

H. LDAP Result Codes.....................................................................................................................173
   H.1. Non-Error Result Codes.........................................................................................................173
   H.2. Result Codes..........................................................................................................................173
   H.3. success (0).............................................................................................................................173
   H.4. operationsError (1)...............................................................................................................173
   H.5. protocolError (2)..................................................................................................................174
   H.6. timeLimitExceeded (3)..........................................................................................................174
   H.7. sizeLimitExceeded (4)............................................................................................................174
   H.8. compareFalse (5)..................................................................................................................174
   H.9. compareTrue (6).....................................................................................................................174
   H.10. authMethodNotSupported (7)............................................................................................174
   H.11. strongerAuthRequired (8)................................................................................................174
   H.12. referral (10).........................................................................................................................174
   H.13. adminLimitExceeded (11)..................................................................................................174
   H.14. unavailableCriticalExtension (12).....................................................................................175
   H.15. confidentialityRequired (13)............................................................................................175
   H.16. saslBindInProgress (14)....................................................................................................175
   H.17. noSuchAttribute (16)..........................................................................................................175
   H.18. undefinedAttributeType (17)............................................................................................175
   H.19. inappropriateMatching (18)..............................................................................................175
Table of Contents

H. LDAP Result Codes
  H.20. constraintViolation (19).............................................................................................................175
  H.21. attributeOrValueExists (20). ........................................................................................................175
  H.22. invalidAttributeSyntax (21). .......................................................................................................175
  H.23. noSuchObject (32). .....................................................................................................................175
  H.24. aliasProblem (33). .......................................................................................................................176
  H.25. invalidDNSyntax (34). ................................................................................................................176
  H.26. aliasDereferencingProblem (36). ..............................................................................................176
  H.27. inappropriateAuthentication (48). ............................................................................................176
  H.28. invalidCredentials (49). ...............................................................................................................176
  H.29. insufficientAccessRights (50). ....................................................................................................176
  H.30. busy (51). ....................................................................................................................................176
  H.31. unavailable (52). ..........................................................................................................................176
  H.32. unwillingToPerform (53). ...........................................................................................................176
  H.33. loopDetect (54). ..........................................................................................................................177
  H.34. namingViolation (64). .................................................................................................................177
  H.35. objectClassViolation (65). ..........................................................................................................177
  H.36. notAllowedOnNonLeaf (66). ......................................................................................................177
  H.37. notAllowedOnRDN (67). ..............................................................................................................177
  H.38. entryAlreadyExists (68). ............................................................................................................177
  H.39. objectClassModsProhibited (69). ............................................................................................177
  H.40. affectsMultipleDSAs (71). ..........................................................................................................177
  H.41. other (80)....................................................................................................................................179

I. Glossary........................................................................................................................................................179
  I.1. Terms.............................................................................................................................................182
  I.2. Related Organizations....................................................................................................................183
  I.3. Related Products............................................................................................................................183
  I.4. References.....................................................................................................................................187

J. Generic configure Instructions..................................................................................................................191

K. OpenLDAP Software Copyright Notices.................................................................................................191
  K.1. OpenLDAP Copyright Notice......................................................................................................191
  K.2. Additional Copyright Notice........................................................................................................192
  K.3. University of Michigan Copyright Notice...................................................................................193

L. OpenLDAP Public License.......................................................................................................................title
Preface

Copyright

Copyright 1998-2007, The OpenLDAP Foundation, All Rights Reserved.

Copyright 1992-1996, Regents of the University of Michigan, All Rights Reserved.

This document is considered a part of OpenLDAP Software. This document is subject to terms of conditions set forth in OpenLDAP Software Copyright Notices and the OpenLDAP Public License. Complete copies of the notices and associated license can be found in Appendix K and L, respectively.

Scope of this Document

This document provides a guide for installing OpenLDAP Software 2.4 (http://www.openldap.org/software/) on UNIX (and UNIX-like) systems. The document is aimed at experienced system administrators with basic understanding of LDAP-based directory services.

This document is meant to be used in conjunction with other OpenLDAP information resources provided with the software package and on the project's site (http://www.OpenLDAP.org/) on the World Wide Web. The site makes available a number of resources.

OpenLDAP Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue Tracking System</td>
<td><a href="http://www.OpenLDAP.org/its/">http://www.OpenLDAP.org/its/</a></td>
</tr>
<tr>
<td>Mailing Lists</td>
<td><a href="http://www.OpenLDAP.org/lists/">http://www.OpenLDAP.org/lists/</a></td>
</tr>
<tr>
<td>Software Pages</td>
<td><a href="http://www.OpenLDAP.org/software/">http://www.OpenLDAP.org/software/</a></td>
</tr>
<tr>
<td>Support Pages</td>
<td><a href="http://www.OpenLDAP.org/support/">http://www.OpenLDAP.org/support/</a></td>
</tr>
</tbody>
</table>

Acknowledgments

The OpenLDAP Project is comprised of a team of volunteers. This document would not be possible without their contribution of time and energy.

The OpenLDAP Project would also like to thank the University of Michigan LDAP Team for building the foundation of LDAP software and information to which OpenLDAP Software is built upon. This document is based upon University of Michigan document: The SLAPD and SLURPD Administrators Guide.

Amendments

Suggested enhancements and corrections to this document should be submitted using the OpenLDAP Issue Tracking System (http://www.openldap.org/its/).
About this document

This document was produced using the Simple Document Format (SDF) documentation system (http://search.cpan.org/src/IANC/sdf-2.001/doc/catalog.html) developed by Ian Clatworthy. Tools for SDF are available from CPAN (http://search.cpan.org/search?query=SDF&mode=dist).
1. Introduction to OpenLDAP Directory Services

This document describes how to build, configure, and operate OpenLDAP Software to provide directory services. This includes details on how to configure and run the Standalone LDAP Daemon, \texttt{slapd(8)}. It is intended for new and experienced administrators alike. This section provides a basic introduction to directory services and, in particular, the directory services provided by \texttt{slapd(8)}. This introduction is only intended to provide enough information so one might get started learning about LDAP, X.500, and directory services.

1.1. What is a directory service?

A directory is a specialized database specifically designed for searching and browsing, in additional to supporting basic lookup and update functions.

\textbf{Note:} A directory is defined by some as merely a database optimized for read access. This definition, at best, is overly simplistic.

Directories tend to contain descriptive, attribute-based information and support sophisticated filtering capabilities. Directories generally do not support complicated transaction or roll-back schemes found in database management systems designed for handling high-volume complex updates. Directory updates are typically simple all-or-nothing changes, if they are allowed at all. Directories are generally tuned to give quick response to high-volume lookup or search operations. They may have the ability to replicate information widely in order to increase availability and reliability, while reducing response time. When directory information is replicated, temporary inconsistencies between the replicas may be okay, as long as inconsistencies are resolved in a timely manner.

There are many different ways to provide a directory service. Different methods allow different kinds of information to be stored in the directory, place different requirements on how that information can be referenced, queried and updated, how it is protected from unauthorized access, etc. Some directory services are \textit{local}, providing service to a restricted context (e.g., the finger service on a single machine). Other services are global, providing service to a much broader context (e.g., the entire Internet). Global services are usually \textit{distributed}, meaning that the data they contain is spread across many machines, all of which cooperate to provide the directory service. Typically a global service defines a uniform \textit{namespace} which gives the same view of the data no matter where you are in relation to the data itself.

A web directory, such as provided by the \textit{Open Directory Project} \langle\texttt{http://dmoz.org}\rangle, is a good example of a directory service. These services catalog web pages and are specifically designed to support browsing and searching.

While some consider the Internet Domain Name System (DNS) is an example of a globally distributed directory service, DNS is not browseable nor searchable. It is more properly described as a globally distributed \textit{lookup} service.

1.2. What is LDAP?

LDAP stands for Lightweight Directory Access Protocol. As the name suggests, it is a lightweight protocol for accessing directory services, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection oriented transfer services. LDAP is an IETF Standard Track protocol and is specified in "Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map" RFC4510.
This section gives an overview of LDAP from a user's perspective.

What kind of information can be stored in the directory? The LDAP information model is based on entries. An entry is a collection of attributes that has a globally-unique Distinguished Name (DN). The DN is used to refer to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like "cn" for common name, or "mail" for email address. The syntax of values depend on the attribute type. For example, a cn attribute might contain the value Babs Jensen. A mail attribute might contain the value "babs@example.com". A jpegPhoto attribute would contain a photograph in the JPEG (binary) format.

How is the information arranged? In LDAP, directory entries are arranged in a hierarchical tree-like structure. Traditionally, this structure reflected the geographic and/or organizational boundaries. Entries representing countries appear at the top of the tree. Below them are entries representing states and national organizations. Below them might be entries representing organizational units, people, printers, documents, or just about anything else you can think of. Figure 1.1 shows an example LDAP directory tree using traditional naming.

![LDAP directory tree (traditional naming)](image)

Figure 1.1: LDAP directory tree (traditional naming)

The tree may also be arranged based upon Internet domain names. This naming approach is becoming increasing popular as it allows for directory services to be located using the DNS. Figure 1.2 shows an example LDAP directory tree using domain-based naming.
In addition, LDAP allows you to control which attributes are required and allowed in an entry through the use of a special attribute called `objectClass`. The values of the `objectClass` attribute determine the schema rules the entry must obey.

**How is the information referenced?** An entry is referenced by its distinguished name, which is constructed by taking the name of the entry itself (called the Relative Distinguished Name or RDN) and concatenating the names of its ancestor entries. For example, the entry for Barbara Jensen in the Internet naming example above has an RDN of `uid=babs` and a DN of `uid=babs,ou=People,dc=example,dc=com`. The full DN format is described in RFC4514, "LDAP: String Representation of Distinguished Names."

**How is the information accessed?** LDAP defines operations for interrogating and updating the directory. Operations are provided for adding and deleting an entry from the directory, changing an existing entry, and changing the name of an entry. Most of the time, though, LDAP is used to search for information in the directory. The LDAP search operation allows some portion of the directory to be searched for entries that match some criteria specified by a search filter. Information can be requested from each entry that matches the criteria.

For example, you might want to search the entire directory subtree at and below `dc=example,dc=com` for people with the name Barbara Jensen, retrieving the email address of each entry found. LDAP lets you do this easily. Or you might want to search the entries directly below the `st=California,c=US` entry for organizations with the string `Acme` in their name, and that have a fax number. LDAP lets you do this too. The next section describes in more detail what you can do with LDAP and how it might be useful to you.

**How is the information protected from unauthorized access?** Some directory services provide no protection, allowing anyone to see the information. LDAP provides a mechanism for a client to authenticate, or prove its identity to a directory server, paving the way for rich access control to protect the information the server contains. LDAP also supports data security (integrity and confidentiality) services.
1.3. When should I use LDAP?

This is a very good question. In general, you should use a Directory server when you require data to be centrally managed, stored and accessible via standards based methods.

Some common examples found throughout the industry are, but not limited to:

- Machine Authentication
- User Authentication
- User/System Groups
- Address book
- Organization Representation
- Asset Tracking
- Telephony Information Store
- User resource management
- E-mail address lookups
- Application Configuration store
- PBX Configuration store
- etc....

There are various Distributed Schema Files that are standards based, but you can always create your own Schema Specification.

There are always new ways to use a Directory and apply LDAP principles to address certain problems, therefore there is no simple answer to this question.

If in doubt, join the general LDAP forum for non-commercial discussions and information relating to LDAP at: http://www.umich.edu/~dirsvcs/ldap/mailinglist.html and ask

1.4. When should I not use LDAP?

When you start finding yourself bending the directory to do what you require, maybe a redesign is needed. Or if you only require one application to use and manipulate your data (for discussion of LDAP vs RDBMS, please read the LDAP vs RDBMS section).

It will become obvious when LDAP is the right tool for the job.

1.5. How does LDAP work?

LDAP utilizes a client-server model. One or more LDAP servers contain the data making up the directory information tree (DIT). The client connects to servers and asks it a question. The server responds with an answer and/or with a pointer to where the client can get additional information (typically, another LDAP server). No matter which LDAP server a client connects to, it sees the same view of the directory; a name presented to one LDAP server references the same entry it would at another LDAP server. This is an important feature of a global directory service.
1.6. What about X.500?

Technically, LDAP is a directory access protocol to an X.500 directory service, the OSI directory service. Initially, LDAP clients accessed gateways to the X.500 directory service. This gateway ran LDAP between the client and gateway and X.500's Directory Access Protocol (DAP) between the gateway and the X.500 server. DAP is a heavyweight protocol that operates over a full OSI protocol stack and requires a significant amount of computing resources. LDAP is designed to operate over TCP/IP and provides most of the functionality of DAP at a much lower cost.

While LDAP is still used to access X.500 directory service via gateways, LDAP is now more commonly directly implemented in X.500 servers.

The Standalone LDAP Daemon, or slapd(8), can be viewed as a lightweight X.500 directory server. That is, it does not implement the X.500's DAP nor does it support the complete X.500 models.

If you are already running a X.500 DAP service and you want to continue to do so, you can probably stop reading this guide. This guide is all about running LDAP via slapd(8), without running X.500 DAP. If you are not running X.500 DAP, want to stop running X.500 DAP, or have no immediate plans to run X.500 DAP, read on.

It is possible to replicate data from an LDAP directory server to a X.500 DAP DSA. This requires an LDAP/DAP gateway. OpenLDAP Software does not include such a gateway.

1.7. What is the difference between LDAPv2 and LDAPv3?

LDAPv3 was developed in the late 1990's to replace LDAPv2. LDAPv3 adds the following features to LDAP:

- Strong authentication and data security services via SASL
- Certificate authentication and data security services via TLS (SSL)
- Internationalization through the use of Unicode
- Referrals and Continuations
- Schema Discovery
- Extensibility (controls, extended operations, and more)

LDAPv2 is historic (RFC3494). As most so-called LDAPv2 implementations (including slapd(8)) do not conform to the LDAPv2 technical specification, interoperability amongst implementations claiming LDAPv2 support is limited. As LDAPv2 differs significantly from LDAPv3, deploying both LDAPv2 and LDAPv3 simultaneously is quite problematic. LDAPv2 should be avoided. LDAPv2 is disabled by default.

1.8. LDAP vs RDBMS

This question is raised many times, in different forms. The most common, however, is: Why doesn't OpenLDAP drop Berkeley DB and use a relational database management system (RDBMS) instead? In general, expecting that the sophisticated algorithms implemented by commercial-grade RDBMS would make OpenLDAP be faster or somehow better and, at the same time, permitting sharing of data with other applications.

The short answer is that use of an embedded database and custom indexing system allows OpenLDAP to provide greater performance and scalability without loss of reliability. OpenLDAP uses Berkeley DB
concurrent / transactional database software. This is the same software used by leading commercial directory software.

Now for the long answer. We are all confronted all the time with the choice RDBMSes vs. directories. It is a hard choice and no simple answer exists.

It is tempting to think that having a RDBMS backend to the directory solves all problems. However, it is a pig. This is because the data models are very different. Representing directory data with a relational database is going to require splitting data into multiple tables.

Think for a moment about the person objectclass. Its definition requires attribute types objectclass, sn and cn and allows attribute types userPassword, telephoneNumber, seeAlso and description. All of these attributes are multivalued, so a normalization requires putting each attribute type in a separate table.

Now you have to decide on appropriate keys for those tables. The primary key might be a combination of the DN, but this becomes rather inefficient on most database implementations.

The big problem now is that accessing data from one entry requires seeking on different disk areas. On some applications this may be OK but in many applications performance suffers.

The only attribute types that can be put in the main table entry are those that are mandatory and single-value. You may add also the optional single-valued attributes and set them to NULL or something if not present.

But wait, the entry can have multiple objectclasses and they are organized in an inheritance hierarchy. An entry of objectclass organizationalPerson now has the attributes from person plus a few others and some formerly optional attribute types are now mandatory.

What to do? Should we have different tables for the different objectclasses? This way the person would have an entry on the person table, another on organizationalPerson, etc. Or should we get rid of person and put everything on the second table?

But what do we do with a filter like (cn=*) where cn is an attribute type that appears in many, many objectclasses. Should we search all possible tables for matching entries? Not very attractive.

Once this point is reached, three approaches come to mind. One is to do full normalization so that each attribute type, no matter what, has its own separate table. The simplistic approach where the DN is part of the primary key is extremely wasteful, and calls for an approach where the entry has a unique numeric id that is used instead for the keys and a main table that maps DN's to ids. The approach, anyway, is very inefficient when several attribute types from one or more entries are requested. Such a database, though cumbersomely, can be managed from SQL applications.

The second approach is to put the whole entry as a blob in a table shared by all entries regardless of the objectclass and have additional tables that act as indices for the first table. Index tables are not database indices, but are fully managed by the LDAP server-side implementation. However, the database becomes unusable from SQL. And, thus, a fully fledged database system provides little or no advantage. The full generality of the database is unneeded. Much better to use something light and fast, like Berkeley DB.

A completely different way to see this is to give up any hopes of implementing the directory data model. In this case, LDAP is used as an access protocol to data that provides only superficially the directory data model. For instance, it may be read only or, where updates are allowed, restrictions are applied, such as making single-value attribute types that would allow for multiple values. Or the impossibility to add new objectclasses...
to an existing entry or remove one of those present. The restrictions span the range from allowed restrictions (that might be elsewhere the result of access control) to outright violations of the data model. It can be, however, a method to provide LDAP access to preexisting data that is used by other applications. But in the understanding that we don't really have a "directory".

Existing commercial LDAP server implementations that use a relational database are either from the first kind or the third. I don't know of any implementation that uses a relational database to do inefficiently what BDB does efficiently. For those who are interested in "third way" (exposing EXISTING data from RDBMS as LDAP tree, having some limitations compared to classic LDAP model, but making it possible to interoperate between LDAP and SQL applications):

OpenLDAP includes back-sql - the backend that makes it possible. It uses ODBC + additional metainformation about translating LDAP queries to SQL queries in your RDBMS schema, providing different levels of access - from read-only to full access depending on RDBMS you use, and your schema.

For more information on concept and limitations, see slapd-sql(5) man page, or the Backends section. There are also several examples for several RDBMSes in back-sql/rdbms_depend/* subdirectories.

1.9. What is slapd and what can it do?

slapd(8) is an LDAP directory server that runs on many different platforms. You can use it to provide a directory service of your very own. Your directory can contain pretty much anything you want to put in it. You can connect it to the global LDAP directory service, or run a service all by yourself. Some of slapd's more interesting features and capabilities include:

LDAPv3: slapd implements version 3 of Lightweight Directory Access Protocol. slapd supports LDAP over both IPv4 and IPv6 and Unix IPC.

Simple Authentication and Security Layer: slapd supports strong authentication and data security (integrity and confidentiality) services through the use of SASL. slapd's SASL implementation utilizes Cyrus SASL software which supports a number of mechanisms including DIGEST-MD5, EXTERNAL, and GSSAPI.

Transport Layer Security: slapd supports certificate-based authentication and data security (integrity and confidentiality) services through the use of TLS (or SSL). slapd's TLS implementation can utilize either OpenSSL or GnuTLS software.

Topology control: slapd can be configured to restrict access at the socket layer based upon network topology information. This feature utilizes TCP wrappers.

Access control: slapd provides a rich and powerful access control facility, allowing you to control access to the information in your database(s). You can control access to entries based on LDAP authorization information, IP address, domain name and other criteria. slapd supports both static and dynamic access control information.

Internationalization: slapd supports Unicode and language tags.

Choice of database backends: slapd comes with a variety of different database backends you can choose from. They include BDB, a high-performance transactional database backend; HDB, a hierarchical high-performance transactional backend; SHELL, a backend interface to arbitrary shell scripts; and PASSWD, a simple backend interface to the passwd(5) file. The BDB and HDB backends utilize Oracle Berkeley DB.
Multiple database instances: slapd can be configured to serve multiple databases at the same time. This means that a single slapd server can respond to requests for many logically different portions of the LDAP tree, using the same or different database backends.

Generic modules API: If you require even more customization, slapd lets you write your own modules easily. slapd consists of two distinct parts: a front end that handles protocol communication with LDAP clients; and modules which handle specific tasks such as database operations. Because these two pieces communicate via a well-defined C API, you can write your own customized modules which extend slapd in numerous ways. Also, a number of programmable database modules are provided. These allow you to expose external data sources to slapd using popular programming languages (Perl, shell, and SQL).

Threads: slapd is threaded for high performance. A single multi-threaded slapd process handles all incoming requests using a pool of threads. This reduces the amount of system overhead required while providing high performance.

Replication: slapd can be configured to maintain shadow copies of directory information. This single-master/multiple-slave replication scheme is vital in high-volume environments where a single slapd installation just doesn't provide the necessary availability or reliability. For extremely demanding environments where a single point of failure is not acceptable, multi-master replication is also available. slapd includes support for LDAP Sync-based replication.

Proxy Cache: slapd can be configured as a caching LDAP proxy service.

Configuration: slapd is highly configurable through a single configuration file which allows you to change just about everything you'd ever want to change. Configuration options have reasonable defaults, making your job much easier. Configuration can also be performed dynamically using LDAP itself, which greatly improves manageability.
2. A Quick-Start Guide

The following is a quick start guide to OpenLDAP Software 2.4, including the Standalone LDAP Daemon, \texttt{slapd}(8).

It is meant to walk you through the basic steps needed to install and configure OpenLDAP Software. It should be used in conjunction with the other chapters of this document, manual pages, and other materials provided with the distribution (e.g. the \texttt{INSTALL} document) or on the OpenLDAP web site (http://www.OpenLDAP.org), in particular the OpenLDAP Software FAQ (http://www.OpenLDAP.org/faq/?file=2).

If you intend to run OpenLDAP Software seriously, you should review all of this document before attempting to install the software.

Note: This quick start guide does not use strong authentication nor any integrity or confidential protection services. These services are described in other chapters of the OpenLDAP Administrator's Guide.

1. Get the software
   You can obtain a copy of the software by following the instructions on the OpenLDAP Software download page (http://www.openldap.org/software/download/). It is recommended that new users start with the latest release.

2. Unpack the distribution
   Pick a directory for the source to live under, change directory to there, and unpack the distribution using the following commands:
   \texttt{gunzip -c openldap-VERSION.tgz | tar xvfB -}
   then relocate yourself into the distribution directory:
   \texttt{cd openldap-VERSION}
   You'll have to replace \texttt{VERSION} with the version name of the release.

3. Review documentation
   You should now review the \texttt{COPYRIGHT}, \texttt{LICENSE}, \texttt{README} and \texttt{INSTALL} documents provided with the distribution. The \texttt{COPYRIGHT} and \texttt{LICENSE} provide information on acceptable use, copying, and limitation of warranty of OpenLDAP Software.

   You should also review other chapters of this document. In particular, the Building and Installing OpenLDAP Software chapter of this document provides detailed information on prerequisite software and installation procedures.

4. Run configure
   You will need to run the provided \texttt{configure} script to \texttt{configure} the distribution for building on your system. The \texttt{configure} script accepts many command line options that enable or disable optional software features. Usually the defaults are okay, but you may want to change them. To get a complete list of options that \texttt{configure} accepts, use the \texttt{--help} option:
   \texttt{./configure --help}
   However, given that you are using this guide, we'll assume you are brave enough to just let \texttt{configure} determine what's best:
./configure

Assuming configure doesn't dislike your system, you can proceed with building the software. If configure did complain, well, you'll likely need to go to the Software FAQ Installation section (http://www.openldap.org/faq/?file=8) and/or actually read the Building and Installing OpenLDAP Software chapter of this document.

5. Build the software.
   The next step is to build the software. This step has two parts, first we construct dependencies and then we compile the software:
   `make depend`
   `make`
   Both makes should complete without error.

6. Test the build.
   To ensure a correct build, you should run the test suite (it only takes a few minutes):
   `make test`
   Tests which apply to your configuration will run and they should pass. Some tests, such as the replication test, may be skipped.

7. Install the software.
   You are now ready to install the software; this usually requires super-user privileges:
   `su root -c 'make install'`
   Everything should now be installed under /usr/local (or whatever installation prefix was used by configure).

8. Edit the configuration file.
   Use your favorite editor to edit the provided `slapd.conf` example (usually installed as
   `/usr/local/etc/openldap/slapd.conf`) to contain a BDB database definition of the form:
   `database bdb
    suffix "dc=<MY-DOMAIN>,dc=<COM>"
    rootdn "cn=Manager,dc=<MY-DOMAIN>,dc=<COM>"
    rootpw secret
    directory /usr/local/var/openldap-data`
   Be sure to replace `<MY-DOMAIN>` and `<COM>` with the appropriate domain components of your domain name. For example, for example.com, use:
   `database bdb
    suffix "dc=example,dc=com"
    rootdn "cn=Manager,dc=example,dc=com"
    rootpw secret
    directory /usr/local/var/openldap-data`
   If your domain contains additional components, such as eng.uni.edu.eu, use:
   `database bdb
    suffix "dc=eng,dc=uni,dc=edu,dc=eu"
    rootdn "cn=Manager,dc=eng,dc=uni,dc=edu,dc=eu"
    rootpw secret
    directory /usr/local/var/openldap-data`
   Details regarding configuring `slapd(8)` can be found in the `slapd.conf(5)` manual page and the The slapd Configuration File chapter of this document. Note that the specified directory must exist prior to starting `slapd(8)`.
9. **Start SLAPD.**

You are now ready to start the Standalone LDAP Daemon, `slapd(8)`, by running the command:
```
su root -c /usr/local/libexec/slapd
```
To check to see if the server is running and configured correctly, you can run a search against it with `ldapsearch(1)`. By default, `ldapsearch` is installed as `/usr/local/bin/ldapsearch`:
```
ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
```
Note the use of single quotes around command parameters to prevent special characters from being interpreted by the shell. This should return:
```
dn: namingContexts: dc=example,dc=com
```
Details regarding running `slapd(8)` can be found in the `slapd(8)` manual page and the Running slapd chapter of this document.

10. **Add initial entries to your directory.**

You can use `ldapadd(1)` to add entries to your LDAP directory. `ldapadd` expects input in LDIF form. We'll do it in two steps:

1. **Create an LDIF file.**

   Use your favorite editor and create an LDIF file that contains:
   ```
   dn: dc=<MY-DOMAIN>,dc=<COM>
   objectclass: dcObject
   objectclass: organization
   o: <MY ORGANIZATION>
   dc: <MY-DOMAIN>
   
   dn: cn=Manager,dc=<MY-DOMAIN>,dc=<COM>
   objectclass: organizationalRole
   cn: Manager
   
   Be sure to replace `<MY-DOMAIN>` and `<COM>` with the appropriate domain components of your domain name. `<MY ORGANIZATION>` should be replaced with the name of your organization. When you cut and paste, be sure to trim any leading and trailing whitespace from the example.
   
   Now, you may run `ldapadd(1)` to insert these entries into your directory.
   ```
   ldapadd -x -D "cn=Manager,dc=<MY-DOMAIN>,dc=<COM>" -W -f example.ldif
   ```
   Be sure to replace `<MY-DOMAIN>` and `<COM>` with the appropriate domain components of your domain name. You will be prompted for the "secret" specified in `slapd.conf`. For example, for `example.com`, use:
   ```
   ldapadd -x -D "cn=Manager,dc=example,dc=com" -W -f example.ldif
   ```
   where `example.ldif` is the file you created above.

   Additional information regarding directory creation can be found in the Database Creation and
11. **See if it works.**

Now we're ready to verify the added entries are in your directory. You can use any LDAP client to do this, but our example uses the `ldapsearch(1)` tool. Remember to replace `dc=example,dc=com` with the correct values for your site:

```
ldapsearch -x -b 'dc=example,dc=com' '(objectclass=*)'
```

This command will search for and retrieve every entry in the database.

You are now ready to add more entries using `ldapadd(1)` or another LDAP client, experiment with various configuration options, backend arrangements, etc..

Note that by default, the `slapd(8)` database grants *read access to everybody* excepting the *super-user* (as specified by the `rootdn` configuration directive). It is highly recommended that you establish controls to restrict access to authorized users. Access controls are discussed in the *The access Configuration Directive* section of *The slapd Configuration File* chapter. You are also encouraged to read the Security Considerations, Using SASL and Using TLS sections.

The following chapters provide more detailed information on making, installing, and running `slapd(8)`. 
3. The Big Picture - Configuration Choices

This section gives a brief overview of various LDAP directory configurations, and how your Standalone LDAP Daemon `slapd(8)` fits in with the rest of the world.

3.1. Local Directory Service

In this configuration, you run a `slapd(8)` instance which provides directory service for your local domain only. It does not interact with other directory servers in any way. This configuration is shown in Figure 3.1.

Use this configuration if you are just starting out (it's the one the quick-start guide makes for you) or if you want to provide a local service and are not interested in connecting to the rest of the world. It's easy to upgrade to another configuration later if you want.

3.2. Local Directory Service with Referrals

In this configuration, you run a `slapd(8)` instance which provides directory service for your local domain and configure it to return referrals to other servers capable of handling requests. You may run this service (or services) yourself or use one provided to you. This configuration is shown in Figure 3.2.

Use this configuration if you want to provide local service and participate in the Global Directory, or you want to delegate responsibility for subordinate entries to another server.

3.3. Replicated Directory Service

`slapd(8)` includes support for `LDAP Sync`-based replication, called `syncrepl`, which may be used to maintain shadow copies of directory information on multiple directory servers. In its most basic configuration, the `master` is a syncrepl provider and one or more `slave` (or `shadow`) are syncrepl consumers. An example
master-slave configuration is shown in figure 3.3.

This configuration can be used in conjunction with either of the first two configurations in situations where a single slapd(8) instance does not provide the required reliability or availability.

### 3.4. Distributed Local Directory Service

In this configuration, the local service is partitioned into smaller services, each of which may be replicated, and glued together with superior and subordinate referrals.
4. Building and Installing OpenLDAP Software

This chapter details how to build and install the OpenLDAP Software package including `slapd(8)`, the Standalone LDAP Daemon. Building and installing OpenLDAP Software requires several steps: installing prerequisite software, configuring OpenLDAP Software itself, making, and finally installing. The following sections describe this process in detail.

4.1. Obtaining and Extracting the Software

You can obtain OpenLDAP Software from the project's download page at http://www.openldap.org/software/download/ or directly from the project's FTP service at ftp://ftp.openldap.org/pub/OpenLDAP/.

The project makes available two series of packages for general use. The project makes releases as new features and bug fixes come available. Though the project takes steps to improve stability of these releases, it is common for problems to arise only after release. The stable release is the latest release which has demonstrated stability through general use.

Users of OpenLDAP Software can choose, depending on their desire for the latest features versus demonstrated stability, the most appropriate series to install.

After downloading OpenLDAP Software, you need to extract the distribution from the compressed archive file and change your working directory to the top directory of the distribution:

```bash
gunzip -c openldap-VERSION.tgz | tar xf -
cd openldap-VERSION
```

You'll have to replace `VERSION` with the version name of the release.

You should now review the COPYRIGHT, LICENSE, README and INSTALL documents provided with the distribution. The COPYRIGHT and LICENSE provide information on acceptable use, copying, and limitation of warranty of OpenLDAP Software. The README and INSTALL documents provide detailed information on prerequisite software and installation procedures.

4.2. Prerequisite software

OpenLDAP Software relies upon a number of software packages distributed by third parties. Depending on the features you intend to use, you may have to download and install a number of additional software packages. This section details commonly needed third party software packages you might have to install. However, for an up-to-date prerequisite information, the README document should be consulted. Note that some of these third party packages may depend on additional software packages. Install each package per the installation instructions provided with it.

4.2.1. Transport Layer Security

OpenLDAP clients and servers require installation of either OpenSSL or GnuTLS TLS libraries to provide Transport Layer Security services. Though some operating systems may provide these libraries as part of the base system or as an optional software component, OpenSSL and GnuTLS often require separate installation.

OpenLDAP Software will not be fully LDAPv3 compliant unless OpenLDAP's configure detects a usable TLS library.

### 4.2.2. Simple Authentication and Security Layer

OpenLDAP clients and servers require installation of Cyrus SASL libraries to provide Simple Authentication and Security Layer services. Though some operating systems may provide this library as part of the base system or as an optional software component, Cyrus SASL often requires separate installation.

Cyrus SASL is available from http://asg.web.cmu.edu/sasl/sasl-library.html. Cyrus SASL will make use of OpenSSL and Kerberos/GSSAPI libraries if preinstalled.

OpenLDAP Software will not be fully LDAPv3 compliant unless OpenLDAP's configure detects a usable Cyrus SASL installation.

### 4.2.3. Kerberos Authentication Service

OpenLDAP clients and servers support Kerberos authentication services. In particular, OpenLDAP supports the Kerberos V GSS-API SASL authentication mechanism known as the GSSAPI mechanism. This feature requires, in addition to Cyrus SASL libraries, either Heimdal or MIT Kerberos V libraries.


Use of strong authentication services, such as those provided by Kerberos, is highly recommended.

### 4.2.4. Database Software

OpenLDAP's `slapd(8)` BDB and HDB primary database backends require Oracle Corporation Berkeley DB. If not available at configure time, you will not be able build `slapd(8)` with these primary database backends.

Your operating system may provide a supported version of Berkeley DB in the base system or as an optional software component. If not, you'll have to obtain and install it yourself.


There are several versions available. Generally, the most recent release (with published patches) is recommended. This package is required if you wish to use the BDB or HDB database backends.

**Note:** Please see Recommended OpenLDAP Software Dependency Versions for more information.

### 4.2.5. Threads

OpenLDAP is designed to take advantage of threads. OpenLDAP supports POSIX `pthreads`, Mach `CThreads`, and a number of other varieties. configure will complain if it cannot find a suitable thread subsystem. If this occurs, please consult the Software|Installation|Platform Hints section of the
4.2.6. TCP Wrappers

slapd(8) supports TCP Wrappers (IP level access control filters) if preinstalled. Use of TCP Wrappers or other IP-level access filters (such as those provided by an IP-level firewall) is recommended for servers containing non-public information.

4.3. Running configure

Now you should probably run the configure script with the --help option. This will give you a list of options that you can change when building OpenLDAP. Many of the features of OpenLDAP can be enabled or disabled using this method.

```
./configure --help
```

The configure script will also look at various environment variables for certain settings. These environment variables include:

Table 4.1: Environment Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>Specify alternative C Compiler</td>
</tr>
<tr>
<td>CFLAGS</td>
<td>Specify additional compiler flags</td>
</tr>
<tr>
<td>CPPFLAGS</td>
<td>Specify C Preprocessor flags</td>
</tr>
<tr>
<td>LDFLAGS</td>
<td>Specify linker flags</td>
</tr>
<tr>
<td>LIBS</td>
<td>Specify additional libraries</td>
</tr>
</tbody>
</table>

Now run the configure script with any desired configuration options or environment variables.

```
[[env] settings] ./configure [options]
```

As an example, let’s assume that we want to install OpenLDAP with BDB backend and TCP Wrappers support. By default, BDB is enabled and TCP Wrappers is not. So, we just need to specify --with-wrappers to include TCP Wrappers support:

```
./configure --with-wrappers
```

However, this will fail to locate dependent software not installed in system directories. For example, if TCP Wrappers headers and libraries are installed in /usr/local/include and /usr/local/lib respectively, the configure script should be called as follows:

```
env CPPFLAGS="-I/usr/local/include" LDFLAGS="-L/usr/local/lib" \
./configure --with-wrappers
```

**Note:** Some shells, such as those derived from the Bourne sh(1), do not require use of the env(1) command. In some cases, environmental variables have to be specified using alternative syntaxes.

The configure script will normally auto-detect appropriate settings. If you have problems at this stage, consult any platform specific hints and check your configure options, if any.
4.4. Building the Software

Once you have run the `configure` script the last line of output should be:

```
Please "make depend" to build dependencies
```

If the last line of output does not match, `configure` has failed, and you will need to review its output to determine what went wrong. You should not proceed until `configure` completes successfully.

To build dependencies, run:

```
made depend
```

Now build the software, this step will actually compile OpenLDAP.

```
made
```

You should examine the output of this command carefully to make sure everything is built correctly. Note that this command builds the LDAP libraries and associated clients as well as `slapd(8)`.

4.5. Testing the Software

Once the software has been properly configured and successfully made, you should run the test suite to verify the build.

```
made test
```

Tests which apply to your configuration will run and they should pass. Some tests, such as the replication test, may be skipped if not supported by your configuration.

4.6. Installing the Software

Once you have successfully tested the software, you are ready to install it. You will need to have write permission to the installation directories you specified when you ran `configure`. By default OpenLDAP Software is installed in `/usr/local`. If you changed this setting with the `--prefix configure` option, it will be installed in the location you provided.

Typically, the installation requires `super-user` privileges. From the top level OpenLDAP source directory, type:

```
su root -c 'make install'
```

and enter the appropriate password when requested.

You should examine the output of this command carefully to make sure everything is installed correctly. You will find the configuration files for `slapd(8)` in `/usr/local/etc/openldap` by default. See the chapter Configuring `slapd` for additional information.
5. Configuring slapd

Once the software has been built and installed, you are ready to configure "slapd(8)" for use at your site. Unlike previous OpenLDAP releases, the slapd(8) runtime configuration in 2.3 (and later) is fully LDAP-enabled and can be managed using the standard LDAP operations with data in LDIF. The LDAP configuration engine allows all of slapd's configuration options to be changed on the fly, generally without requiring a server restart for the changes to take effect. The old style "slapd.conf(5)" file is still supported, but must be converted to the new "slapd-config(5)" format to allow runtime changes to be saved. While the old style configuration uses a single file, normally installed as /usr/local/etc/openldap/slapd.conf, the new style uses a slapd backend database to store the configuration. The configuration database normally resides in the /usr/local/etc/openldap/slapd.d directory. When converting from the slapd.conf format to slapd.d format, any include files will also be integrated into the resulting configuration database.

An alternate configuration directory (or file) can be specified via a command-line option to "slapd(8)". This chapter describes the general format of the configuration system, followed by a detailed description of commonly used config settings.

**Note:** some of the backends and of the distributed overlays do not support runtime configuration yet. In those cases, the old style "slapd.conf(5)" file must be used.

5.1. Configuration Layout

The slapd configuration is stored as a special LDAP directory with a predefined schema and DIT. There are specific objectClasses used to carry global configuration options, schema definitions, backend and database definitions, and assorted other items. A sample config tree is shown in Figure 5.1.

```
Figure 5.1: Sample configuration tree.
```

Other objects may be part of the configuration but were omitted from the illustration for clarity.

The "slapd-config" configuration tree has a very specific structure. The root of the tree is named cn=config and contains global configuration settings. Additional settings are contained in separate child entries:
Dynamically loaded modules
These may only be used if the --enable-modules option was used to configure the software.

Schema definitions
The cn=schema,cn=config entry contains the system schema (all the schema that is hard-coded in slapd).
Child entries of cn=schema,cn=config contain user schema as loaded from config files or added at runtime.

Backend-specific configuration
Database-specific configuration
Overlays are defined in children of the Database entry.
Databases and Overlays may also have other miscellaneous children.

The usual rules for LDIF files apply to the configuration information: Comment lines beginning with a '#' character are ignored. If a line begins with a single space, it is considered a continuation of the previous line (even if the previous line is a comment) and the single leading space is removed. Entries are separated by blank lines.

The general layout of the config LDIF is as follows:

```ldif
# global configuration settings
dn: cn=config
objectClass: olcGlobal
cn: config
<global config settings>

# schema definitions
dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema
<system schema>

dn: cn={X}core,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: {X}core
<core schema>

# additional user-specified schema
...

# backend definitions
dn: olcBackend=<typeA>,cn=config
objectClass: olcBackendConfig
olcBackend: <typeA>
<backend-specific settings>

# database definitions
dn: olcDatabase={X}<typeA>,cn=config
objectClass: olcDatabaseConfig
olcDatabase: (X)<typeA>
<database-specific settings>

# subsequent definitions and settings
...
```

Some of the entries listed above have a numeric index "{X}" in their names. While most configuration settings have an inherent ordering dependency (i.e., one setting must take effect before a subsequent one may
be set), LDAP databases are inherently unordered. The numeric index is used to enforce a consistent ordering in the configuration database, so that all ordering dependencies are preserved. In most cases the index does not have to be provided; it will be automatically generated based on the order in which entries are created.

Configuration directives are specified as values of individual attributes. Most of the attributes and objectClasses used in the slapd configuration have a prefix of "olc" (OpenLDAP Configuration) in their names. Generally there is a one-to-one correspondence between the attributes and the old-style slapd.conf configuration keywords, using the keyword as the attribute name, with the "olc" prefix attached.

A configuration directive may take arguments. If so, the arguments are separated by white space. If an argument contains white space, the argument should be enclosed in double quotes "like this". In the descriptions that follow, arguments that should be replaced by actual text are shown in brackets <>.

The distribution contains an example configuration file that will be installed in the /usr/local/etc/openldap directory. A number of files containing schema definitions (attribute types and object classes) are also provided in the /usr/local/etc/openldap/schema directory.

5.2. Configuration Directives

This section details commonly used configuration directives. For a complete list, see the slapd-config(5) manual page. This section will treat the configuration directives in a top-down order, starting with the global directives in the cn=config entry. Each directive will be described along with its default value (if any) and an example of its use.

5.2.1. cn=config

Directives contained in this entry generally apply to the server as a whole. Most of them are system or connection oriented, not database related. This entry must have the olcGlobal objectClass.

5.2.1.1. olcIdleTimeout: <integer>

Specify the number of seconds to wait before forcibly closing an idle client connection. A value of 0, the default, disables this feature.

5.2.1.2. olcLogLevel: <level>

This directive specifies the level at which debugging statements and operation statistics should be syslogged (currently logged to the syslogd(8) LOG_LOCAL4 facility). You must have configured OpenLDAP --enable-debug (the default) for this to work (except for the two statistics levels, which are always enabled). Log levels may be specified as integers or by keyword. Multiple log levels may be used and the levels are additive. To display what levels correspond to what kind of debugging, invoke slapd with -? or consult the table below. The possible values for <level> are:

<table>
<thead>
<tr>
<th>Level</th>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Any</td>
<td>enable all debugging</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td>no debugging</td>
</tr>
<tr>
<td>1</td>
<td>Trace</td>
<td>trace function calls</td>
</tr>
</tbody>
</table>

Table 5.1: Debugging Levels
Example:

```
olcLogLevel: -1
```

This will cause lots and lots of debugging information to be logged.

```
olcLogLevel: Conns Filter
```

Just log the connection and search filter processing.

Default:

```
olcLogLevel: Stats
```

### 5.2.1.3. `olcReferral <URI>`

This directive specifies the referral to pass back when slapd cannot find a local database to handle a request.

Example:

```
olcReferral: ldap://root.openldap.org
```

This will refer non-local queries to the global root LDAP server at the OpenLDAP Project. Smart LDAP clients can re-ask their query at that server, but note that most of these clients are only going to know how to handle simple LDAP URLs that contain a host part and optionally a distinguished name part.

### 5.2.1.4. Sample Entry

```
dn: cn=config
objectClass: olcGlobal
cn: config
olcIdleTimeout: 30
olcLogLevel: Stats
olcReferral: ldap://root.openldap.org
```
5.2.2. **cn=module**

If support for dynamically loaded modules was enabled when configuring slapd, **cn=module** entries may be used to specify sets of modules to load. Module entries must have the **olcModuleList** objectClass.

5.2.2.1. **olcModuleLoad: <filename>**

Specify the name of a dynamically loadable module to load. The filename may be an absolute path name or a simple filename. Non-absolute names are searched for in the directories specified by the **olcModulePath** directive.

5.2.2.2. **olcModulePath: <pathspec>**

Specify a list of directories to search for loadable modules. Typically the path is colon-separated but this depends on the operating system.

5.2.2.3. **Sample Entries**

```
  dn: cn=module{0},cn=config
  objectClass: olcModuleList
  cn: module{0}
  olcModuleLoad: /usr/local/lib/smbk5pwd.la

  dn: cn=module{1},cn=config
  objectClass: olcModuleList
  cn: module{1}
  olcModulePath: /usr/local/lib:/usr/local/lib/slapd
  olcModuleLoad: accesslog.la
  olcModuleLoad: pcache.la
```

5.2.3. **cn=schema**

The **cn=schema** entry holds all of the schema definitions that are hard-coded in slapd. As such, the values in this entry are generated by slapd so no schema values need to be provided in the config file. The entry must still be defined though, to serve as a base for the user-defined schema to add in underneath. Schema entries must have the **olcSchemaConfig** objectClass.

5.2.3.1. **olcAttributeTypes: <RFC4512 Attribute Type Description>**

This directive defines an attribute type. Please see the Schema Specification chapter for information regarding how to use this directive.

5.2.3.2. **olcObjectClasses: <RFC4512 Object Class Description>**

This directive defines an object class. Please see the Schema Specification chapter for information regarding how to use this directive.

5.2.3.3. **Sample Entries**

```
  dn: cn=schema,cn=config
  objectClass: olcSchemaConfig
  cn: schema
```
5.2.4. Backend-specific Directives

Backend directives apply to all database instances of the same type and, depending on the directive, may be overridden by database directives. Backend entries must have the `olcBackendConfig` objectClass.

5.2.4.1. olcBackend: <type>

This directive names a backend-specific configuration entry. `<type>` should be one of the supported backend types listed in Table 5.2.

<table>
<thead>
<tr>
<th>Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdb</td>
<td>Berkeley DB transactional backend</td>
</tr>
<tr>
<td>config</td>
<td>Slapd configuration backend</td>
</tr>
<tr>
<td>dnssrv</td>
<td>DNS SRV backend</td>
</tr>
<tr>
<td>hdb</td>
<td>Hierarchical variant of bdb backend</td>
</tr>
<tr>
<td>ldap</td>
<td>Lightweight Directory Access Protocol (Proxy) backend</td>
</tr>
<tr>
<td>ldif</td>
<td>Lightweight Data Interchange Format backend</td>
</tr>
<tr>
<td>meta</td>
<td>Meta Directory backend</td>
</tr>
<tr>
<td>monitor</td>
<td>Monitor backend</td>
</tr>
<tr>
<td>passwd</td>
<td>Provides read-only access to <code>passwd(5)</code></td>
</tr>
<tr>
<td>perl</td>
<td>Perl Programmable backend</td>
</tr>
<tr>
<td>shell</td>
<td>Shell (extern program) backend</td>
</tr>
<tr>
<td>sql</td>
<td>SQL Programmable backend</td>
</tr>
</tbody>
</table>

Example:

```
olcBackend: bdb
```

There are no other directives defined for this entry. Specific backend types may define additional attributes for their particular use but so far none have ever been defined. As such, these directives usually do not appear in any actual configurations.

5.2.4.2. Sample Entry

```
dn: olcBackend=bdb, cn=config
objectClass: olcBackendConfig
olcBackend: bdb
```
5.2.5. Database-specific Directives

Directives in this section are supported by every type of database. Database entries must have the olcDatabaseConfig objectClass.

5.2.5.1. olcDatabase: [{<index>}]<type>

This directive names a specific database instance. The numeric {<index>} may be provided to distinguish multiple databases of the same type. Usually the index can be omitted, and slapd will generate it automatically. <type> should be one of the supported backend types listed in Table 5.2 or the frontend type.

The frontend is a special database that is used to hold database-level options that should be applied to all the other databases. Subsequent database definitions may also override some frontend settings.

The config database is also special; both the config and the frontend databases are always created implicitly even if they are not explicitly configured, and they are created before any other databases.

Example:

    olcDatabase: bdb

This marks the beginning of a new BDB database instance.

5.2.5.2. olcAccess: to <what> [ by <who> [accesslevel] [control] ]+

This directive grants access (specified by accesslevel) to a set of entries and/or attributes (specified by what) by one or more requestors (specified by who). See the Access Control section of this chapter for a summary of basic usage.

Note: If no olcAccess directives are specified, the default access control policy, to * by * read, allows all users (both authenticated and anonymous) read access.

Note: Access controls defined in the frontend are appended to all other databases' controls.

5.2.5.3. olcReadonly { TRUE | FALSE }

This directive puts the database into "read-only" mode. Any attempts to modify the database will return an "unwilling to perform" error.

Default:

    olcReadonly: FALSE

5.2.5.4. olcRootDN: <DN>

This directive specifies the DN that is not subject to access control or administrative limit restrictions for operations on this database. The DN need not refer to an entry in this database or even in the directory. The DN may refer to a SASL identity.
Entry-based Example:

```
olcRootDN: "cn=Manager,dc=example,dc=com"
```

SASL-based Example:

```
olcRootDN: "uid=root,cn=example.com,cn=digest-md5,cn=auth"
```

See the SASL Authentication section for information on SASL authentication identities.

### 5.2.5.5. `olcRootPW: <password>`

This directive can be used to specify a password for the DN for the rootdn (when the rootdn is set to a DN within the database).

Example:

```
olcRootPW: secret
```

It is also permissible to provide a hash of the password in RFC2307 form. `slappasswd` may be used to generate the password hash.

Example:

```
olcRootPW: {SSHA}ZKKuqbEKJfKSXhUbHG3fG8MDn9j1v4QN
```

The hash was generated using the command `slappasswd -s secret`.

### 5.2.5.6. `olcSizeLimit: <integer>`

This directive specifies the maximum number of entries to return from a search operation.

Default:

```
olcSizeLimit: 500
```

### 5.2.5.7. `olcSuffix: <dn suffix>`

This directive specifies the DN suffix of queries that will be passed to this backend database. Multiple suffix lines can be given, and usually at least one is required for each database definition. (Some backend types, such as frontend and monitor use a hard-coded suffix which may not be overridden in the configuration.)

Example:

```
olcSuffix: "dc=example,dc=com"
```

Queries with a DN ending in "dc=example,dc=com" will be passed to this backend.

**Note:** When the backend to pass a query to is selected, slapd looks at the suffix value(s) in each database definition in the order in which they were configured. Thus, if one database suffix is a prefix of another, it must appear after it in the configuration.
5.2.5.8. olcSyncrepl

This directive specifies the current database as a replica of the master content by establishing the current `slapd`(8) as a replication consumer site running a syncrepl replication engine. The master database is located at the replication provider site specified by the `provider` parameter. The replica database is kept up-to-date with the master content using the LDAP Content Synchronization protocol. See RFC4533 for more information on the protocol.

The `rid` parameter is used for identification of the current `syncrepl` directive within the replication consumer server, where `<replica ID>` uniquely identifies the `syncrepl` specification described by the current `syncrepl` directive. `<replica ID>` is non-negative and is no more than three decimal digits in length.

The `provider` parameter specifies the replication provider site containing the master content as an LDAP URI. The `provider` parameter specifies a scheme, a host and optionally a port where the provider slapd instance can be found. Either a domain name or IP address may be used for `<hostname>`. Examples are `ldap://provider.example.com:389` or `ldaps://192.168.1.1:636`. If `<port>` is not given, the standard LDAP port number (389 or 636) is used. Note that the syncrepl uses a consumer-initiated protocol, and hence its specification is located at the consumer site, whereas the `replica` specification is located at the provider site. `syncrepl` and `replica` directives define two independent replication mechanisms. They do not represent the replication peers of each other.
The content of the syncrepl replica is defined using a search specification as its result set. The consumer slapd will send search requests to the provider slapd according to the search specification. The search specification includes searchbase, scope, filter, attrs, attrsonly, sizelimit, and timelimit parameters as in the normal search specification. The searchbase parameter has no default value and must always be specified. The scope defaults to sub, the filter defaults to (objectclass=*) , attrs defaults to "*, +" to replicate all user and operational attributes, and attrsonly is unset by default. Both sizelimit and timelimit default to "unlimited", and only positive integers or "unlimited" may be specified.

The LDAP Content Synchronization protocol has two operation types: refreshOnly and refreshAndPersist. The operation type is specified by the type parameter. In the refreshOnly operation, the next synchronization search operation is periodically rescheduled at an interval time after each synchronization operation finishes. The interval is specified by the interval parameter. It is set to one day by default. In the refreshAndPersist operation, a synchronization search remains persistent in the provider slapd instance. Further updates to the master replica will generate searchResultEntry to the consumer slapd as the search responses to the persistent synchronization search.

If an error occurs during replication, the consumer will attempt to reconnect according to the retry parameter which is a list of the <retry interval> and <# of retries> pairs. For example, retry="60 10 300 3" lets the consumer retry every 60 seconds for the first 10 times and then retry every 300 seconds for the next three times before stop retrying. + in <# of retries> means indefinite number of retries until success.

The schema checking can be enforced at the LDAP Sync consumer site by turning on the schemachecking parameter. If it is turned on, every replicated entry will be checked for its schema as the entry is stored into the replica content. Every entry in the replica should contain those attributes required by the schema definition. If it is turned off, entries will be stored without checking schema conformance. The default is off.

The binddn parameter gives the DN to bind as for the syncrepl searches to the provider slapd. It should be a DN which has read access to the replication content in the master database.

The bindmethod is simple or sasl, depending on whether simple password-based authentication or SASL authentication is to be used when connecting to the provider slapd instance.

Simple authentication should not be used unless adequate data integrity and confidentiality protections are in place (e.g. TLS or IPsec). Simple authentication requires specification of binddn and credentials parameters.

SASL authentication is generally recommended. SASL authentication requires specification of a mechanism using the saslmech parameter. Depending on the mechanism, an authentication identity and/or credentials can be specified using authcid and credentials, respectively. The authzid parameter may be used to specify an authorization identity.

The realm parameter specifies a realm which a certain mechanisms authenticate the identity within. The secprops parameter specifies Cyrus SASL security properties.

The starttls parameter specifies use of the StartTLS extended operation to establish a TLS session before authenticating to the provider. If the critical argument is supplied, the session will be aborted if the StartTLS request fails. Otherwise the syncrepl session continues without TLS. Note that the main slapd TLS settings are not used by the syncrepl engine; by default the TLS parameters from a ldap.conf(5) configuration file will be used. TLS settings may be specified here, in which case any ldap.conf(5) settings will be
Rather than replicating whole entries, the consumer can query logs of data modifications. This mode of operation is referred to as *delta syncrepl*. In addition to the above parameters, the *logbase* and *logfilter* parameters must be set appropriately for the log that will be used. The *syncdata* parameter must be set to either "accesslog" if the log conforms to the *slapo-accesslog*(5) log format, or "changelog" if the log conforms to the obsolete *changelog* format. If the *syncdata* parameter is omitted or set to "default" then the log parameters are ignored.

The *syncrepl* replication mechanism is supported by the *bdb* and *hdb* backends.

See the LDAP Sync Replication chapter of this guide for more information on how to use this directive.

### 5.2.5.9. *olcTimeLimit: <integer>*

This directive specifies the maximum number of seconds (in real time) slapd will spend answering a search request. If a request is not finished in this time, a result indicating an exceeded timelimit will be returned.

Default:

```
olcTimeLimit: 3600
```

### 5.2.5.10. *olcUpdateref: <URL>*

This directive is only applicable in a slave slapd. It specifies the URL to return to clients which submit update requests upon the replica. If specified multiple times, each URL is provided.

Example:

```
olcUpdateref: ldap://master.example.net
```

### 5.2.5.11. Sample Entries

```
dn: olcDatabase=frontend,cn=config
objectClass: olcDatabaseConfig
objectClass: olcFrontendConfig
olcDatabase: frontend
olcReadOnly: FALSE

dn: olcDatabase=config,cn=config
objectClass: olcDatabaseConfig
olcDatabase: config
olcRootDN: cn=Manager,dc=example,dc=com
```

### 5.2.6. BDB and HDB Database Directives

Directives in this category apply to both the BDB and the HDB database. They are used in an *olcDatabase* entry in addition to the generic database directives defined above. For a complete reference of BDB/HDB configuration directives, see *slapd-bdb*(5). In addition to the *olcDatabaseConfig* objectClass, BDB and HDB database entries must have the *olcBdbConfig* and *olcHdbConfig* objectClass, respectively.
5.2.6.1. **olcDbDirectory: <directory>**

This directive specifies the directory where the BDB files containing the database and associated indices live.

Default:

```
olcDbDirectory: /usr/local/var/openldap-data
```

5.2.6.2. **olcDbCachesize: <integer>**

This directive specifies the size in entries of the in-memory cache maintained by the BDB backend database instance.

Default:

```
olcDbCachesize: 1000
```

5.2.6.3. **olcDbCheckpoint: <kbyte> <min>**

This directive specifies how often to checkpoint the BDB transaction log. A checkpoint operation flushes the database buffers to disk and writes a checkpoint record in the log. The checkpoint will occur if either <kbyte> data has been written or <min> minutes have passed since the last checkpoint. Both arguments default to zero, in which case they are ignored. When the <min> argument is non-zero, an internal task will run every <min> minutes to perform the checkpoint. See the Berkeley DB reference guide for more details.

Example:

```
olcDbCheckpoint: 1024 10
```

5.2.6.4. **olcDbConfig: <DB_CONFIG setting>**

This attribute specifies a configuration directive to be placed in the DB_CONFIG file of the database directory. At server startup time, if no such file exists yet, the DB_CONFIG file will be created and the settings in this attribute will be written to it. If the file exists, its contents will be read and displayed in this attribute. The attribute is multi-valued, to accommodate multiple configuration directives. No default is provided, but it is essential to use proper settings here to get the best server performance.

Any changes made to this attribute will be written to the DB_CONFIG file and will cause the database environment to be reset so the changes can take immediate effect. If the environment cache is large and has not been recently checkpointed, this reset operation may take a long time. It may be advisable to manually perform a single checkpoint using the Berkeley DB db_checkpoint utility before using LDAP Modify to change this attribute.

Example:

```
olcDbConfig: set_cachesize 0 10485760 0
olcDbConfig: set_lg_bsize 2097512
olcDbConfig: set_lg_dir /var/tmp/bdb-log
olcDbConfig: set_flags DB_LOG_AUTOREMOVE
```

In this example, the BDB cache is set to 10MB, the BDB transaction log buffer size is set to 2MB, and the transaction log files are to be stored in the /var/tmp/bdb-log directory. Also a flag is set to tell BDB to delete
transaction log files as soon as their contents have been checkpointed and they are no longer needed. Without this setting the transaction log files will continue to accumulate until some other cleanup procedure removes them. See the Berkeley DB documentation for the `db_archive` command for details.

Ideally the BDB cache must be at least as large as the working set of the database, the log buffer size should be large enough to accommodate most transactions without overflowing, and the log directory must be on a separate physical disk from the main database files. And both the database directory and the log directory should be separate from disks used for regular system activities such as the root, boot, or swap filesystems. See the FAQ-o-Matic and the Berkeley DB documentation for more details.

5.2.6.5. `olcDbNosync: { TRUE | FALSE }`

This option causes on-disk database contents to not be immediately synchronized with in memory changes upon change. Setting this option to `TRUE` may improve performance at the expense of data integrity. This directive has the same effect as using

```
olcDbConfig: set_flags DB_TXN_NOSYNC
```

5.2.6.6. `olcDbIDLcacheSize: <integer>`

Specify the size of the in-memory index cache, in index slots. The default is zero. A larger value will speed up frequent searches of indexed entries. The optimal size will depend on the data and search characteristics of the database, but using a number three times the entry cache size is a good starting point.

Example:

```
olcDbIDLcacheSize: 3000
```

5.2.6.7. `olcDbIndex: {<attrlist> | default} [pres,eq,approx,sub,none]`

This directive specifies the indices to maintain for the given attribute. If only an `<attrlist>` is given, the default indices are maintained. The index keywords correspond to the common types of matches that may be used in an LDAP search filter.

Example:

```
olcDbIndex: default pres,eq
olcDbIndex: uid
olcDbIndex: cn,sn pres,eq,sub
olcDbIndex: objectClass eq
```

The first line sets the default set of indices to maintain to present and equality. The second line causes the default (pres,eq) set of indices to be maintained for the `uid` attribute type. The third line causes present, equality, and substring indices to be maintained for `cn` and `sn` attribute types. The fourth line causes an equality index for the `objectClass` attribute type.

There is no index keyword for inequality matches. Generally these matches do not use an index. However, some attributes do support indexing for inequality matches, based on the equality index.

A substring index can be more explicitly specified as `subinitial`, `subany`, or `subfinal`, corresponding to the three possible components of a substring match filter. A subinitial index only indexes substrings that appear at the beginning of an attribute value. A subfinal index only indexes substrings that appear at the end.
of an attribute value, while subany indexes substrings that occur anywhere in a value.

Note that by default, setting an index for an attribute also affects every subtype of that attribute. E.g., setting an equality index on the `name` attribute causes `cn`, `sn`, and every other attribute that inherits from `name` to be indexed.

By default, no indices are maintained. It is generally advised that minimally an equality index upon `objectClass` be maintained.

```
olcDbindex: objectClass eq
```

Additional indices should be configured corresponding to the most common searches that are used on the database. Presence indexing should not be configured for an attribute unless the attribute occurs very rarely in the database, and presence searches on the attribute occur very frequently during normal use of the directory. Most applications don't use presence searches, so usually presence indexing is not very useful.

If this setting is changed while slapd is running, an internal task will be run to generate the changed index data. All server operations can continue as normal while the indexer does its work. If slapd is stopped before the index task completes, indexing will have to be manually completed using the `slapindex` tool.

**5.2.6.8. olcDbLinearIndex: { TRUE | FALSE }**

If this setting is `TRUE` `slapindex` will index one attribute at a time. The default settings is `FALSE` in which case all indexed attributes of an entry are processed at the same time. When enabled, each indexed attribute is processed individually, using multiple passes through the entire database. This option improves `slapindex` performance when the database size exceeds the BDB cache size. When the BDB cache is large enough, this option is not needed and will decrease performance. Also by default, `slapadd` performs full indexing and so a separate `slapindex` run is not needed. With this option, `slapadd` does no indexing and `slapindex` must be used.

**5.2.6.9. olcDbMode: <integer>**

This directive specifies the file protection mode that newly created database index files should have.

Default:

```
olcDbMode: 0600
```

**5.2.6.10. olcDbSearchStack: <integer>**

Specify the depth of the stack used for search filter evaluation. Search filters are evaluated on a stack to accommodate nested AND / OR clauses. An individual stack is allocated for each server thread. The depth of the stack determines how complex a filter can be evaluated without requiring any additional memory allocation. Filters that are nested deeper than the search stack depth will cause a separate stack to be allocated for that particular search operation. These separate allocations can have a major negative impact on server performance, but specifying too much stack will also consume a great deal of memory. Each search uses 512K bytes per level on a 32-bit machine, or 1024K bytes per level on a 64-bit machine. The default stack depth is 16, thus 8MB or 16MB per thread is used on 32 and 64 bit machines, respectively. Also the 512KB size of a single stack slot is set by a compile-time constant which may be changed if needed; the code must be recompiled for the change to take effect.

Default:
5.2.6.11. olcDbShmKey: <integer>

Specify a key for a shared memory BDB environment. By default the BDB environment uses memory mapped files. If a non-zero value is specified, it will be used as the key to identify a shared memory region that will house the environment.

Example:

olcDbShmKey: 42

5.2.6.12. Sample Entry

dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: hdb
olcSuffix: "dc=example,dc=com"
olcDbDirectory: /usr/local/var/openldap-data
olcDbCacheSize: 1000
olcDbCheckpoint: 1024 10
olcDbConfig: set_cachesize 0 10485760 0
olcDbConfig: set_lg_bsize 2097152
olcDbConfig: set_lg_dir /var/tmp/bdb-log
olcDbConfig: set_flags DB_LOG_AUTOREMOVE
olcDbDLCacheSize: 3000
olcDbIndex: objectClass eq

5.3. Access Control

Access to slapd entries and attributes is controlled by the olcAccess attribute, whose values are a sequence of access directives. The general form of the olcAccess configuration is:

```
olcAccess: <access directive>
<access directive> ::= to <what>
    [by <who> [<access>] [<control>]] [+]
<what> ::= * | [dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
    [filter=<ldapfilter>] [attrs=<attrlist>]
<basic-style> ::= regex | exact
<scope-style> ::= base | one | subtree | children
<attrlist> ::= <attr> [val[.<basic-style>]=<regex>] | <attr>, <attrlist>
<attr> ::= <attrname> | entry | children
<who> ::= * | [anonymous | users | self]
    | dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
    [dnattr=<attrname>]
    [group[/<objectclass>[/<attrname>]/.<basic-style>]=<regex>]
    [peername[.<basic-style>]=<regex>]
    [sockname[.<basic-style>]=<regex>]
    [domain[.<basic-style>]=<regex>]
    [sockurl[.<basic-style>]=<regex>]
    [set=<setspec>]
    [aci=<attrname>]
<access> ::= [self] [<level>] [<priv>]
<level> ::= none | disclose | auth | compare | search | read | write | manage
.priv> ::= {|=|+|-}{m|w|r|s|c|x|d|0}+
```
where the <what> part selects the entries and/or attributes to which the access applies, the <who> part specifies which entities are granted access, and the <access> part specifies the access granted. Multiple <who> <access> <control> triplets are supported, allowing many entities to be granted different access to the same set of entries and attributes. Not all of these access control options are described here; for more details see the `slapd.access(5)` man page.

**5.3.1. What to control access to**

The <what> part of an access specification determines the entries and attributes to which the access control applies. Entries are commonly selected in two ways: by DN and by filter. The following qualifiers select entries by DN:

```
  to *
  to dn[.<basic-style>]=<regex>
  to dn.<scope-style>=<DN>
```

The first form is used to select all entries. The second form may be used to select entries by matching a regular expression against the target entry's normalized DN. (The second form is not discussed further in this document.) The third form is used to select entries which are within the requested scope of DN. The <DN> is a string representation of the Distinguished Name, as described in RFC4514.

The scope can be either base, one, subtree, or children. Where base matches only the entry with provided DN, one matches the entries whose parent is the provided DN, subtree matches all entries in the subtree whose root is the provided DN, and children matches all entries under the DN (but not the entry named by the DN).

For example, if the directory contained entries named:

```
0: o=suffix
1: cn=Manager,o=suffix
2: ou=people,o=suffix
3: uid=kdz,ou=people,o=suffix
4: cn=addresses,uid=kdz,ou=people,o=suffix
5: uid=hyc,ou=people,o=suffix
```

Then:

```
dn.base="ou=people,o=suffix" match 2;
dn.one="ou=people,o=suffix" match 3, and 5;
dn.subtree="ou=people,o=suffix" match 2, 3, 4, and 5; and
dn.children="ou=people,o=suffix" match 3, 4, and 5.
```

Entries may also be selected using a filter:

```
to filter=<ldap filter>
```

where <ldap filter> is a string representation of an LDAP search filter, as described in RFC4515. For example:

```
to filter=(objectClass=person)
```
Note that entries may be selected by both DN and filter by including both qualifiers in the <what> clause.

\texttt{to dn.one="ou=people,o=suffix" filter={(objectClass=person)}}

Attributes within an entry are selected by including a comma-separated list of attribute names in the <what> selector:

\texttt{attrs=<attribute list>}

A specific value of an attribute is selected by using a single attribute name and also using a value selector:

\texttt{attrs=<attribute> val[.<style>]=<regex>}

There are two special \textit{pseudo} attributes \texttt{entry} and \texttt{children}. To read (and hence return) a target entry, the subject must have read access to the target's \texttt{entry} attribute. To add or delete an entry, the subject must have write access to the entry's \texttt{entry} attribute AND must have write access to the entry's parent's \texttt{children} attribute. To rename an entry, the subject must have write access to entry's \texttt{entry} attribute AND have write access to both the old parent's and new parent's \texttt{children} attributes. The complete examples at the end of this section should help clear things up.

Lastly, there is a special entry selector "*" that is used to select any entry. It is used when no other <what> selector has been provided. It's equivalent to "dn=.*"

\textbf{5.3.2. Who to grant access to}

The <who> part identifies the entity or entities being granted access. Note that access is granted to "entities" not "entries." The following table summarizes entity specifiers:

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Specifier} & \textbf{Entities} \\
\hline
* & All, including anonymous and authenticated users \\
anonymous & Anonymous (non-authenticated) users \\
users & Authenticated users \\
self & User associated with target entry \\
dn[.<basic-style>]=<regex> & Users matching a regular expression \\
dn.<scope-style>=<DN> & Users within scope of a DN \\
\hline
\end{tabular}
\caption{Access Entity Specifiers}
\end{table}

The DN specifier behaves much like <what> clause DN specifiers.

Other control factors are also supported. For example, a <who> can be restricted by an entry listed in a DN-valued attribute in the entry to which the access applies:

\texttt{dnattr=<dn-valued attribute name>}

The dnattr specification is used to give access to an entry whose DN is listed in an attribute of the entry (e.g., give access to a group entry to whoever is listed as the owner of the group entry).

Some factors may not be appropriate in all environments (or any). For example, the domain factor relies on IP to domain name lookups. As these can easily spoofed, the domain factor should not be avoided.
5.3.3. The access to grant

The kind of <access> granted can be one of the following:

<table>
<thead>
<tr>
<th>Level</th>
<th>Privileges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>=0</td>
<td>no access</td>
</tr>
<tr>
<td>disclose</td>
<td>=d</td>
<td>needed for information disclosure on error</td>
</tr>
<tr>
<td>auth</td>
<td>=dx</td>
<td>needed to authenticate (bind)</td>
</tr>
<tr>
<td>compare</td>
<td>=cdx</td>
<td>needed to compare</td>
</tr>
<tr>
<td>search</td>
<td>=scdx</td>
<td>needed to apply search filters</td>
</tr>
<tr>
<td>read</td>
<td>=rscdx</td>
<td>needed to read search results</td>
</tr>
<tr>
<td>write</td>
<td>=wrsbcdx</td>
<td>needed to modify/rename</td>
</tr>
<tr>
<td>manage</td>
<td>=mwsbcdx</td>
<td>needed to manage</td>
</tr>
</tbody>
</table>

Each level implies all lower levels of access. So, for example, granting someone write access to an entry also grants them read, search, compare, auth and disclose access. However, one may use the privileges specifier to grant specific permissions.

5.3.4. Access Control Evaluation

When evaluating whether some requester should be given access to an entry and/or attribute, slapd compares the entry and/or attribute to the <what> selectors given in the configuration. For each entry, access controls provided in the database which holds the entry (or the first database if not held in any database) apply first, followed by the global access directives (which are held in the frontend database definition). Within this priority, access directives are examined in the order in which they appear in the configuration attribute. Slapd stops with the first <what> selector that matches the entry and/or attribute. The corresponding access directive is the one slapd will use to evaluate access.

Next, slapd compares the entity requesting access to the <who> selectors within the access directive selected above in the order in which they appear. It stops with the first <who> selector that matches the requester. This determines the access the entity requesting access has to the entry and/or attribute.

Finally, slapd compares the access granted in the selected <access> clause to the access requested by the client. If it allows greater or equal access, access is granted. Otherwise, access is denied.

The order of evaluation of access directives makes their placement in the configuration file important. If one access directive is more specific than another in terms of the entries it selects, it should appear first in the configuration. Similarly, if one <who> selector is more specific than another it should come first in the access directive. The access control examples given below should help make this clear.

5.3.5. Access Control Examples

The access control facility described above is quite powerful. This section shows some examples of its use for descriptive purposes.

A simple example:
This access directive grants read access to everyone.

This directive allows the user to modify their entry, allows anonymous to authenticate against these entries, and allows all others to read these entries. Note that only the first by <who> clause which matches applies. Hence, the anonymous users are granted auth, not read. The last clause could just as well have been "by users read".

It is often desirable to restrict operations based upon the level of protection in place. The following shows how security strength factors (SSF) can be used.

This directive allows users to modify their own entries if security protections of strength 128 or better have been established, allows authentication access to anonymous users, and read access when strength 64 or better security protections have been established. If the client has not establish sufficient security protections, the implicit by * none clause would be applied.

The following example shows the use of style specifiers to select the entries by DN in two access directives where ordering is significant.

Read access is granted to entries under the dc=com subtree, except for those entries under the dc=example,dc=com subtree, to which search access is granted. No access is granted to dc=com as neither access directive matches this DN. If the order of these access directives was reversed, the trailing directive would never be reached, since all entries under dc=example,dc=com are also under dc=com entries.

Also note that if no olcAccess: to directive matches or no by <who> clause, access is denied. That is, every olcAccess: to directive ends with an implicit by * none clause and every access list ends with an implicit olcAccess: to * by * none directive.

The next example again shows the importance of ordering, both of the access directives and the by <who> clauses. It also shows the use of an attribute selector to grant access to a specific attribute and various <who> selectors.
This example applies to entries in the "dc=example,dc=com" subtree. To all attributes except homePhone, an entry can write to itself, entries under example.com entries can search by them, anybody else has no access (implicit by * none) excepting for authentication/authorization (which is always done anonymously). The homePhone attribute is writable by the entry, searchable by entries under example.com, readable by clients connecting from network 10, and otherwise not readable (implicit by * none). All other access is denied by the implicit access to * by * none.

Sometimes it is useful to permit a particular DN to add or remove itself from an attribute. For example, if you would like to create a group and allow people to add and remove only their own DN from the member attribute, you could accomplish it with an access directive like this:

```
olcAccess: to attrs=member,entry
by dnattr=member selfwrite
```

The dnattr <who> selector says that the access applies to entries listed in the member attribute. The selfwrite access selector says that such members can only add or delete their own DN from the attribute, not other values. The addition of the entry attribute is required because access to the entry is required to access any of the entry's attributes.

### 5.3.6. Access Control Ordering

Since the ordering of olcAccess directives is essential to their proper evaluation, but LDAP attributes normally do not preserve the ordering of their values, OpenLDAP uses a custom schema extension to maintain a fixed ordering of these values. This ordering is maintained by prepending a "{:X}" numeric index to each value, similarly to the approach used for ordering the configuration entries. These index tags are maintained automatically by slapd and do not need to be specified when originally defining the values. For example, when you create the settings

```
olcAccess: to attrs=member,entry
by dnattr=member selfwrite
olcAccess: to dn.children="dc=example,dc=com"
by * search
olcAccess: to dn.children="dc=com"
by * read
```

when you read them back using slapcat or ldapsearch they will contain

```
olcAccess: {0}to attrs=member,entry
by dnattr=member selfwrite
olcAccess: {1}to dn.children="dc=example,dc=com"
by * search
olcAccess: {2}to dn.children="dc=com"
by * read
```

The numeric index may be used to specify a particular value to change when using ldapmodify to edit the access rules. This index can be used instead of (or in addition to) the actual access value. Using this numeric index is very helpful when multiple access rules are being managed.

For example, if we needed to change the second rule above to grant write access instead of search, we could
try this LDIF:

```
changetype: modify
delete: olcAccess
  olcAccess: to dn.children="dc=example,dc=com" by * search
  -
  add: olcAccess
  olcAccess: to dn.children="dc=example,dc=com" by * write
  -
```

But this example **will not** guarantee that the existing values remain in their original order, so it will most likely yield a broken security configuration. Instead, the numeric index should be used:

```
changetype: modify
delete: olcAccess
  olcAccess: {1}
  -
  add: olcAccess
  olcAccess: {1}to dn.children="dc=example,dc=com" by * write
  -
```

This example deletes whatever rule is in value #1 of the `olcAccess` attribute (regardless of its value) and adds a new value that is explicitly inserted as value #1. The result will be:

```
olcAccess: {0}to attrs=member,entry
  by dnattr=member selfwrite
olcAccess: {1}to dn.children="dc=example,dc=com" by * write
  by * read
olcAccess: {2}to dn.children="dc=com"
```

which is exactly what was intended.

### 5.4. Configuration Example

The following is an example configuration, interspersed with explanatory text. It defines two databases to handle different parts of the X.500 tree; both are BDB database instances. The line numbers shown are provided for reference only and are not included in the actual file. First, the global configuration section:

```
1.    # example config file - global configuration entry
2.    dn: cn=config
3.    objectClass: olcGlobal
4.    cn: config
5.    olcReferral: ldap://root.openldap.org
6.    
```

Line 1 is a comment. Lines 2-4 identify this as the global configuration entry. The `olcReferral:` directive on line 5 means that queries not local to one of the databases defined below will be referred to the LDAP server running on the standard port (389) at the host `root.openldap.org`. Line 6 is a blank line, indicating the end of this entry.

```
7.    # internal schema
8.    dn: cn=schema,cn=config
9.    objectClass: olcSchemaConfig
10.   cn: schema
11.   
```
Line 7 is a comment. Lines 8-10 identify this as the root of the schema subtree. The actual schema definitions in this entry are hardcoded into slapd so no additional attributes are specified here. Line 11 is a blank line, indicating the end of this entry.

12.    # include the core schema
13.    include: file:///usr/local/etc/openldap/schema/core.ldif
14.

Line 12 is a comment. Line 13 is an LDIF include directive which accesses the core schema definitions in LDIF format. Line 14 is a blank line.

Next comes the database definitions. The first database is the special frontend database whose settings are applied globally to all the other databases.

15.    # global database parameters
16.    dn: olcDatabase=frontend,cn=config
17.    objectClass: olcDatabaseConfig
18.    olcDatabase: frontend
19.    olcAccess: to * by * read
20.

Line 15 is a comment. Lines 16-18 identify this entry as the global database entry. Line 19 is a global access control. It applies to all entries (after any applicable database-specific access controls).

The next entry defines a BDB backend that will handle queries for things in the "dc=example,dc=com" portion of the tree. Indices are to be maintained for several attributes, and the userPassword attribute is to be protected from unauthorized access.

21.    # BDB definition for example.com
22.    dn: olcDatabase=bdb,cn=config
23.    objectClass: olcDatabaseConfig
24.    objectClass: olcBdbConfig
25.    olcDatabase: bdb
26.    olcSuffix: "dc=example,dc=com"
27.    olcDbDirectory: /usr/local/var/openldap-data
28.    olcRootDN: "cn=Manager,dc=example,dc=com"
29.    olcRootPW: secret
30.    olcDbIndex: uid pres,eq
31.    olcDbIndex: cn,sn,uid pres,eq,approx,sub
32.    olcDbIndex: objectClass eq
33.    olcAccess: to attrs=userPassword
34.      by self write
35.      by anonymous auth
36.      by dn.base="cn=Admin,dc=example,dc=com" write
37.      by * none
38.    olcAccess: to *
39.      by self write
40.      by dn.base="cn=Admin,dc=example,dc=com" write
41.      by * read
42.

Line 21 is a comment. Lines 22-25 identify this entry as a BDB database configuration entry. Line 26 specifies the DN suffix for queries to pass to this database. Line 27 specifies the directory in which the database files will live.
Lines 28 and 29 identify the database *super-user* entry and associated password. This entry is not subject to access control or size or time limit restrictions.

Lines 30 through 32 indicate the indices to maintain for various attributes.

Lines 33 through 41 specify access control for entries in this database. As this is the first database, the controls also apply to entries not held in any database (such as the Root DSE). For all applicable entries, the *userPassword* attribute is writable by the entry itself and by the "admin" entry. It may be used for authentication/authorization purposes, but is otherwise not readable. All other attributes are writable by the entry and the "admin" entry, but may be read by all users (authenticated or not).

Line 42 is a blank line, indicating the end of this entry.

The next section of the example configuration file defines another BDB database. This one handles queries involving the *dc=example,dc=net* subtree but is managed by the same entity as the first database. Note that without line 52, the read access would be allowed due to the global access rule at line 19.

```
43. # BDB definition for example.net
44. dn: olcDatabase=bdb,cn=config
45. objectClass: olcDatabaseConfig
46. objectClass: olcBdbConfig
47. olcDatabase: bdb
48. olcSuffix: "dc=example,dc=net"
50. olcRootDN: "cn=Manager,dc=example,dc=com"
51. olcDbIndex: objectClass eq
52. olcAccess: to * by users read
```

### 5.5. Converting from slapd.conf(8) to a cn=config directory format

Discuss slap* -f slapd.conf -F slapd.d/ (man slapd-config)
6. The slapd Configuration File

Once the software has been built and installed, you are ready to configure *slapd*(8) for use at your site. The slapd runtime configuration is primarily accomplished through the *slapd.conf*(5) file, normally installed in the /usr/local/etc/openldap directory.

An alternate configuration file location can be specified via a command-line option to *slapd*(8). This chapter describes the general format of the *slapd.conf*(5) configuration file, followed by a detailed description of commonly used config file directives.

6.1. Configuration File Format

The *slapd.conf*(5) file consists of three types of configuration information: global, backend specific, and database specific. Global information is specified first, followed by information associated with a particular backend type, which is then followed by information associated with a particular database instance. Global directives can be overridden in backend and/or database directives, and backend directives can be overridden by database directives.

Blank lines and comment lines beginning with a '#' character are ignored. If a line begins with white space, it is considered a continuation of the previous line (even if the previous line is a comment).

The general format of slapd.conf is as follows:

```plaintext
# global configuration directives
<global config directives>

# backend definition
backend <typeA>
<backend-specific directives>

# first database definition & config directives
database <typeA>
<database-specific directives>

# second database definition & config directives
database <typeB>
<database-specific directives>

# second database definition & config directives
database <typeA>
<database-specific directives>

# subsequent backend & database definitions & config directives
...
```

A configuration directive may take arguments. If so, they are separated by white space. If an argument contains white space, the argument should be enclosed in double quotes "like this". If an argument contains a double quote or a backslash character \`, the character should be preceded by a backslash character `\`.

The distribution contains an example configuration file that will be installed in the /usr/local/etc/openldap directory. A number of files containing schema definitions (attribute types and object classes) are also provided in the /usr/local/etc/openldap/schema directory.
6.2. Configuration File Directives

This section details commonly used configuration directives. For a complete list, see the slapd.conf(5) manual page. This section separates the configuration file directives into global, backend-specific and data-specific categories, describing each directive and its default value (if any), and giving an example of its use.

6.2.1. Global Directives

Directives described in this section apply to all backends and databases unless specifically overridden in a backend or database definition. Arguments that should be replaced by actual text are shown in brackets <>.

6.2.1.1. access to <what> [ by <who> [<accesslevel>] [<control>]+

This directive grants access (specified by <accesslevel>) to a set of entries and/or attributes (specified by <what>) by one or more requestors (specified by <who>). See the The access Configuration Directive section of this chapter for a summary of basic usage.

Note: If no access directives are specified, the default access control policy, access to * by * read, allows all both authenticated and anonymous users read access.

6.2.1.2. attributetype <RFC4512 Attribute Type Description>

This directive defines an attribute type. Please see the Schema Specification chapter for information regarding how to use this directive.

6.2.1.3. idletimeout <integer>

Specify the number of seconds to wait before forcibly closing an idle client connection. An idletimeout of 0, the default, disables this feature.

6.2.1.4. include <filename>

This directive specifies that slapd should read additional configuration information from the given file before continuing with the next line of the current file. The included file should follow the normal slapd config file format. The file is commonly used to include files containing schema specifications.

Note: You should be careful when using this directive - there is no small limit on the number of nested include directives, and no loop detection is done.

6.2.1.5. loglevel <integer>

This directive specifies the level at which debugging statements and operation statistics should be syslogged (currently logged to the syslogd(8) LOG_LOCAL4 facility). You must have configured OpenLDAP --enable-debug (the default) for this to work (except for the two statistics levels, which are always enabled). Log levels are additive. To display what numbers correspond to what kind of debugging, invoke slapd with --? or consult the table below. The possible values for <integer> are:

Table 6.1: Debugging Levels
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>enable all debugging</td>
</tr>
<tr>
<td>0</td>
<td>no debugging</td>
</tr>
<tr>
<td>1</td>
<td>trace function calls</td>
</tr>
<tr>
<td>2</td>
<td>debug packet handling</td>
</tr>
<tr>
<td>4</td>
<td>heavy trace debugging</td>
</tr>
<tr>
<td>8</td>
<td>connection management</td>
</tr>
<tr>
<td>16</td>
<td>print out packets sent and received</td>
</tr>
<tr>
<td>32</td>
<td>search filter processing</td>
</tr>
<tr>
<td>64</td>
<td>configuration file processing</td>
</tr>
<tr>
<td>128</td>
<td>access control list processing</td>
</tr>
<tr>
<td>256</td>
<td>stats log connections/operations/results</td>
</tr>
<tr>
<td>512</td>
<td>stats log entries sent</td>
</tr>
<tr>
<td>1024</td>
<td>print communication with shell backends</td>
</tr>
<tr>
<td>2048</td>
<td>print entry parsing debugging</td>
</tr>
</tbody>
</table>

Example:

    loglevel -1

This will cause lots and lots of debugging information to be logged.

Default:

    loglevel 256

6.2.1.6. objectclass <RFC4512 Object Class Description>

This directive defines an object class. Please see the Schema Specification chapter for information regarding how to use this directive.

6.2.1.7. referral <URI>

This directive specifies the referral to pass back when slapd cannot find a local database to handle a request.

Example:

    referral ldap://root.openldap.org

This will refer non-local queries to the global root LDAP server at the OpenLDAP Project. Smart LDAP clients can re-ask their query at that server, but note that most of these clients are only going to know how to handle simple LDAP URLs that contain a host part and optionally a distinguished name part.

6.2.1.8. sizelimit <integer>

This directive specifies the maximum number of entries to return from a search operation.

Default:
sizelimit 500

6.2.1.9. timelimit <integer>

This directive specifies the maximum number of seconds (in real time) slapd will spend answering a search request. If a request is not finished in this time, a result indicating an exceeded timelimit will be returned.

Default:

    timelimit 3600

6.2.2. General Backend Directives

Directives in this section apply only to the backend in which they are defined. They are supported by every type of backend. Backend directives apply to all databases instances of the same type and, depending on the directive, may be overridden by database directives.

6.2.2.1. backend <type>

This directive marks the beginning of a backend declaration. <type> should be one of the supported backend types listed in Table 6.2.

Table 5.2: Database Backends

<table>
<thead>
<tr>
<th>Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdb</td>
<td>Berkeley DB transactional backend</td>
</tr>
<tr>
<td>dnssrv</td>
<td>DNS SRV backend</td>
</tr>
<tr>
<td>hdb</td>
<td>Hierarchical variant of bdb backend</td>
</tr>
<tr>
<td>ldap</td>
<td>Lightweight Directory Access Protocol (Proxy) backend</td>
</tr>
<tr>
<td>meta</td>
<td>Meta Directory backend</td>
</tr>
<tr>
<td>monitor</td>
<td>Monitor backend</td>
</tr>
<tr>
<td>passwd</td>
<td>Provides read-only access to passwd(5)</td>
</tr>
<tr>
<td>perl</td>
<td>Perl Programmable backend</td>
</tr>
<tr>
<td>shell</td>
<td>Shell (extern program) backend</td>
</tr>
<tr>
<td>sql</td>
<td>SQL Programmable backend</td>
</tr>
</tbody>
</table>

Example:

    backend bdb

This marks the beginning of a new BDB backend definition.

6.2.3. General Database Directives

Directives in this section apply only to the database in which they are defined. They are supported by every type of database.
6.2.3.1. database <type>

This directive marks the beginning of a database instance declaration. <type> should be one of the supported backend types listed in Table 6.2.

Example:

database bdb

This marks the beginning of a new BDB database instance declaration.

6.2.3.2. readonly { on | off }

This directive puts the database into "read-only" mode. Any attempts to modify the database will return an "unwilling to perform" error.

Default:

readonly off

6.2.3.3. rootdn <DN>

This directive specifies the DN that is not subject to access control or administrative limit restrictions for operations on this database. The DN need not refer to an entry in this database or even in the directory. The DN may refer to a SASL identity.

Entry-based Example:

    rootdn "cn=Manager,dc=example,dc=com"

SASL-based Example:

    rootdn "uid=root,cn=example.com,cn=digest-md5,cn=auth"

See the SASL Authentication section for information on SASL authentication identities.

6.2.3.4. rootpw <password>

This directive can be used to specifies a password for the DN for the rootdn (when the rootdn is set to a DN within the database).

Example:

    rootpw secret

It is also permissible to provide hash of the password in RFC2307 form. \texttt{slappasswd(8)} may be used to generate the password hash.

Example:

    rootpw {SSHA}ZKKuqbEKJfKSXhUbHG3fG8MDn9j1v4QN
The hash was generated using the command `slappasswd -s secret`.

### 6.2.3.5. suffix <dn suffix>

This directive specifies the DN suffix of queries that will be passed to this backend database. Multiple suffix lines can be given, and at least one is required for each database definition.

Example:

```
suffix "dc=example,dc=com"
```

Queries with a DN ending in "dc=example,dc=com" will be passed to this backend.

**Note:** When the backend to pass a query to is selected, slapd looks at the suffix line(s) in each database definition in the order they appear in the file. Thus, if one database suffix is a prefix of another, it must appear after it in the config file.

### 6.2.3.6. syncrepl

```
syncrepl rid=<replica ID>
  provider=ldap[s]://<hostname>[:port]
  [type=refreshOnly|refreshAndPersist]
  [interval=dd:hh:mm:ss]
  [retry=[<retry interval> <# of retries>]+]
  searchbase=<base DN>
  [filter=<filter str>]
  [scope=sub|one|base]
  [attrsonly]
  [sizelimit=<limit>]
  [timelimit=<limit>]
  [schemachecking=on|off]
  [bindmethod=simple|sasl]
  [binddn=<DN>]
  [saslmech=<mech>]
  [authcid=<identity>]
  [authzid=<identity>]
  [credentials=<passwd>]
  [realm=<realm>]
  [secprops=<properties>]
```

This directive specifies the current database as a replica of the master content by establishing the current `slapd` as a replication consumer site running a syncrepl replication engine. The master database is located at the replication provider site specified by the `provider` parameter. The replica database is kept up-to-date with the master content using the LDAP Content Synchronization protocol. See RFC4533 for more information on the protocol.

The `rid` parameter is used for identification of the current syncrepl directive within the replication consumer server, where `<replica ID>` uniquely identifies the syncrepl specification described by the current syncrepl directive. `<replica ID>` is non-negative and is no more than three decimal digits in length.

The `provider` parameter specifies the replication provider site containing the master content as an LDAP URI. The `provider` parameter specifies a scheme, a host and optionally a port where the provider slapd
instance can be found. Either a domain name or IP address may be used for <hostname>. Examples are ldap://provider.example.com:389 or ldaps://192.168.1.1:636. If <port> is not given, the standard LDAP port number (389 or 636) is used. Note that the syncrepl uses a consumer-initiated protocol, and hence its specification is located at the consumer site, whereas the replica specification is located at the provider site. syncrepl and replica directives define two independent replication mechanisms. They do not represent the replication peers of each other.

The content of the syncrepl replica is defined using a search specification as its result set. The consumer slapd will send search requests to the provider slapd according to the search specification. The search specification includes searchbase, scope, filter, attrs, attrsonly, sizelimit, and timelimit parameters as in the normal search specification. The searchbase parameter has no default value and must always be specified. The scope defaults to sub, the filter defaults to (objectclass=*), attrs defaults to ",, +" to replicate all user and operational attributes, and attrsonly is unset by default. Both sizelimit and timelimit default to "unlimited", and only integers or "unlimited" may be specified.

The LDAP Content Synchronization protocol has two operation types: refreshOnly and refreshAndPersist. The operation type is specified by the type parameter. In the refreshOnly operation, the next synchronization search operation is periodically rescheduled at an interval time after each synchronization operation finishes. The interval is specified by the interval parameter. It is set to one day by default. In the refreshAndPersist operation, a synchronization search remains persistent in the provider slapd. Further updates to the master replica will generate searchResultEntry to the consumer slapd as the search responses to the persistent synchronization search.

If an error occurs during replication, the consumer will attempt to reconnect according to the retry parameter which is a list of the <retry interval> and <# of retries> pairs. For example, retry="60 10 300 3" lets the consumer retry every 60 seconds for the first 10 times and then retry every 300 seconds for the next three times before stop retrying. + in <# of retries> means indefinite number of retries until success.

The schema checking can be enforced at the LDAP Sync consumer site by turning on the schemachecking parameter. If it is turned on, every replicated entry will be checked for its schema as the entry is stored into the replica content. Every entry in the replica should contain those attributes required by the schema definition. If it is turned off, entries will be stored without checking schema conformance. The default is off.

The binddn parameter gives the DN to bind as for the syncrepl searches to the provider slapd. It should be a DN which has read access to the replication content in the master database.

The bindmethod is simple or sasl, depending on whether simple password-based authentication or SASL authentication is to be used when connecting to the provider slapd.

Simple authentication should not be used unless adequate data integrity and confidentiality protections are in place (e.g. TLS or IPsec). Simple authentication requires specification of binddn and credentials parameters.

SASL authentication is generally recommended. SASL authentication requires specification of a mechanism using the saslmech parameter. Depending on the mechanism, an authentication identity and/or credentials can be specified using authcid and credentials, respectively. The authzid parameter may be used to specify an authorization identity.

The realm parameter specifies a realm which a certain mechanisms authenticate the identity within. The secprops parameter specifies Cyrus SASL security properties.
The syncrepl replication mechanism is supported by the two primary database backends: back-bdb and back-hdb.

See the LDAP Sync Replication chapter of the admin guide for more information on how to use this directive.

**6.2.3.7. updateref <URL>**

This directive is only applicable in a *slave* (or *shadow*) *slapd*(8) instance. It specifies the URL to return to clients which submit update requests upon the replica. If specified multiple times, each URL is provided.

Example:

```
updateref       ldap://master.example.net
```

**6.2.4. BDB and HDB Database Directives**

Directives in this category only apply to both the BDB and the HDB database. That is, they must follow a "database bdb" or "database hdb" line and come before any subsequent "backend" or "database" line. For a complete reference of BDB/HDB configuration directives, see *slapd-bdb*(5).

**6.2.4.1. directory <directory>**

This directive specifies the directory where the BDB files containing the database and associated indices live.

Default:

```
directory /usr/local/var/openldap-data
```

**6.3. The access Configuration Directive**

Access to entries and attributes is controlled by the access configuration file directive. The general form of an access line is:

```
<access directive> ::= access to <what>
   [by <who> [<access>] [<control>] ]+
<what> ::= * | [dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>] | [filter=<ldapfilter>] [attrs=<attrlist>] | [basic-style ::= regex | exact]
<scope-style ::= base | one | subtree | children]
<attrlist ::= <attr> [val[.<basic-style>]=<regex>] | <attr> , <attrlist>
<attr ::= <attrname> | entry | children
<who ::= * | [anonymous | users | self | dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>] [dnattr=<attrname>] [group[/<objectclass>/[<attrname>][.<basic-style>]=<regex>]] [peername[.<basic-style>]=<regex>] [sockname[.<basic-style>]=<regex>] [domain[.<basic-style>]=<regex>] [sockurl[.<basic-style>]=<regex>] [set=<setspec>] [aci=<attrname>] [access ::= [self]{<level>|<priv>}
<level ::= none | disclose | auth | compare | search | read | write | manage
```
where the <what> part selects the entries and/or attributes to which the access applies, the <who> part specifies which entities are granted access, and the <access> part specifies the access granted. Multiple <who> <access> <control> triplets are supported, allowing many entities to be granted different access to the same set of entries and attributes. Not all of these access control options are described here; for more details see the slapd.access(5) man page.

### 6.3.1. What to control access to

The <what> part of an access specification determines the entries and attributes to which the access control applies. Entries are commonly selected in two ways: by DN and by filter. The following qualifiers select entries by DN:

```
to *  
to dn[.<basic-style>=<regex>]  
to dn.<scope-style>=<DN>
```

The first form is used to select all entries. The second form may be used to select entries by matching a regular expression against the target entry's normalized DN. (The second form is not discussed further in this document.) The third form is used to select entries which are within the requested scope of DN. The <DN> is a string representation of the Distinguished Name, as described in RFC4514.

The scope can be either base, one, subtree, or children. Where base matches only the entry with provided DN, one matches the entries whose parent is the provided DN, subtree matches all entries in the subtree whose root is the provided DN, and children matches all entries under the DN (but not the entry named by the DN).

For example, if the directory contained entries named:

```
0: o=suffix
1: cn=Manager,o=suffix
2: ou=people,o=suffix
3: uid=kdz,ou=people,o=suffix
4: cn=addresses,uid=kdz,ou=people,o=suffix
5: uid=hyc,ou=people,o=suffix
```

Then:

```
dn.base="ou=people,o=suffix" match 2;  
dn.one="ou=people,o=suffix" match 3, and 5;  
dn.subtree="ou=people,o=suffix" match 2, 3, 4, and 5; and  
dn.children="ou=people,o=suffix" match 3, 4, and 5.  
```

Entries may also be selected using a filter:

```
to filter=<ldap filter>
```

where <ldap filter> is a string representation of an LDAP search filter, as described in RFC4515. For example:

```
to filter=(objectClass=person)
```
Note that entries may be selected by both DN and filter by including both qualifiers in the <what> clause.

```plaintext
to dn.one="ou=people,o=suffix" filter=(objectClass=person)
```

Attributes within an entry are selected by including a comma-separated list of attribute names in the <what> selector:

```plaintext
attrs=<attribute list>
```

A specific value of an attribute is selected by using a single attribute name and also using a value selector:

```plaintext
attrs=<attribute> val[.<style>]=<regex>
```

There are two special *pseudo* attributes `entry` and `children`. To read (and hence return) a target entry, the subject must have read access to the target's `entry` attribute. To add or delete an entry, the subject must have write access to the entry's `entry` attribute AND must have write access to the entry's parent's `children` attribute. To rename an entry, the subject must have write access to entry's `entry` attribute AND have write access to both the old parent's and new parent's `children` attributes. The complete examples at the end of this section should help clear things up.

Lastly, there is a special entry selector "*" that is used to select any entry. It is used when no other <what> selector has been provided. It's equivalent to "dn=.*"

### 6.3.2. Who to grant access to

The <who> part identifies the entity or entities being granted access. Note that access is granted to "entities" not "entries." The following table summarizes entity specifiers:

<table>
<thead>
<tr>
<th>Specifier</th>
<th>Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All, including anonymous and authenticated users</td>
</tr>
<tr>
<td>anonymous</td>
<td>Anonymous (non-authenticated) users</td>
</tr>
<tr>
<td>users</td>
<td>Authenticated users</td>
</tr>
<tr>
<td>self</td>
<td>User associated with target entry</td>
</tr>
<tr>
<td>dn[.&lt;basic-style&gt;=&lt;regex&gt;]</td>
<td>Users matching a regular expression</td>
</tr>
<tr>
<td>dn.&lt;scope-style&gt;=&lt;DN&gt;</td>
<td>Users within scope of a DN</td>
</tr>
</tbody>
</table>

The DN specifier behaves much like <what> clause DN specifiers.

Other control factors are also supported. For example, a <who> can be restricted by an entry listed in a DN-valued attribute in the entry to which the access applies:

```plaintext
dnattr=<dn-valued attribute name>
```

The dnattr specification is used to give access to an entry whose DN is listed in an attribute of the entry (e.g., give access to a group entry to whoever is listed as the owner of the group entry).

Some factors may not be appropriate in all environments (or any). For example, the domain factor relies on IP to domain name lookups. As these can easily spoofed, the domain factor should not be avoided.
6.3.3. The access to grant

The kind of <access> granted can be one of the following:

Table 6.4: Access Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Privileges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>=0</td>
<td>no access</td>
</tr>
<tr>
<td>disclose</td>
<td>=d</td>
<td>needed for information disclosure on error</td>
</tr>
<tr>
<td>auth</td>
<td>=dx</td>
<td>needed to authenticate (bind)</td>
</tr>
<tr>
<td>compare</td>
<td>=cdx</td>
<td>needed to compare</td>
</tr>
<tr>
<td>search</td>
<td>=scdx</td>
<td>needed to apply search filters</td>
</tr>
<tr>
<td>read</td>
<td>=rscdx</td>
<td>needed to read search results</td>
</tr>
<tr>
<td>write</td>
<td>=wrscdx</td>
<td>needed to modify/rename</td>
</tr>
<tr>
<td>manage</td>
<td>=mwrscdx</td>
<td>needed to manage</td>
</tr>
</tbody>
</table>

Each level implies all lower levels of access. So, for example, granting someone write access to an entry also grants them read, search, compare, auth and disclose access. However, one may use the privileges specifier to grant specific permissions.

6.3.4. Access Control Evaluation

When evaluating whether some requester should be given access to an entry and/or attribute, slapd compares the entry and/or attribute to the <what> selectors given in the configuration file. For each entry, access controls provided in the database which holds the entry (or the first database if not held in any database) apply first, followed by the global access directives. Within this priority, access directives are examined in the order in which they appear in the config file. Slapd stops with the first <what> selector that matches the entry and/or attribute. The corresponding access directive is the one slapd will use to evaluate access.

Next, slapd compares the entity requesting access to the <who> selectors within the access directive selected above in the order in which they appear. It stops with the first <who> selector that matches the requester. This determines the access the entity requesting access has to the entry and/or attribute. The corresponding access directive is the one slapd will use to evaluate access.

Finally, slapd compares the access granted in the selected <access> clause to the access requested by the client. If it allows greater or equal access, access is granted. Otherwise, access is denied.

The order of evaluation of access directives makes their placement in the configuration file important. If one access directive is more specific than another in terms of the entries it selects, it should appear first in the config file. Similarly, if one <who> selector is more specific than another it should come first in the access directive. The access control examples given below should help make this clear.

6.3.5. Access Control Examples

The access control facility described above is quite powerful. This section shows some examples of its use for descriptive purposes.

A simple example:

access to * by * read
This access directive grants read access to everyone.

```
access to *
  by self write
  by anonymous auth
  by * read
```

This directive allows the user to modify their entry, allows anonymous to authentication against these entries, and allows all others to read these entries. Note that only the first by `<who>` clause which matches applies. Hence, the anonymous users are granted auth, not read. The last clause could just as well have been "by users read".

It is often desirable to restrict operations based upon the level of protection in place. The following shows how security strength factors (SSF) can be used.

```
access to *
  by ssf=128 self write
  by ssf=64 anonymous auth
  by ssf=64 users read
```

This directive allows users to modify their own entries if security protections have of strength 128 or better have been established, allows authentication access to anonymous users, and read access when 64 or better security protections have been established. If client has not establish sufficient security protections, the implicit by * none clause would be applied.

The following example shows the use of a style specifiers to select the entries by DN in two access directives where ordering is significant.

```
access to dn.children="dc=example,dc=com"
  by * search
access to dn.children="dc=com"
  by * read
```

Read access is granted to entries under the dc=com subtree, except for those entries under the dc=example,dc=com subtree, to which search access is granted. No access is granted to dc=com as neither access directive matches this DN. If the order of these access directives was reversed, the trailing directive would never be reached, since all entries under dc=example,dc=com are also under dc=com entries.

Also note that if no access to directive matches or no by `<who>` clause, access is denied. That is, every access to directive ends with an implicit by * none clause and every access list ends with an implicit access to * by * none directive.

The next example again shows the importance of ordering, both of the access directives and the by `<who>` clauses. It also shows the use of an attribute selector to grant access to a specific attribute and various `<who>` selectors.

```
access to dn.subtree="dc=example,dc=com" attrs=homePhone
  by self write
  by dn.children="dc=example,dc=com" search
  by peername.regex=IP:10\.+ read
access to dn.subtree="dc=example,dc=com"
  by self write
  by dn.children="dc=example,dc=com" search
```
This example applies to entries in the "dc=example,dc=com" subtree. To all attributes except homePhone, an entry can write to itself, entries under example.com entries can search by them, anybody else has no access (implicit by * none) excepting for authentication/authorization (which is always done anonymously). The homePhone attribute is writable by the entry, searchable by entries under example.com, readable by clients connecting from network 10, and otherwise not readable (implicit by * none). All other access is denied by the implicit access to * by * none.

Sometimes it is useful to permit a particular DN to add or remove itself from an attribute. For example, if you would like to create a group and allow people to add and remove only their own DN from the member attribute, you could accomplish it with an access directive like this:

```
access to attrs=member,entry
    by dnattr=member selfwrite
```

The dnattr <who> selector says that the access applies to entries listed in the member attribute. The selfwrite access selector says that such members can only add or delete their own DN from the attribute, not other values. The addition of the entry attribute is required because access to the entry is required to access any of the entry's attributes.

### 6.4. Configuration File Example

The following is an example configuration file, interspersed with explanatory text. It defines two databases to handle different parts of the X.500 tree: both are BDB database instances. The line numbers shown are provided for reference only and are not included in the actual file. First, the global configuration section:

```
1.    # example config file - global configuration section
2.    include /usr/local/etc/schema/core.schema
3.    referral ldap://root.openldap.org
4.    access to * by * read
```

Line 1 is a comment. Line 2 includes another config file which contains core schema definitions. The referral directive on line 3 means that queries not local to one of the databases defined below will be referred to the LDAP server running on the standard port (389) at the host root.openldap.org.

Line 4 is a global access control. It applies to all entries (after any applicable database-specific access controls).

The next section of the configuration file defines a BDB backend that will handle queries for things in the "dc=example,dc=com" portion of the tree. The database is to be replicated to two slave slapds, one on truelies, the other on judgmentday. Indices are to be maintained for several attributes, and the userPassword attribute is to be protected from unauthorized access.

```
5.    # BDB definition for the example.com
6.    database bdb
7.    suffix "dc=example,dc=com"
8.    directory /usr/local/var/openldap-data
9.    rootdn "cn=Manager,dc=example,dc=com"
10.   rootpw secret
11.   # indexed attribute definitions
12.   index uid pres,eq
13.   index cn,sn,uid pres,eq,approx,sub
```
Line 5 is a comment. The start of the database definition is marked by the database keyword on line 6. Line 7 specifies the DN suffix for queries to pass to this database. Line 8 specifies the directory in which the database files will live.

Lines 9 and 10 identify the database super-user entry and associated password. This entry is not subject to access control or size or time limit restrictions.

Lines 12 through 14 indicate the indices to maintain for various attributes.

Lines 16 through 24 specify access control for entries in this database. As this is the first database, the controls also apply to entries not held in any database (such as the Root DSE). For all applicable entries, the userPassword attribute is writable by the entry itself and by the "admin" entry. It may be used for authentication/authorization purposes, but is otherwise not readable. All other attributes are writable by the entry and the "admin" entry, but may be read by all users (authenticated or not).

The next section of the example configuration file defines another BDB database. This one handles queries involving the dc=example,dc=net subtree but is managed by the same entity as the first database. Note that without line 39, the read access would be allowed due to the global access rule at line 4.
7. Running slapd

`slapd`(8) is designed to be run as a standalone service. This allows the server to take advantage of caching, manage concurrency issues with underlying databases, and conserve system resources. Running from `inetd`(8) is **NOT** an option.

7.1. Command-Line Options

`slapd`(8) supports a number of command-line options as detailed in the manual page. This section details a few commonly used options.

- **-f <filename>**
  
  This option specifies an alternate configuration file for slapd. The default is normally `/usr/local/etc/openldap/slapd.conf`.

- **-F <slapd-config-directory>**
  
  Specifies the slapd configuration directory. The default is `/usr/local/etc/openldap/slapd.d`.

If both `-f` and `-F` are specified, the config file will be read and converted to config directory format and written to the specified directory. If neither option is specified, slapd will attempt to read the default config directory before trying to use the default config file. If a valid config directory exists then the default config file is ignored. All of the slap tools that use the config options observe this same behavior.

- **-h <URLs>**
  
  This option specifies alternative listener configurations. The default is `ldap://` which implies LDAP over TCP on all interfaces on the default LDAP port 389. You can specify specific host-port pairs or other protocol schemes (such as `ldaps://` or `ldapi://`). For example, `-h "ldaps://127.0.0.1:666"` will create two listeners: one for the (non-standard) `ldaps://` scheme on all interfaces on the default `ldaps://` port 636, and one for the standard `ldap://` scheme on the `localhost` (loopback) interface on port 666. Hosts may be specified using hostnames or IPv4 or IPv6 addresses. Port values must be numeric.

- **-n <service-name>**
  
  This option specifies the service name used for logging and other purposes. The default service name is slapd.

- **-l <syslog-local-user>**
  
  This option specifies the local user for the `syslog`(8) facility. Values can be `LOCAL0`, `LOCAL1`, `LOCAL2`, ..., and `LOCAL7`. The default is `LOCAL4`. This option may not be supported on all systems.

- **-u user -g group**
  
  These options specify the user and group, respectively, to run as. `<user>` can be either a user name or uid. `<group>` can be either a group name or gid.

- **-r directory**
This option specifies a run-time directory. slapd will `chroot(2)` to this directory after opening listeners but before reading any configuration files or initializing any backends.

```
-d <level> | ??
```

This option sets the slapd debug level to `<level>`. When level is a `?’ character, the various debugging levels are printed and slapd exits, regardless of any other options you give it. Current debugging levels are

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>enable all debugging</td>
</tr>
<tr>
<td>0</td>
<td>no debugging</td>
</tr>
<tr>
<td>1</td>
<td>trace function calls</td>
</tr>
<tr>
<td>2</td>
<td>debug packet handling</td>
</tr>
<tr>
<td>4</td>
<td>heavy trace debugging</td>
</tr>
<tr>
<td>8</td>
<td>connection management</td>
</tr>
<tr>
<td>16</td>
<td>print out packets sent and received</td>
</tr>
<tr>
<td>32</td>
<td>search filter processing</td>
</tr>
<tr>
<td>64</td>
<td>configuration file processing</td>
</tr>
<tr>
<td>128</td>
<td>access control list processing</td>
</tr>
<tr>
<td>256</td>
<td>stats log connections/operations/results</td>
</tr>
<tr>
<td>512</td>
<td>stats log entries sent</td>
</tr>
<tr>
<td>1024</td>
<td>print communication with shell backends</td>
</tr>
<tr>
<td>2048</td>
<td>print entry parsing debugging</td>
</tr>
</tbody>
</table>

You may enable multiple levels by specifying the debug option once for each desired level. Or, since debugging levels are additive, you can do the math yourself. That is, if you want to trace function calls and watch the config file being processed, you could set level to the sum of those two levels (in this case, `-d 65`). Or, you can let slapd do the math, (e.g. `-d 1 -d 64`). Consult `<ldap_log.h>` for more details.

**Note:** slapd must have been compiled with `-DLDAP_DEBUG` defined for any debugging information beyond the two stats levels to be available.

### 7.2. Starting slapd

In general, slapd is run like this:

```
/usr/local/libexec/slapd [<option>] *
```

where `/usr/local/libexec` is determined by `configure` and `<option>` is one of the options described above (or in `slapd(8)`). Unless you have specified a debugging level (including level 0), slapd will automatically fork and detach itself from its controlling terminal and run in the background.

### 7.3. Stopping slapd

To kill off `slapd(8)` safely, you should give a command like this
kill -INT `cat /usr/local/var/slapd.pid`

where /usr/local/var is determined by configure.

Killing slapd by a more drastic method may cause information loss or database corruption.
8. Database Creation and Maintenance Tools

This section tells you how to create a slapd database from scratch, and how to do trouble shooting if you run into problems. There are two ways to create a database. First, you can create the database on-line using LDAP. With this method, you simply start up slapd and add entries using the LDAP client of your choice. This method is fine for relatively small databases (a few hundred or thousand entries, depending on your requirements). This method works for database types which support updates.

The second method of database creation is to do it off-line using special utilities provided with slapd(8). This method is best if you have many thousands of entries to create, which would take an unacceptably long time using the LDAP method, or if you want to ensure the database is not accessed while it is being created. Note that not all database types support these utilities.

8.1. Creating a database over LDAP

With this method, you use the LDAP client of your choice (e.g., the ldapadd(1)) to add entries, just like you would once the database is created. You should be sure to set the following options in the configuration file before starting slapd(8).

```
suffix <dn>
```

As described in the General Database Directives section, this option defines which entries are to be held by this database. You should set this to the DN of the root of the subtree you are trying to create. For example:

```
suffix "dc=example,dc=com"
```

You should be sure to specify a directory where the index files should be created:

```
directory <directory>
```

For example:

```
directory /usr/local/var/openldap-data
```

You need to create this directory with appropriate permissions such that slapd can write to it.

You need to configure slapd so that you can connect to it as a directory user with permission to add entries. You can configure the directory to support a special super-user or root user just for this purpose. This is done through the following two options in the database definition:

```
rootdn <dn>
rootpw <passwd>
```

For example:

```
rootdn "cn=Manager,dc=example,dc=com"
rootpw secret
```

These options specify a DN and password that can be used to authenticate as the super-user entry of the database (i.e., the entry allowed to do anything). The DN and password specified here will always work, regardless of whether the entry named actually exists or has the password given. This solves the
chicken-and-egg problem of how to authenticate and add entries before any entries yet exist.

Finally, you should make sure that the database definition contains the index definitions you want:

\[
\text{index } \{<\text{attrlist}> \mid \text{default}\} \ [\text{pres,eq,approx,sub,none}]
\]

For example, to index the cn, sn, uid and objectClass attributes, the following index directives could be used:

\[
\text{index } \text{cn,sn,uid } \text{pres,eq,approx,sub} \\
\text{index objectClass eq}
\]

This would create presence, equality, approximate, and substring indices for the cn, sn, and uid attributes and an equality index for the objectClass attribute. Note that not all index types are available with all attribute types. See The slapd Configuration File section for more information on this option.

Once you have configured things to your liking, start up slapd, connect with your LDAP client, and start adding entries. For example, to add an organization entry and an organizational role entry using the \textit{ldapadd} tool, you could create an LDIF file called \textit{entries.ldif} with the contents:

\begin{verbatim}
# Organization for Example Corporation
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
dc: example
o: Example Corporation
description: The Example Corporation

# Organizational Role for Directory Manager
dn: cn=Manager,dc=example,dc=com
objectClass: organizationalRole
cn: Manager
description: Directory Manager
\end{verbatim}

and then use a command like this to actually create the entry:

\[
\text{ldapadd -f entries.ldif -x -D "cn=Manager,dc=example,dc=com" -w secret}
\]

The above command assumes settings provided in the above examples.

\section*{8.2. Creating a database off-line}

The second method of database creation is to do it off-line, using the slapd database tools described below. This method is best if you have many thousands of entries to create, which would take an unacceptably long time to add using the LDAP method described above. These tools read the slapd configuration file and an input file containing a text representation of the entries to add. For database types which support the tools, they produce the database files directly (otherwise you must use the on-line method above). There are several important configuration options you will want to be sure and set in the config file database definition first:

\[
\text{suffix } \text{<dn>}
\]

As described in the General Database Directives section, this option defines which entries are to be held by this database. You should set this to the DN of the root of the subtree you are trying to create. For example:
8.2.1. The slapadd program

Once you’ve configured things to your liking, you create the primary database and associated indices by running the `slapadd(8)` program:

```
slapadd -l <inputfile> -f <slapdconfigfile>
    [-d <debuglevel>] [-n <integer>|-b <suffix>]
```

The arguments have the following meanings:

- `-l <inputfile>`
  Specifies the LDIF input file containing the entries to add in text form (described below in the The LDIF text entry format section).

- `-f <slapdconfigfile>`
  Specifies the slapd configuration file that tells where to create the indices, what indices to create, etc.

- `-F <slapdconfdirectory>`
  Specifies a config directory. If both `-f` and `-F` are specified, the config file will be read and converted to config directory format and written to the specified directory. If neither option is specified, an attempt to read the default config directory will be made before trying to use the default config file. If a valid config directory exists then the default config file is ignored. If dryrun mode is also specified, no conversion will occur.

- `-d <debuglevel>`
  Turn on debugging, as specified by `<debuglevel>`. The debug levels are the same as for slapd. See the Command-Line Options section in Running slapd.
An optional argument that specifies which database to modify. The first database listed in the configuration file is 1, the second 2, etc. By default, the first database in the configuration file is used. Should not be used in conjunction with \(-b\).

\[-n <databasenumber>\]

An optional argument that specifies which database to modify. The provided suffix is matched against a database suffix directive to determine the database number. Should not be used in conjunction with \(-n\).

\[-b <suffix>\]

8.2.2. The \textit{slapindex} program

Sometimes it may be necessary to regenerate indices (such as after modifying \textit{slapd.conf}(5)). This is possible using the \textit{slapindex}(8) program. \textit{slapindex} is invoked like this:

\[
\text{slapindex} \ -f \ \text{<slapdconfigfile>} \\
\quad \quad \quad \quad [-d \ <\text{debuglevel}>] \ [-n \ <\text{databasenumber}>|-b \ <\text{suffix}>]
\]

Where the \(-f\), \(-d\), \(-n\) and \(-b\) options are the same as for the \textit{slapadd}(1) program. \textit{slapindex} rebuilds all indices based upon the current database contents.

8.2.3. The \textit{slapcat} program

The \textit{slapcat} program is used to dump the database to an LDIF file. This can be useful when you want to make a human-readable backup of your database or when you want to edit your database off-line. The program is invoked like this:

\[
\text{slapcat} \ -l \ <\text{filename}> \ -f \ \text{<slapdconfigfile>} \\
\quad \quad \quad \quad [-d \ <\text{debuglevel}>] \ [-n \ <\text{databasenumber}>|-b \ <\text{suffix}>]
\]

where \(-n\) or \(-b\) is used to select the database in the \textit{slapd.conf}(5) specified using \(-f\). The corresponding LDIF output is written to standard output or to the file specified using the \(-l\) option.

8.3. The LDIF text entry format

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format. This section provides a brief description of the LDIF entry format which complements \textit{ldif}(5) and the technical specification RFC2849.

The basic form of an entry is:

\[
\# \ \text{comment} \\
\text{dn: <distinguished name>} \\
<\text{attrdesc}: <attrvalue}> \\
<\text{attrdesc}: <attrvalue}> \\
\ldots
\]

Lines starting with a '#' character are comments. An attribute description may be a simple attribute type like \texttt{cn} or \texttt{objectClass} or 1.2.3 (an OID associated with an attribute type) or may include options such as \texttt{cn;lang_en_US} or \texttt{userCertificate;binary}. 66
A line may be continued by starting the next line with a single space or tab character. For example:

```
     dn: cn=Barbara J Jensen,dc=example,dc=com
     cn: Barbara J Jensen
```

is equivalent to:

```
     dn: cn=Barbara J Jensen,dc=example,dc=com
     cn: Barbara J Jensen
```

Multiple attribute values are specified on separate lines. For example:

```
     cn: Barbara J Jensen
     cn: Babs Jensen
```

If an `<attribvalue>` contains non-printing characters or begins with a space, a colon (`:`), or a less than (`<`), the `<attrdesc>` is followed by a double colon and the base64 encoding of the value. For example, the value "begins with a space" would be encoded like this:

```
     cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

You can also specify a URL containing the attribute value. For example, the following specifies the `jpegPhoto` value should be obtained from the file `/path/to/file.jpeg`.

```
     cn:< file:///path/to/file.jpeg
```

Multiple entries within the same LDIF file are separated by blank lines. Here's an example of an LDIF file containing three entries.

```
# Barbara's Entry
     dn: cn=Barbara J Jensen,dc=example,dc=com
     cn: Barbara J Jensen
     cn: Babs Jensen
     objectClass: person
     sn: Jensen

# Bjorn's Entry
     dn: cn=Bjorn J Jensen,dc=example,dc=com
     cn: Bjorn J Jensen
     cn: Bjorn Jensen
     objectClass: person
     sn: Jensen
# Base64 encoded JPEG photo
     jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
     A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFx0Q
     ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxLz2F/2wBDAESEhqVG

# Jennifer's Entry
     dn: cn=Jennifer J Jensen,dc=example,dc=com
     cn: Jennifer J Jensen
     cn: Jennifer Jensen
     objectClass: person
     sn: Jensen
# JPEG photo from file
     jpegPhoto:< file:///path/to/file.jpeg
```
Notice that the `jpegPhoto` in Bjorn's entry is base 64 encoded and the `jpegPhoto` in Jennifer's entry is obtained from the location indicated by the URL.

**Note:** Trailing spaces are not trimmed from values in an LDIF file. Nor are multiple internal spaces compressed. If you don't want them in your data, don't put them there.
9. Backends

9.1. Berkeley DB Backends

9.1.1. Overview

The bdb backend to slapd(8) is the recommended primary backend for a normal slapd database. It uses the Oracle Berkeley DB (BDB) package to store data. It makes extensive use of indexing and caching (see the Tuning section) to speed data access.

hdb is a variant of the bdb backend that uses a hierarchical database layout which supports subtree renames. It is otherwise identical to the bdb behavior, and all the same configuration options apply.

Note: An hdb database needs a large idlcachesize for good search performance, typically three times the cachesize (entry cache size) or larger.

9.1.2. back-bdb/back-hdb Configuration

MORE LATER

9.1.3. Further Information

slapd-bdb(5)

9.2. LDAP

9.2.1. Overview

The LDAP backend to slapd(8) is not an actual database; instead it acts as a proxy to forward incoming requests to another LDAP server. While processing requests it will also chase referrals, so that referrals are fully processed instead of being returned to the slapd client.

Sessions that explicitly Bind to the back-ldap database always create their own private connection to the remote LDAP server. Anonymous sessions will share a single anonymous connection to the remote server. For sessions bound through other mechanisms, all sessions with the same DN will share the same connection. This connection pooling strategy can enhance the proxy’s efficiency by reducing the overhead of repeatedly making/breaking multiple connections.

The ldap database can also act as an information service, i.e. the identity of locally authenticated clients is asserted to the remote server, possibly in some modified form. For this purpose, the proxy binds to the remote server with some administrative identity, and, if required, authorizes the asserted identity.

9.2.2. back-ldap Configuration

LATER
9.2.3. Further Information

slapd-ldap(5)

9.3. LDIF

9.3.1. Overview

The LDIF backend to slapd(8) is a basic storage backend that stores entries in text files in LDIF format, and exploits the filesystem to create the tree structure of the database. It is intended as a cheap, low performance easy to use backend.

When using the cn=config dynamic configuration database with persistent storage, the configuration data is stored using this backend. See slapd-config(5) for more information.

9.3.2. back-ldif Configuration

LATER

9.3.3. Further Information

slapd-ldif(5)

9.4. Metadirectory

9.4.1. Overview

The meta backend to slapd(8) performs basic LDAP proxying with respect to a set of remote LDAP servers, called "targets". The information contained in these servers can be presented as belonging to a single Directory Information Tree (DIT).

A basic knowledge of the functionality of the slapd-ldap(5) backend is recommended. This backend has been designed as an enhancement of the ldap backend. The two backends share many features (actually they also share portions of code). While the ldap backend is intended to proxy operations directed to a single server, the meta backend is mainly intended for proxying of multiple servers and possibly naming context masquerading.

These features, although useful in many scenarios, may result in excessive overhead for some applications, so its use should be carefully considered.

9.4.2. back-meta Configuration

LATER

9.4.3. Further Information

slapd-meta(5)
9.5. Monitor

9.5.1. Overview

The monitor backend to `slapd(8)` is not an actual database; if enabled, it is automatically generated and dynamically maintained by `slapd` with information about the running status of the daemon.

To inspect all monitor information, issue a subtree search with base `cn=Monitor`, requesting that attributes "+" and "*" are returned. The monitor backend produces mostly operational attributes, and LDAP only returns operational attributes that are explicitly requested. Requesting attribute "+" is an extension which requests all operational attributes.

See the Monitoring section.

9.5.2. `back-monitor` Configuration

LATER

9.5.3. Further Information

`slapd-monitor(5)`

9.6. Null

9.6.1. Overview

The Null backend to `slapd(8)` is surely the most useful part of `slapd`:

- Searches return success but no entries.
- Compares return `compareFalse`.
- Updates return success (unless `readonly` is on) but do nothing.
- Binds other than as the rootdn fail unless the database option "bind on" is given.
- The `slapadd(8)` and `slapcat(8)` tools are equally exciting.

Inspired by the `/dev/null` device.

9.6.2. `back-null` Configuration

LATER

9.6.3. Further Information

`slapd-null(5)`

9.7. Passwd
9.7.1. Overview

The PASSWD backend to *slapd*(8) serves up the user account information listed in the system *passwd*(5) file.

This backend is provided for demonstration purposes only. The DN of each entry is "uid=<username>,<suffix>".

9.7.2. back-passwd Configuration

LATER

9.7.3. Further Information

*sldap-passwd*(5)

9.8. Perl/Shell

9.8.1. Overview

The Perl backend to *slapd*(8) works by embedding a *perl*(1) interpreter into *slapd*(8). Any perl database section of the configuration file *slapd.conf*(5) must then specify what Perl module to use. Slapd then creates a new Perl object that handles all the requests for that particular instance of the backend.

The Shell backend to *slapd*(8) executes external programs to implement operations, and is designed to make it easy to tie an existing database to the slapd front-end. This backend is primarily intended to be used in prototypes.

9.8.2. back-perl/back-shell Configuration

LATER

9.8.3. Further Information

*sldap-shell*(5) and *slapd-perl*(5)

9.9. Relay

9.9.1. Overview

The primary purpose of this *slapd*(8) backend is to map a naming context defined in a database running in the same *slapd*(8) instance into a virtual naming context, with attributeType and objectClass manipulation, if required. It requires the rwm overlay.

This backend and the above mentioned overlay are experimental.
9.9.2. back-relay Configuration

LATER

9.9.3. Further Information

slapd-relay(5)

9.10. SQL

9.10.1. Overview

The primary purpose of this slapd(8) backend is to PRESENT information stored in some RDBMS as an LDAP subtree without any programming (some SQL and maybe stored procedures can’t be considered programming, anyway ;).

That is, for example, when you (some ISP) have account information you use in an RDBMS, and want to use modern solutions that expect such information in LDAP (to authenticate users, make email lookups etc.). Or you want to synchronize or distribute information between different sites/applications that use RDBMSes and/or LDAP. Or whatever else...

It is NOT designed as a general-purpose backend that uses RDBMS instead of BerkeleyDB (as the standard BDB backend does), though it can be used as such with several limitations. Please see LDAP vs RDBMS for discussion.

The idea is to use some meta-information to translate LDAP queries to SQL queries, leaving relational schema untouched, so that old applications can continue using it without any modifications. This allows SQL and LDAP applications to interoperate without replication, and exchange data as needed.

The SQL backend is designed to be tunable to virtually any relational schema without having to change source (through that meta-information mentioned). Also, it uses ODBC to connect to RDBMSes, and is highly configurable for SQL dialects RDBMSes may use, so it may be used for integration and distribution of data on different RDBMSes, OSes, hosts etc., in other words, in highly heterogeneous environment.

This backend is experimental.

9.10.2. back-sql Configuration

LATER

9.10.3. Further Information

slapd-sql(5)
10. Overlays

Overlays are software components that provide hooks to functions analogous to those provided by backends, which can be stacked on top of the backend calls and as callbacks on top of backend responses to alter their behavior.

Overlays may be compiled statically into slapd, or when module support is enabled, they may be dynamically loaded. Most of the overlays are only allowed to be configured on individual databases, but some may also be configured globally.

Essentially they represent a means to:

- customize the behavior of existing backends without changing the backend code and without requiring one to write a new custom backend with complete functionality
- write functionality of general usefulness that can be applied to different backend types

Overlays are usually documented by separate specific man pages in section 5; the naming convention is

\text{slapo-<overlay name>}

Not all distributed overlays have a man page yet. Feel free to contribute one, if you think you well understood the behavior of the component and the implications of all the related configuration directives.

Official overlays are located in

\text{servers/slapd/overlays/}

That directory also contains the file slapover.txt, which describes the rationale of the overlay implementation, and may serve as guideline for the development of custom overlays.

Contribware overlays are located in

\text{contrib/slapd-modules/<overlay name>/}

along with other types of run-time loadable components; they are officially distributed, but not maintained by the project.

They can be stacked on the frontend as well; this means that they can be executed after a request is parsed and validated, but right before the appropriate database is selected. The main purpose is to affect operations regardless of the database they will be handled by, and, in some cases, to influence the selection of the database by massaging the request DN.

All the current overlays in 2.4 are listed and described in detail in the following sections.

10.1. Access Logging

10.1.1. Overview

This overlay can record accesses to a given backend database on another database.
10.1.2. Access Logging Configuration

10.2. Audit Logging

This overlay records changes on a given backend database to an LDIF log file.

10.2.1. Overview

10.2.2. Audit Logging Configuration

10.3. Chaining

10.3.1. Overview

The chain overlay provides basic chaining capability to the underlying database.

What is chaining? It indicates the capability of a DSA to follow referrals on behalf of the client, so that distributed systems are viewed as a single virtual DSA by clients that are otherwise unable to "chase" (i.e. follow) referrals by themselves.

The chain overlay is built on top of the ldap backend; it is compiled by default when --enable-ldap.

10.3.2. Chaining Configuration

In order to demonstrate how this overlay works, we shall discuss a typical scenario which might be one master server and three Syncrepl slaves.

On each replica, add this near the top of the file (global), before any database definitions:

```
overlay                    chain
chain-uri                  "ldap://ldapmaster.example.com"
chain-ldassert-bind        bindmethod="simple"
                          binddn="cn=Manager,dc=example,dc=com"
                          credentials="<secret>"
                          mode="self"
chain-tls                  start
chain-return-error         TRUE
```

Add this below your `syncrepl` statement:

```
updateref                  "ldap://ldapmaster.example.com/"
```

The `chain-tls` statement enables TLS from the slave to the ldap master. The DITs are exactly the same between these machines, therefore whatever user bound to the slave will also exist on the master. If that DN does not have update privileges on the master, nothing will happen.

You will need to restart the slave after these changes. Then, if you are using `loglevel 256`, you can monitor an `ldapmodify` on the slave and the master.

Now start an `ldapmodify` on the slave and watch the logs. You should expect something like:
And on the master you will see this:

Note: You can clearly see the PROXYAUTHZ line on the master, indicating the proper identity assertion for the update on the master. Also note the slave immediately receiving the Syncrepl update from the master.

10.3.3. Handling Chaining Errors

By default, if chaining fails, the original referral is returned to the client under the assumption that the client might want to try and follow the referral.

With the following directive however, if the chaining fails at the provider side, the actual error is returned to the client.

    chain-return-error TRUE

10.4. Constraints

10.4.1. Overview

This overlay enforces a regular expression constraint on all values of specified attributes. It is used to enforce a more rigorous syntax when the underlying attribute syntax is too general.

10.4.2. Constraint Configuration

10.5. Dynamic Directory Services

10.5.1. Overview

This overlay supports dynamic objects, which have a limited life after which they expire and are automatically deleted.
10.5.2. Dynamic Directory Service Configuration

10.6. Dynamic Groups

10.6.1. Overview

This overlay extends the Compare operation to detect members of a dynamic group. This overlay is now deprecated as all of its functions are available using the Dynamic Lists overlay.

10.6.2. Dynamic Group Configuration

10.7. Dynamic Lists

10.7.1. Overview

This overlay allows expansion of dynamic groups and more.

10.7.2. Dynamic List Configuration

10.8. Reverse Group Membership Maintenance

10.8.1. Overview

In some scenarios, it may be desirable for a client to be able to determine which groups an entry is a member of, without performing an additional search. Examples of this are applications using the DIT for access control based on group authorization.

The memberof overlay updates an attribute (by default memberOf) whenever changes occur to the membership attribute (by default member) of entries of the objectclass (by default groupOfNames) configured to trigger updates.

Thus, it provides maintenance of the list of groups an entry is a member of, when usual maintenance of groups is done by modifying the members on the group entry.

10.8.2. Member Of Configuration

The typical use of this overlay requires just enabling the overlay for a specific database. For example, with the following minimal slapd.conf:

```
include /usr/share/openldap/schema/core.schema
include /usr/share/openldap/schema/cosine.schema
modulepath /usr/lib/openldap
moduleload memberof.la
authz-regexp "gidNumber=0\\ uidNumber=0, cn=peercred, cn=external, cn=auth"
  "cn=Manager, dc=example, dc=com"
database bdb
suffix "dc=example, dc=com"
rootdn "cn=Manager, dc=example, dc=com"
rootpw secret
directory /var/lib/ldap
```
Results in the following output from a search on the test1 user:

# ldapsearch -LL -Y EXTERNAL -H ldapi:/// "(uid=test1)" -b dc=example,dc=com memberOf
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
version: 1

   dn: uid=test1,ou=People,dc=example,dc=com
   memberOf: cn=testgroup,ou=Group,dc=example,dc=com

Note that the **memberOf** attribute is an operational attribute, so it must be requested explicitly.

### 10.9. The Proxy Cache Engine

LDAP servers typically hold one or more subtrees of a DIT. Replica (or shadow) servers hold shadow copies of entries held by one or more master servers. Changes are propagated from the master server to replica (slave) servers using LDAP Sync replication. An LDAP cache is a special type of replica which holds entries corresponding to search filters instead of subtrees.

#### 10.9.1. Overview

The proxy cache extension of slapd is designed to improve the responsiveness of the ldap and meta backends. It handles a search request (query) by first determining whether it is contained in any cached search filter. Contained requests are answered from the proxy cache's local database. Other requests are passed on to the underlying ldap or meta backend and processed as usual.
E.g. (shoesize>=9) is contained in (shoesize>=8) and (sn=Richardson) is contained in (sn=Richards*)

Correct matching rules and syntaxes are used while comparing assertions for query containment. To simplify the query containment problem, a list of cacheable “templates” (defined below) is specified at configuration time. A query is cached or answered only if it belongs to one of these templates. The entries corresponding to cached queries are stored in the proxy cache local database while its associated meta information (filter, scope, base, attributes) is stored in main memory.

A template is a prototype for generating LDAP search requests. Templates are described by a prototype search filter and a list of attributes which are required in queries generated from the template. The representation for prototype filter is similar to RFC4515, except that the assertion values are missing. Examples of prototype filters are: (sn=),(&(sn=)(givenname=)) which are instantiated by search filters (sn=Doe) and (&(sn=Doe)(givenname=John)) respectively.

The cache replacement policy removes the least recently used (LRU) query and entries belonging to only that query. Queries are allowed a maximum time to live (TTL) in the cache thus providing weak consistency. A background task periodically checks the cache for expired queries and removes them.

The Proxy Cache paper (http://www.openldap.org/pub/kapurva/proxycaching.pdf) provides design and implementation details.

10.9.2. Proxy Cache Configuration

The cache configuration specific directives described below must appear after a overlay proxycache directive within a "database meta" or database ldap section of the server's slapd.conf(5) file.

10.9.2.1. Setting cache parameters

proxyCache <DB> <maxentries> <nattrsets> <entrylimit> <period>

This directive enables proxy caching and sets general cache parameters. The <DB> parameter specifies which underlying database is to be used to hold cached entries. It should be set to bdb or hdb. The <maxentries> parameter specifies the total number of entries which may be held in the cache. The <nattrsets> parameter specifies the total number of attribute sets (as specified by the proxyAttrSet directive) that may be defined. The <entrylimit> parameter specifies the maximum number of entries in a cacheable query. The <period> specifies the consistency check period (in seconds). In each period, queries with expired TTLs are removed.

10.9.2.2. Defining attribute sets

proxyAttrset <index> <attrs...>

Used to associate a set of attributes to an index. Each attribute set is associated with an index number from 0 to <numattrsets>-1. These indices are used by the proxyTemplate directive to define cacheable templates.

10.9.2.3. Specifying cacheable templates

proxyTemplate <prototype_string> <attrset_index> <TTL>
 Specifies a cacheable template and the "time to live" (in sec) <TTL> for queries belonging to the template. A template is described by its prototype filter string and set of required attributes identified by <attrset_index>.

**10.9.2.4. Example**

An example *slapd.conf*(5) database section for a caching server which proxies for the "dc=example,dc=com" subtree held at server ldap.example.com.

```
database        ldap
suffix          "dc=example,dc=com"
rootdn          "dc=example,dc=com"
uri             ldap://ldap.example.com/dc=example%2cdc=com
overlay proxycache
proxycache    bdb 100000 1 1000 100
proxyAttrset 0 mail postaladdress telephonenumber
proxyTemplate (sn=) 0 3600
proxyTemplate (&(sn=)(givenName=)) 0 3600
proxyTemplate (&(departmentNumber=)(secretary=*)) 0 3600

```
cachesize 20
directory ./testrun/db.2.a
index     objectClass eq
index     cn,sn,uid,mail pres,eq,sub

**10.9.2.4.1. Cacheable Queries**

A LDAP search query is cacheable when its filter matches one of the templates as defined in the "proxyTemplate" statements and when it references only the attributes specified in the corresponding attribute set. In the example above the attribute set number 0 defines that only the attributes: mail postaladdress telephonenumber are cached for the following proxyTemplates.

**10.9.2.4.2. Examples:**

Filter: (&(sn=Richard*)(givenName=jack))
Attrs: mail telephoneNumber

is cacheable, because it matches the template (&(sn=)(givenName=)) and its attributes are contained in proxyAttrset 0.

Filter: (&(sn=Richard*)(telephoneNumber))
Attrs: givenName

is not cacheable, because the filter does not match the template, nor is the attribute givenName stored in the cache

Filter: (|(sn=Richard*)(givenName=jack))
Attrs: mail telephoneNumber

is not cacheable, because the filter does not match the template ( logical OR "|") condition instead of logical AND "&")

**10.10. Password Policies**
10.10.1. Overview

This overlay provides a variety of password control mechanisms, e.g. password aging, password reuse and duplication control, mandatory password resets, etc.

10.10.2. Password Policy Configuration

10.11. Referential Integrity

10.11.1. Overview

This overlay can be used with a backend database such as slapd-bdb (5) to maintain the cohesiveness of a schema which utilizes reference attributes.

10.11.2. Referential Integrity Configuration

10.12. Return Code

10.12.1. Overview

This overlay is useful to test the behavior of clients when server-generated erroneous and/or unusual responses occur.

10.12.2. Return Code Configuration

10.13. Rewrite/Remap

10.13.1. Overview

It performs basic DN/data rewrite and objectClass/attributeType mapping.

10.13.2. Rewrite/Remap Configuration

10.14. Sync Provider

10.14.1. Overview

This overlay implements the provider-side support for syncrepl replication, including persistent search functionality

10.14.2. Sync Provider Configuration

10.15. Translucent Proxy
10.15.1. Overview

This overlay can be used with a backend database such as slapd-bdb (5) to create a "translucent proxy". Content of entries retrieved from a remote LDAP server can be partially overridden by the database.

10.15.2. Translucent Proxy Configuration

10.16. Attribute Uniqueness

10.16.1. Overview

This overlay can be used with a backend database such as slapd-bdb (5) to enforce the uniqueness of some or all attributes within a subtree.

10.16.2. Attribute Uniqueness Configuration

10.17. Value Sorting

10.17.1. Overview

This overlay can be used to enforce a specific order for the values of an attribute when it is returned in a search.

10.17.2. Value Sorting Configuration

10.18. Overlay Stacking

10.18.1. Overview

10.18.2. Example Scenarios

10.18.2.1. Samba
11. Schema Specification

This chapter describes how to extend the user schema used by `slapd(8)`. The chapter assumes the reader is familiar with the LDAP/X.500 information model.

The first section, Distributed Schema Files, details optional schema definitions provided in the distribution and where to obtain other definitions. The second section, Extending Schema, details how to define new schema items.

This chapter does not discuss how to extend system schema used by `slapd(8)` as this requires source code modification. System schema includes all operational attribute types or any object class which allows or requires an operational attribute (directly or indirectly).

### 11.1. Distributed Schema Files

OpenLDAP Software is distributed with a set of schema specifications for your use. Each set is defined in a file suitable for inclusion (using the `include` directive) in your `slapd.conf(5)` file. These schema files are normally installed in the `/usr/local/etc/openldap/schema` directory.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>core.schema</td>
<td>OpenLDAP core (required)</td>
</tr>
<tr>
<td>cosine.schema</td>
<td>Cosine and Internet X.500 (useful)</td>
</tr>
<tr>
<td>inetorgperson.schema</td>
<td>InetOrgPerson (useful)</td>
</tr>
<tr>
<td>misc.schema</td>
<td>Assorted (experimental)</td>
</tr>
<tr>
<td>nis.schema</td>
<td>Network Information Services (FYI)</td>
</tr>
<tr>
<td>openldap.schema</td>
<td>OpenLDAP Project (experimental)</td>
</tr>
</tbody>
</table>

To use any of these schema files, you only need to include the desired file in the global definitions portion of your `slapd.conf(5)` file. For example:

```bash
# include schema
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
```

Additional files may be available. Please consult the OpenLDAP FAQ (http://www.openldap.org/faq/).

**Note:** You should not modify any of the schema items defined in provided files.

### 11.2. Extending Schema

Schema used by `slapd(8)` may be extended to support additional syntaxes, matching rules, attribute types, and object classes. This chapter details how to add user application attribute types and object classes using the syntaxes and matching rules already supported by slapd. slapd can also be extended to support additional syntaxes, matching rules and system schema, but this requires some programming and hence is not discussed here.
There are five steps to defining new schema:

1. obtain Object Identifier
2. choose a name prefix
3. create local schema file
4. define custom attribute types (if necessary)
5. define custom object classes

### 11.2.1. Object Identifiers

Each schema element is identified by a globally unique Object Identifier (OID). OIDs are also used to identify other objects. They are commonly found in protocols described by ASN.1. In particular, they are heavily used by the Simple Network Management Protocol (SNMP). As OIDs are hierarchical, your organization can obtain one OID and branch it as needed. For example, if your organization were assigned OID 1.1, you could branch the tree as follows:

<table>
<thead>
<tr>
<th>OID</th>
<th>Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Organization's OID</td>
</tr>
<tr>
<td>1.1.1</td>
<td>SNMP Elements</td>
</tr>
<tr>
<td>1.1.2</td>
<td>LDAP Elements</td>
</tr>
<tr>
<td>1.1.2.1</td>
<td>AttributeTypes</td>
</tr>
<tr>
<td>1.1.2.1.1</td>
<td>x-my-Attribute</td>
</tr>
<tr>
<td>1.1.2.2</td>
<td>ObjectClasses</td>
</tr>
<tr>
<td>1.1.2.2.1</td>
<td>x-my-ObjectClass</td>
</tr>
</tbody>
</table>

You are, of course, free to design a hierarchy suitable to your organizational needs under your organization's OID. No matter what hierarchy you choose, you should maintain a registry of assignments you make. This can be a simple flat file or something more sophisticated such as the OpenLDAP OID Registry (http://www.openldap.org/faq/index.cgi?file=197).

For more information about Object Identifiers (and a listing service) see http://www.alvestrand.no/harald/objectid/.

*Under no circumstances should you hijack OID namespace!*

To obtain a registered OID at no cost, apply for a OID under the Internet Assigned Numbers Authority (ORG:IANA) maintained Private Enterprise arc. Any private enterprise (organization) may request a Private Enterprise Number (PEN) to be assigned under this arc. Just fill out the IANA form at http://pen.iana.org/pen/PenApplication.page and your official PEN will be sent to you usually within a few days. Your base OID will be something like 1.3.6.1.4.1.X where X is an integer.

---

**Note:** PENs obtained using this form may be used for any purpose including identifying LDAP schema elements.

Alternatively, OID name space may be available from a national authority (e.g., ANSI, BSI).
11.2.2. Naming Elements

In addition to assigning a unique object identifier to each schema element, you should provide a least one
textual name for each element. Names should be registered with the IANA or prefixed with "x-" to place in
the "private use" name space.

The name should be both descriptive and not likely to clash with names of other schema elements. In
particular, any name you choose should not clash with present or future Standard Track names (this is assured
if you registered names or use names beginning with "x-").

It is noted that you can obtain your own registered name prefix so as to avoid having to register your names
individually. See RFC4520 for details.

In the examples below, we have used a short prefix 'x-my-'. Such a short prefix would only be suitable for a
very large, global organization. In general, we recommend something like 'x-de-Firm-' (German company)
or 'x-com-Example' (elements associated with organization associated with example.com).

11.2.3. Local schema file

The objectclass and attributeTypes configuration file directives can be used to define schema rules
on entries in the directory. It is customary to create a file to contain definitions of your custom schema items.
We recommend you create a file local.schema in
/usr/local/etc/openldap/schema/local.schema and then include this file in your
slapd.conf(5) file immediately after other schema include directives.

```
#include schema
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
#include local.schema
include /usr/local/etc/openldap/schema/local.schema
```

11.2.4. Attribute Type Specification

The attributetype directive is used to define a new attribute type. The directive uses the same Attribute Type
Description (as defined in RFC4512) used by the attributeTypes attribute found in the subschema subentry,
e.g.:

```
attributetype <RFC4512 Attribute Type Description>
```

where Attribute Type Description is defined by the following ABNF:

```
AttributeTypeDescription = "(" whsp
    numericoid whsp ; AttributeType identifier
    [ "NAME" qdescrs ] ; name used in AttributeType
    [ "DESC" qdstring ] ; description
    [ "OBSOLETE" whsp ]
    [ "SUP" woid ] ; derived from this other
    [ "EQUALITY" woid ] ; Matching Rule name
    [ "ORDERING" woid ] ; Matching Rule name
    [ "SUBSTR" woid ] ; Matching Rule name
    [ "SYNTAX" whsp noidlen whsp ] ; Syntax OID
```
where whsp is a space (' '), numericoid is a globally unique OID in dotted-decimal form (e.g. 1.1.0), qdescrs is one or more names, woid is either the name or OID optionally followed by a length specifier (e.g. {10}).

For example, the attribute types name and cn are defined in core.schema as:

```
attributeType ( 2.5.4.41 NAME 'name'
   DESC 'name(s) associated with the object'
   EQUALITY caseIgnoreMatch
   SUBSTR caseIgnoreSubstringsMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
attributeType ( 2.5.4.3 NAME ( 'cn' 'commonName' )
   DESC 'common name(s) associated with the object'
   SUP name )
```

Notice that each defines the attribute's OID, provides a short name, and a brief description. Each name is an alias for the OID. slapd(8) returns the first listed name when returning results.

The first attribute, name, holds values of directoryString (UTF-8 encoded Unicode) syntax. The syntax is specified by OID (1.3.6.1.4.1.1466.115.121.1.15 identifies the directoryString syntax). A length recommendation of 32768 is specified. Servers should support values of this length, but may support longer values. The field does NOT specify a size constraint, so is ignored on servers (such as slapd) which don’t impose such size limits. In addition, the equality and substring matching uses case ignore rules. Below are tables listing commonly used syntax and matching rules (slapd(8) supports these and many more).

### Table 8.3: Commonly Used Syntaxes

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boolean</td>
<td>1.3.6.1.4.1.1466.115.121.1.7</td>
<td>boolean value</td>
</tr>
<tr>
<td>directoryString</td>
<td>1.3.6.1.4.1.1466.115.121.1.15</td>
<td>Unicode (UTF-8) string</td>
</tr>
<tr>
<td>distinguishedName</td>
<td>1.3.6.1.4.1.1466.115.121.1.12</td>
<td>LDAP DN</td>
</tr>
<tr>
<td>integer</td>
<td>1.3.6.1.4.1.1466.115.121.1.27</td>
<td>integer</td>
</tr>
<tr>
<td>numericString</td>
<td>1.3.6.1.4.1.1466.115.121.1.36</td>
<td>numeric string</td>
</tr>
<tr>
<td>OID</td>
<td>1.3.6.1.4.1.1466.115.121.1.38</td>
<td>object identifier</td>
</tr>
<tr>
<td>octetString</td>
<td>1.3.6.1.4.1.1466.115.121.1.40</td>
<td>arbitrary octets</td>
</tr>
</tbody>
</table>

### Table 8.4: Commonly Used Matching Rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
The second attribute, \texttt{cn}, is a subtype of \texttt{name} hence it inherits the syntax, matching rules, and usage of \texttt{name}. \texttt{commonName} is an alternative name.

Neither attribute is restricted to a single value. Both are meant for usage by user applications. Neither is obsolete nor collective.

The following subsections provide a couple of examples.

\subsection*{11.2.4.1. x-my-UniqueName}

Many organizations maintain a single unique name for each user. Though one could use \texttt{displayName} (RFC2798), this attribute is really meant to be controlled by the user, not the organization. We could just copy the definition of \texttt{displayName} from \texttt{inetorgperson.schema} and replace the OID, name, and description, e.g:

\begin{verbatim}
attributetype ( 1.1.2.1.1 NAME 'x-my-UniqueName'
    DESC 'unique name with my organization'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )
\end{verbatim}

However, if we want this name to be used in \texttt{name} assertions, e.g. \texttt{(name=*Jane*)}, the attribute could alternatively be defined as a subtype of \texttt{name}, e.g:

\begin{verbatim}
attributetype ( 1.1.2.1.1 NAME 'x-my-UniqueName'
    DESC 'unique name with my organization'
    SUP name )
\end{verbatim}
11.2.4.2. x-my-Photo

Many organizations maintain a photo of each user. A x-my-Photo attribute type could be defined to hold a photo. Of course, one could use just use jpegPhoto (RFC2798) (or a subtype) to hold the photo. However, you can only do this if the photo is in JPEG File Interchange Format. Alternatively, an attribute type which uses the Octet String syntax can be defined, e.g.:

```plaintext
attributetype ( 1.1.2.1.2 NAME 'x-my-Photo'
                DESC 'a photo (application defined format)'
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
                SINGLE-VALUE )
```

In this case, the syntax doesn't specify the format of the photo. It's assumed (maybe incorrectly) that all applications accessing this attribute agree on the handling of values.

If you wanted to support multiple photo formats, you could define a separate attribute type for each format, prefix the photo with some typing information, or describe the value using ASN.1 and use the ;binary transfer option.

Another alternative is for the attribute to hold a URI pointing to the photo. You can model such an attribute after labeledURI (RFC2079) or simply create a subtype, e.g.:

```plaintext
attributetype ( 1.1.2.1.3 NAME 'x-my-PhotoURI'
                DESC 'URI and optional label referring to a photo'
                SUP labeledURI )
```

11.2.5. Object Class Specification

The objectclasses directive is used to define a new object class. The directive uses the same Object Class Description (as defined in RFC4512) used by the objectClasses attribute found in the subschema subentry, e.g.:

```plaintext
objectclass <RFC4512 Object Class Description>
```

where Object Class Description is defined by the following ABNF:

```plaintext
ObjectClassDescription = "{" whsp
    numericoid whsp ; ObjectClass identifier
    [ "NAME" qdescrs ]
    [ "DESC" qdstring ]
    [ "OBSOLETE" whsp ]
    [ "SUP" oids ] ; Superior ObjectClasses
    [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; default structural
    [ "MUST" oids ] ; AttributeTypes
    [ "MAY" oids ] ; AttributeTypes
    whsp "}"
```

where whsp is a space (" "), numericoid is a globally unique OID in dotted-decimal form (e.g. 1.1.0), qdescrs is one or more names, and oids is one or more names and/or OIDs.
11.2.5.1. x-my-PhotoObject

To define an auxiliary object class which allows x-my-Photo to be added to any existing entry.

```plaintext
objectclass ( 1.1.2.2.1 NAME 'x-my-PhotoObject'
               DESC 'mixin x-my-Photo'
               AUXILIARY
               MAY x-my-Photo )
```

11.2.5.2. x-my-Person

If your organization would like have a private structural object class to instantiate users, you can subclass one of the existing person classes, such as inetOrgPerson (RFC2798), and add any additional attributes which you desire.

```plaintext
objectclass ( 1.1.2.2.2 NAME 'x-my-Person'
               DESC 'my person'
               SUP inetOrgPerson
               MUST ( x-my-UniqueName $ givenName )
               MAY x-my-Photo )
```

The object class inherits the required/allowed attribute types of inetOrgPerson but requires x-my-UniqueName and givenName and allows x-my-Photo.

11.2.6. OID Macros

To ease the management and use of OIDs, slapd(8) supports Object Identifier macros. The objectIdentifier directive is used to equate a macro (name) with a OID. The OID may possibly be derived from a previously defined OID macro. The slapd.conf(5) syntax is:

```plaintext
objectIdentifier <name> { <oid> | <name>[::<suffix>] }
```

The following demonstrates definition of a set of OID macros and their use in defining schema elements:

```plaintext
objectIdentifier myOID  1.1
objectIdentifier mySNMP myOID:1
objectIdentifier myLDAP myOID:2
objectIdentifier myAttributeType myLDAP:1
objectIdentifier myObjectClass myLDAP:2
attributetype ( myAttributeType:3 NAME 'x-my-PhotoURI'
                DESC 'URI and optional label referring to a photo'
                SUP labeledURI )
objectclass ( myObjectClass:1 NAME 'x-my-PhotoObject'
             DESC 'mixin x-my-Photo'
             AUXILIARY
             MAY x-my-Photo )
```
12. Security Considerations

OpenLDAP Software is designed to run in a wide variety of computing environments from tightly-controlled closed networks to the global Internet. Hence, OpenLDAP Software supports many different security mechanisms. This chapter describes these mechanisms and discusses security considerations for using OpenLDAP Software.

12.1. Network Security

12.1.1. Selective Listening

By default, `slapd(8)` will listen on both the IPv4 and IPv6 "any" addresses. It is often desirable to have `slapd` listen on select address/port pairs. For example, listening only on the IPv4 address 127.0.0.1 will disallow remote access to the directory server. E.g.:

```
slapd -h ldap://127.0.0.1
```

While the server can be configured to listen on a particular interface address, this doesn't necessarily restrict access to the server to only those networks accessible via that interface. To selective restrict remote access, it is recommend that an IP Firewall be used to restrict access.

See Command-line Options and `slapd(8)` for more information.

12.1.2. IP Firewall

IP firewall capabilities of the server system can be used to restrict access based upon the client's IP address and/or network interface used to communicate with the client.

Generally, `slapd(8)` listens on port 389/tcp for ldap:// sessions and port 636/tcp for ldaps:// sessions. `slapd(8)` may be configured to listen on other ports.

As specifics of how to configure IP firewall are dependent on the particular kind of IP firewall used, no examples are provided here. See the document associated with your IP firewall.

12.1.3. TCP Wrappers

`slapd(8)` supports TCP Wrappers. TCP Wrappers provide a rule-based access control system for controlling TCP/IP access to the server. For example, the `host_options(5)` rule:

```
slapd: 10.0.0.0/255.0.0.0 127.0.0.1 : ALLOW
slapd: ALL : DENY
```

allows only incoming connections from the private network 10.0.0.0 and localhost (127.0.0.1) to access the directory service. Note that IP addresses are used as `slapd(8)` is not normally configured to perform reverse lookups.

It is noted that TCP wrappers require the connection to be accepted. As significant processing is required just to deny a connection, it is generally advised that IP firewall protection be used instead of TCP wrappers.
See *hosts_access*(5) for more information on TCP wrapper rules.

### 12.2. Data Integrity and Confidentiality Protection

Transport Layer Security (TLS) can be used to provide data integrity and confidentiality protection. OpenLDAP supports negotiation of TLS (SSL) via both StartTLS and ldaps://. See the Using TLS chapter for more information. StartTLS is the standard track mechanism.

A number of Simple Authentication and Security Layer (SASL) mechanisms, such as DIGEST-MD5 and GSSAPI, also provide data integrity and confidentiality protection. See the Using SASL chapter for more information.

#### 12.2.1. Security Strength Factors

The server uses Security Strength Factors (SSF) to indicate the relative strength of protection. A SSF of zero (0) indicates no protections are in place. A SSF of one (1) indicates integrity protection are in place. A SSF greater than one (>1) roughly correlates to the effective encryption key length. For example, DES is 56, 3DES is 112, and AES 128, 192, or 256.

A number of administrative controls rely on SSFs associated with TLS and SASL protection in place on an LDAP session.

```
security controls disallow operations when appropriate protections are not in place. For example:

    security ssf=1 update_ssf=112
```

requires integrity protection for all operations and encryption protection, 3DES equivalent, for update operations (e.g. add, delete, modify, etc.). See *slapd.conf*(5) for details.

For fine-grained control, SSFs may be used in access controls. See The access Configuration Directive section of the The slapd Configuration File for more information.

### 12.3. Authentication Methods

#### 12.3.1. "simple" method

The LDAP "simple" method has three modes of operation:

- anonymous,
- unauthenticated, and
- user/password authenticated.

Anonymous access is requested by providing no name and no password to the "simple" bind operation. Unauthenticated access is requested by providing a name but no password. Authenticated access is requested by providing a valid name and password.

An anonymous bind results in an *anonymous* authorization association. Anonymous bind mechanism is enabled by default, but can be disabled by specifying "disallow bind_anon" in *slapd.conf*(5). Note that disabling the anonymous bind mechanism does not prevent anonymous access to the directory. To require authentication to access the directory, one should instead specify "require authc".
An unauthenticated bind also results in an *anonymous* authorization association. Unauthenticated bind mechanism is disabled by default, but can be enabled by specifying "allow bind_anon_cred" in *slapd.conf*(5). As a number of LDAP applications mistakenly generate unauthenticated bind request when authenticated access was intended (that is, they do not ensure a password was provided), this mechanism should generally remain disabled.

A successful user/password authenticated bind results in a user authorization identity, the provided name, being associated with the session. User/password authenticated bind is enabled by default. However, as this mechanism itself offers no eavesdropping protection (e.g., the password is set in the clear), it is recommended that it be used only in tightly controlled systems or when the LDAP session is protected by other means (e.g., TLS, IPsec). Where the administrator relies on TLS to protect the password, it is recommended that unprotected authentication be disabled. This is done using the *security directive's simple_bind* option, which provides fine grain control over the level of confidential protection to require for *simple* user/password authentication. E.g., using *security simple_bind=56* would require *simple* binds to use encryption of DES equivalent or better.

The user/password authenticated bind mechanism can be completely disabled by setting "disallow bind_simple".

---

**Note:** An unsuccessful bind always results in the session having an *anonymous* authorization association.

### 12.3.2. SASL method

The LDAP SASL method allows use of any SASL authentication mechanism. The Using SASL discusses use of SASL.
13. Using SASL

OpenLDAP clients and servers are capable of authenticating via the Simple Authentication and Security Layer (SASL) framework, which is detailed in RFC4422. This chapter describes how to make use of SASL in OpenLDAP.

There are several industry standard authentication mechanisms that can be used with SASL, including GSSAPI for Kerberos V, DIGEST-MD5, and PLAIN and EXTERNAL for use with Transport Layer Security (TLS).

The standard client tools provided with OpenLDAP Software, such as ldapsearch(1) and ldapmodify(1), will by default attempt to authenticate the user to the LDAP directory server using SASL. Basic authentication service can be set up by the LDAP administrator with a few steps, allowing users to be authenticated to the slapd server as their LDAP entry. With a few extra steps, some users and services can be allowed to exploit SASL’s proxy authorization feature, allowing them to authenticate themselves and then switch their identity to that of another user or service.

This chapter assumes you have read Cyrus SASL for System Administrators, provided with the Cyrus SASL package (in doc/sysadmin.html) and have a working Cyrus SASL installation. You should use the Cyrus SASL sample_client and sample_server to test your SASL installation before attempting to make use of it with OpenLDAP Software.

Note that in the following text the term user is used to describe a person or application entity who is connecting to the LDAP server via an LDAP client, such as ldapsearch(1). That is, the term user not only applies to both an individual using an LDAP client, but to an application entity which issues LDAP client operations without direct user control. For example, an e-mail server which uses LDAP operations to access information held in an LDAP server is an application entity.

13.1. SASL Security Considerations

SASL offers many different authentication mechanisms. This section briefly outlines security considerations.

Some mechanisms, such as PLAIN and LOGIN, offer no greater security over LDAP simple authentication. Like LDAP simple authentication, such mechanisms should not be used unless you have adequate security protections in place. It is recommended that these mechanisms be used only in conjunction with Transport Layer Security (TLS). Use of PLAIN and LOGIN are not discussed further in this document.

The DIGEST-MD5 mechanism is the mandatory-to-implement authentication mechanism for LDAPv3. Though DIGEST-MD5 is not a strong authentication mechanism in comparison with trusted third party authentication systems (such as Kerberos or public key systems), it does offer significant protections against a number of attacks. Unlike the CRAM-MD5 mechanism, it prevents chosen plaintext attacks. DIGEST-MD5 is favored over the use of plaintext password mechanisms. The CRAM-MD5 mechanism is deprecated in favor of DIGEST-MD5. Use of DIGEST-MD5 is discussed below.

The GSSAPI mechanism utilizes GSS-API Kerberos V to provide secure authentication services. The KERBEROS_V4 mechanism is available for those using Kerberos IV. Kerberos is viewed as a secure, distributed authentication system suitable for both small and large enterprises. Use of GSSAPI and KERBEROS_V4 are discussed below.
The EXTERNAL mechanism utilizes authentication services provided by lower level network services such as TLS (TLS). When used in conjunction with TLS X.509-based public key technology, EXTERNAL offers strong authentication. Use of EXTERNAL is discussed in the Using TLS chapter.

There are other strong authentication mechanisms to choose from, including OTP (one time passwords) and SRP (secure remote passwords). These mechanisms are not discussed in this document.

13.2. SASL Authentication

Getting basic SASL authentication running involves a few steps. The first step configures your slapd server environment so that it can communicate with client programs using the security system in place at your site. This usually involves setting up a service key, a public key, or other form of secret. The second step concerns mapping authentication identities to LDAP DN’s, which depends on how entries are laid out in your directory. An explanation of the first step will be given in the next section using Kerberos V4 as an example mechanism. The steps necessary for your site’s authentication mechanism will be similar, but a guide to every mechanism available under SASL is beyond the scope of this chapter. The second step is described in the section Mapping Authentication Identities.

13.2.1. GSSAPI

This section describes the use of the SASL GSSAPI mechanism and Kerberos V with OpenLDAP. It will be assumed that you have Kerberos V deployed, you are familiar with the operation of the system, and that your users are trained in its use. This section also assumes you have familiarized yourself with the use of the GSSAPI mechanism by reading Configuring GSSAPI and Cyrus SASL (provided with Cyrus SASL in the doc/gssapi file) and successfully experimented with the Cyrus provided sample_server and sample_client applications. General information about Kerberos is available at http://web.mit.edu/kerberos/www/.

To use the GSSAPI mechanism with slapd(8) one must create a service key with a principal for ldap service within the realm for the host on which the service runs. For example, if you run slapd on directory.example.com and your realm is EXAMPLE.COM, you need to create a service key with the principal:

    ldap/directory.example.com@EXAMPLE.COM

When slapd(8) runs, it must have access to this key. This is generally done by placing the key into a keytab file, /etc/krb5.keytab. See your Kerberos and Cyrus SASL documentation for information regarding keytab location settings.

To use the GSSAPI mechanism to authenticate to the directory, the user obtains a Ticket Granting Ticket (TGT) prior to running the LDAP client. When using OpenLDAP client tools, the user may mandate use of the GSSAPI mechanism by specifying -Y GSSAPI as a command option.

For the purposes of authentication and authorization, slapd(8) associates an authentication request DN of the form:

    uid=<primary[/instance]>,cn=<realm>,cn=gssapi,cn=auth

Continuing our example, a user with the Kerberos principal kurt@EXAMPLE.COM would have the associated DN:
and the principal ursula/admin@FOREIGN.REALM would have the associated DN:

uid=ursula/admin, cn=foreign.realm, cn=gssapi, cn=auth

The authentication request DN can be used directly ACLs and groupOfNames "member" attributes, since it is of legitimate LDAP DN format. Or alternatively, the authentication DN could be mapped before use. See the section Mapping Authentication Identities for details.

13.2.2. KERBEROS_V4

This section describes the use of the SASL KERBEROS_V4 mechanism with OpenLDAP. It will be assumed that you are familiar with the workings of the Kerberos IV security system, and that your site has Kerberos IV deployed. Your users should be familiar with authentication policy, how to receive credentials in a Kerberos ticket cache, and how to refresh expired credentials.

Note: KERBEROS_V4 and Kerberos IV are deprecated in favor of GSSAPI and Kerberos V.

Client programs will need to be able to obtain a session key for use when connecting to your LDAP server. This allows the LDAP server to know the identity of the user, and allows the client to know it is connecting to a legitimate server. If encryption layers are to be used, the session key can also be used to help negotiate that option.

The slapd server runs the service called "ldap", and the server will require a srvtab file with a service key. SASL aware client programs will be obtaining an "ldap" service ticket with the user's ticket granting ticket (TGT), with the instance of the ticket matching the hostname of the OpenLDAP server. For example, if your realm is named EXAMPLE.COM and the slapd server is running on the host named directory.example.com, the /etc/srvtab file on the server will have a service key

ldap.directory@EXAMPLE.COM

When an LDAP client is authenticating a user to the directory using the KERBEROS_IV mechanism, it will request a session key for that same principal, either from the ticket cache or by obtaining a new one from the Kerberos server. This will require the TGT to be available and valid in the cache as well. If it is not present or has expired, the client may print out the message:

ldap_sasl_interactive_bind_s: Local error

When the service ticket is obtained, it will be passed to the LDAP server as proof of the user's identity. The server will extract the identity and realm out of the service ticket using SASL library calls, and convert them into an authentication request DN of the form

uid=<username>, cn=<realm>, cn=<mechanism>, cn=auth

So in our above example, if the user's name were "adamson", the authentication request DN would be:

uid=adamsom, cn=example.com, cn=kerberos_v4, cn=auth

This authentication request DN can be used directly ACLs or, alternatively, mapped prior to use. See the section Mapping Authentication Identities for details.
13.2.3. DIGEST-MD5

This section describes the use of the SASL DIGEST-MD5 mechanism using secrets stored either in the directory itself or in Cyrus SASL’s own database. DIGEST-MD5 relies on the client and the server sharing a "secret", usually a password. The server generates a challenge and the client a response proving that it knows the shared secret. This is much more secure than simply sending the secret over the wire.

Cyrus SASL supports several shared-secret mechanisms. To do this, it needs access to the plaintext password (unlike mechanisms which pass plaintext passwords over the wire, where the server can store a hashed version of the password).

The server’s copy of the shared-secret may be stored in Cyrus SASL’s own sasldb database, in an external system accessed via saslauthd, or in LDAP database itself. In either case it is very important to apply file access controls and LDAP access controls to prevent exposure of the passwords. The configuration and commands discussed in this section assume the use of Cyrus SASL 2.1.

To use secrets stored in sasldb, simply add users with the saslpasswd2 command:

```
saslpasswd2 -c <username>
```

The passwords for such users must be managed with the saslpasswd2 command.

To use secrets stored in the LDAP directory, place plaintext passwords in the userPassword attribute. It will be necessary to add an option to slapd.conf to make sure that passwords set using the LDAP Password Modify Operation are stored in plaintext:

```
password-hash {CLEARTEXT}
```

Passwords stored in this way can be managed either with ldappasswd(1) or by simply modifying the userPassword attribute. Regardless of where the passwords are stored, a mapping will be needed from authentication request DN to user’s DN.

The DIGEST-MD5 mechanism produces authentication IDs of the form:

```
uid=<username>,cn=<realm>,cn=digest-md5, cn=auth
```

If the default realm is used, the realm name is omitted from the ID, giving:

```
uid=<username>,cn=digest-md5, cn=auth
```

See Mapping Authentication Identities below for information on optional mapping of identities.

With suitable mappings in place, users can specify SASL IDs when performing LDAP operations and sldb} and the directory itself will be used to verify the authentication. For example, the user identified by the directory entry:

```diff
    dn: cn=Andrew Findlay+uid=u000997,dc=example,dc=com
    objectclass: inetOrgPerson
    objectclass: person
    sn: Findlay
    uid: u000997
    userPassword: secret
```
can issue commands of the form:

    ldapsearch -Y DIGEST-MD5 -U u000997 ...

**Note:** in each of the above cases, no authorization identity (e.g. `-X`) was provided. Unless you are attempting SASL Proxy Authorization, no authorization identity should be specified. The server will infer an authorization identity from authentication identity (as described below).

### 13.2.4. Mapping Authentication Identities

The authentication mechanism in the slapd server will use SASL library calls to obtain the authenticated user's "username", based on whatever underlying authentication mechanism was used. This username is in the namespace of the authentication mechanism, and not in the normal LDAP namespace. As stated in the sections above, that username is reformatted into an authentication request DN of the form

    uid=<username>,cn=<realm>,cn=<mechanism>,cn=auth

or

    uid=<username>,cn=<mechanism>,cn=auth

depending on whether or not `<mechanism>` employs the concept of "realms". Note also that the realm part will be omitted if the default realm was used in the authentication.

The `ldapwhoami(1)` command may be used to determine the identity associated with the user. It is very useful for determining proper function of mappings.

It is not intended that you should add LDAP entries of the above form to your LDAP database. Chances are you have an LDAP entry for each of the persons that will be authenticating to LDAP, laid out in your directory tree, and the tree does not start at `cn=auth`. But if your site has a clear mapping between the "username" and an LDAP entry for the person, you will be able to configure your LDAP server to automatically map a authentication request DN to the user's authentication DN.

**Note:** it is not required that the authentication request DN nor the user's authentication DN resulting from the mapping refer to an entry held in the directory. However, additional capabilities become available (see below).

The LDAP administrator will need to tell the slapd server how to map an authentication request DN to a user's authentication DN. This is done by adding one or more `authz-regexp` directives to the `slapd.conf(5)` file. This directive takes two arguments:

    authz-regexp   <search pattern>   <replacement pattern>

The authentication request DN is compared to the search pattern using the regular expression functions `regcomp()` and `regexec()`, and if it matches, it is rewritten as the replacement pattern. If there are multiple `authz-regexp` directives, only the first whose search pattern matches the authentication identity is used. The string that is output from the replacement pattern should be the authentication DN of the user or an LDAP URL. If replacement string produces a DN, the entry named by this DN need not be held by this server. If the replace string produces an LDAP URL, that LDAP URL must evaluate to one and only one entry held by this server.
The search pattern can contain any of the regular expression characters listed in `regexec(3C)`. The main characters of note are dot ".", asterisk "*", and the open and close parenthesis "(" and ")". Essentially, the dot matches any character, the asterisk allows zero or more repeats of the immediately preceding character or pattern, and terms in parenthesis are remembered for the replacement pattern.

The replacement pattern will produce either a DN or URL referring to the user. Anything from the authentication request DN that matched a string in parenthesis in the search pattern is stored in the variable "$1". That variable "$1" can appear in the replacement pattern, and will be replaced by the string from the authentication request DN. If there were multiple sets of parentheses in the search pattern, the variables $2, $3, etc are used.

### 13.2.5. Direct Mapping

Where possible, direct mapping of the authentication request DN to the user's DN is generally recommended. Aside from avoiding the expense of searching for the user's DN, it allows mapping to DNs which refer to entries not held by this server.

Suppose the authentication request DN is written as:

```
uid=adamson,cn=example.com,cn=gssapi,cn=auth
```

and the user's actual LDAP entry is:

```
uid=adamson,ou=people,dc=example,dc=com
```

then the following `authz-regexp` directive in `slapd.conf(5)` would provide for direct mapping.

```
authz-regexp
  uid=([^,]*),cn=example.com,cn=gssapi,sn=auth
  uid=$1,ou=people,dc=example,dc=com
```

An even more lenient rule could be written as

```
authz-regexp
  uid=([^,]*),cn=([^,]*),cn=auth
  uid=$1,ou=people,dc=example,dc=com
```

Be careful about setting the search pattern too leniently, however, since it may mistakenly allow persons to become authenticated as a DN to which they should not have access. It is better to write several strict directives than one lenient directive which has security holes. If there is only one authentication mechanism in place at your site, and zero or one realms in use, you might be able to map between authentication identities and LDAP DN's with a single `authz-regexp` directive.

Don't forget to allow for the case where the realm is omitted as well as the case with an explicitly specified realm. This may well require a separate `authz-regexp` directive for each case, with the explicit-realm entry being listed first.

### 13.2.6. Search-based mappings

There are a number of cases where mapping to a LDAP URL may be appropriate. For instance, some sites may have person objects located in multiple areas of the LDAP tree, such as if there were an `ou=accounting` tree and an `ou=engineering` tree, with persons interspersed between them. Or, maybe
the desired mapping must be based upon information in the user's information. Consider the need to map the
above authentication request DN to user whose entry is as follows:

```
dn: cn=Mark Adamson,ou=People,dc=Example,dc=COM
objectclass: person
  cn: Mark Adamson
  uid: adamson
```

The information in the authentication request DN is insufficient to allow the user's DN to be directly derived,
instead the user's DN must be searched for. For these situations, a replacement pattern which produces a
LDAP URL can be used in the `authz-regexp` directives. This URL will then be used to perform an
internal search of the LDAP database to find the person's authentication DN.

An LDAP URL, similar to other URL's, is of the form

```
```

This contains all of the elements necessary to perform an LDAP search: the name of the server `<host>`, the
LDAP DN search base `<base>`, the LDAP attributes to retrieve `<attrs>`, the search scope `<scope>` which is
one of the three options "base", "one", or "sub", and lastly an LDAP search filter `<filter>`. Since the search is
for an LDAP DN within the current server, the `<host>` portion should be empty. The `<attrs>` field is also
ignored since only the DN is of concern. These two elements are left in the format of the URL to maintain the
clarity of what information goes where in the string.

Suppose that the person in the example from above did in fact have an authentication username of "adamson"
and that information was kept in the attribute "uid" in their LDAP entry. The `authz-regexp` directive
might be written as

```
authz-regexp
  uid=([^,\*]*),cn=example.com,cn=gssapi,cn=auth
  ldap:///ou=people,dc=example,dc=com??one?(uid=$1)
```

This will initiate an internal search of the LDAP database inside the slapd server. If the search returns exactly
one entry, it is accepted as being the DN of the user. If there are more than one entries returned, or if there are
zero entries returned, the authentication fails and the user's connection is left bound as the authentication
request DN.

The attributes that are used in the search filter `<filter>` in the URL should be indexed to allow faster searching.
If they are not, the authentication step alone can take uncomfortably long periods, and users may assume the
server is down.

A more complex site might have several realms in use, each mapping to a different subtree in the directory.
These can be handled with statements of the form:

```
# Match Engineering realm
authz-regexp
  uid=([^,\*]*),cn=engineering.example.com,cn=digest-md5,cn=auth
  ldap:///dc=eng,dc=example,dc=com??one?(objectClass=person)
```

```
# Match Accounting realm
authz-regexp
  uid=([^,\*]*),cn=accounting.example.com,cn=digest-md5,cn=auth
  ldap:///dc=accounting,dc=example,dc=com??one?(objectClass=person)
```
# Default realm is customers.example.com

```bash
authz-regexp
    uid=(^[^,]*),cn=digest-md5,cn=auth
ldap:///dc=customers,dc=example,dc=com??one?(&(uid=$1)(objectClass=person))
```

Note that the explicitly-named realms are handled first, to avoid the realm name becoming part of the UID. Also note the use of scope and filters to limit matching to desirable entries.

Note as well that `authz-regexp` internal search are subject to access controls. Specifically, the authentication identity must have `auth` access.

See `slapd.conf(5)` for more detailed information.

## 13.3. SASL Proxy Authorization

The SASL offers a feature known as *proxy authorization*, which allows an authenticated user to request that they act on the behalf of another user. This step occurs after the user has obtained an authentication DN, and involves sending an authorization identity to the server. The server will then make a decision on whether or not to allow the authorization to occur. If it is allowed, the user's LDAP connection is switched to have a binding DN derived from the authorization identity, and the LDAP session proceeds with the access of the new authorization DN.

The decision to allow an authorization to proceed depends on the rules and policies of the site where LDAP is running, and thus cannot be made by SASL alone. The SASL library leaves it up to the server to make the decision. The LDAP administrator sets the guidelines of who can authorize to what identity by adding information into the LDAP database entries. By default, the authorization features are disabled, and must be explicitly configured by the LDAP administrator before use.

### 13.3.1. Uses of Proxy Authorization

This sort of service is useful when one entity needs to act on the behalf of many other users. For example, users may be directed to a web page to make changes to their personal information in their LDAP entry. The users authenticate to the web server to establish their identity, but the web server CGI cannot authenticate to the LDAP server as that user to make changes for them. Instead, the web server authenticates itself to the LDAP server as a service identity, say,

```bash
    cn=WebUpdate,dc=example,dc=com
```

and then it will SASL authorize to the DN of the user. Once so authorized, the CGI makes changes to the LDAP entry of the user, and as far as the slapd server can tell for its ACLs, it is the user themself on the other end of the connection. The user could have connected to the LDAP server directly and authenticated as themself, but that would require the user to have more knowledge of LDAP clients, knowledge which the web page provides in an easier format.

Proxy authorization can also be used to limit access to an account that has greater access to the database. Such an account, perhaps even the root DN specified in `slapd.conf(5)`, can have a strict list of people who can authorize to that DN. Changes to the LDAP database could then be only allowed by that DN, and in order to become that DN, users must first authenticate as one of the persons on the list. This allows for better auditing of who made changes to the LDAP database. If people were allowed to authenticate directly to the privileged account, possibly through the `rootpw slapd.conf(5)` directive or through a `userPassword` attribute, then auditing becomes more difficult.
Note that after a successful proxy authorization, the original authentication DN of the LDAP connection is overwritten by the new DN from the authorization request. If a service program is able to authenticate itself as its own authentication DN and then authorize to other DN's, and if it is planning on switching to several different identities during one LDAP session, it will need to authenticate itself each time before authorizing to another DN (or use a different proxy authorization mechanism). The slapd server does not keep record of the service program's ability to switch to other DN's. On authentication mechanisms like Kerberos this will not require multiple connections being made to the Kerberos server, since the user's TGT and "ldap" session key are valid for multiple uses for the several hours of the ticket lifetime.

13.3.2. SASL Authorization Identities

The SASL authorization identity is sent to the LDAP server via the \texttt{-X} switch for 	extit{ldapsearch(1)} and other tools, or in the \texttt{*authzid} parameter to the \textit{lutil_sasl_defaults()} call. The identity can be in one of two forms, either

\begin{verbatim}
  u:<username>
\end{verbatim}

or

\begin{verbatim}
  dn:<dn>
\end{verbatim}

In the first form, the \texttt{<username>} is from the same namespace as the authentication identities above. It is the user's username as it is referred to by the underlying authentication mechanism. Authorization identities of this form are converted into a DN format by the same function that the authentication process used, producing an \texttt{authorization request DN} of the form

\begin{verbatim}
  uid=<username>,cn=<realm>,cn=<mechanism>,cn=auth
\end{verbatim}

That authorization request DN is then run through the same \texttt{authz-regexp} process to convert it into a legitimate authorization DN from the database. If it cannot be converted due to a failed search from an LDAP URL, the authorization request fails with "inappropriate access". Otherwise, the DN string is now a legitimate authorization DN ready to undergo approval.

If the authorization identity was provided in the second form, with a \texttt{"dn:"} prefix, the string after the prefix is already in authorization DN form, ready to undergo approval.

13.3.3. Proxy Authorization Rules

Once slapd has the authorization DN, the actual approval process begins. There are two attributes that the LDAP administrator can put into LDAP entries to allow authorization:

\begin{verbatim}
  authzTo
  authzFrom
\end{verbatim}

Both can be multivalued. The \texttt{authzTo} attribute is a source rule, and it is placed into the entry associated with the authentication DN to tell what authorization DNs the authenticated DN is allowed to assume. The second attribute is a destination rule, and it is placed into the entry associated with the requested authorization DN to tell which authenticated DNs may assume it.

The choice of which authorization policy attribute to use is up to the administrator. Source rules are checked first in the person's authentication DN entry, and if none of the \texttt{authzTo} rules specify the authorization is
permitted, the \texttt{authzFrom} rules in the authorization DN entry are then checked. If neither case specifies that the request be honored, the request is denied. Since the default behavior is to deny authorization requests, rules only specify that a request be allowed; there are no negative rules telling what authorizations to deny.

The value(s) in the two attributes are of the same form as the output of the replacement pattern of a \texttt{authz-regexp} directive: either a DN or an LDAP URL. For example, if a \texttt{authzTo} value is a DN, that DN is one the authenticated user can authorize to. On the other hand, if the \texttt{authzTo} value is an LDAP URL, the URL is used as an internal search of the LDAP database, and the authenticated user can become ANY DN returned by the search. If an LDAP entry looked like:

\begin{verbatim}
  dn: cn=WebUpdate,dc=example,dc=com
  authzTo: ldap:///dc=example,dc=com??sub?(objectclass=person)
\end{verbatim}

then any user who authenticated as \texttt{cn=WebUpdate,dc=example,dc=com} could authorize to any other LDAP entry under the search base \texttt{dc=example,dc=com} which has an \texttt{objectClass} of \texttt{Person}.

\subsection*{13.3.3.1. Notes on Proxy Authorization Rules}

An LDAP URL in a \texttt{authzTo} or \texttt{authzFrom} attribute will return a set of DNs. Each DN returned will be checked. Searches which return a large set can cause the authorization process to take an uncomfortably long time. Also, searches should be performed on attributes that have been indexed by \texttt{slapd}.

To help produce more sweeping rules for \texttt{authzFrom} and \texttt{authzTo}, the values of these attributes are allowed to be DNs with regular expression characters in them. This means a source rule like

\begin{verbatim}
  authzTo: dn.regex=^uid=[^,]*,dc=example,dc=com$
\end{verbatim}

would allow that authenticated user to authorize to any DN that matches the regular expression pattern given. This regular expression comparison can be evaluated much faster than an LDAP search for \texttt{(uid=*)}.

Also note that the values in an authorization rule must be one of the two forms: an LDAP URL or a DN (with or without regular expression characters). Anything that does not begin with \texttt{"ldap://"} is taken as a DN. It is not permissible to enter another authorization identity of the form \texttt{"u:<username>"} as an authorization rule.

\subsection*{13.3.3.2. Policy Configuration}

The decision of which type of rules to use, \texttt{authzFrom} or \texttt{authzTo}, will depend on the site's situation. For example, if the set of people who may become a given identity can easily be written as a search filter, then a single destination rule could be written. If the set of people is not easily defined by a search filter, and the set of people is small, it may be better to write a source rule in the entries of each of those people who should be allowed to perform the proxy authorization.

By default, processing of proxy authorization rules is disabled. The \texttt{authz-policy} directive must be set in the \texttt{slapd.conf(5)} file to enable authorization. This directive can be set to \texttt{none} for no rules (the default), \texttt{to} for source rules, \texttt{from} for destination rules, or \texttt{both} for both source and destination rules.

Source rules are extremely powerful. If ordinary users have access to write the \texttt{authzTo} attribute in their own entries, then they can write rules that would allow them to authorize as anyone else. As such, when using source rules, the \texttt{authzTo} attribute should be protected with an ACL that only allows privileged users to set its values.
14. Using TLS

OpenLDAP clients and servers are capable of using the Transport Layer Security (TLS) framework to provide integrity and confidentiality protections and to support LDAP authentication using the SASL EXTERNAL mechanism. TLS is defined in RFC4346.

Note: For generating certificates, please reference http://www.openldap.org/faq/data/cache/185.html

14.1. TLS Certificates

TLS uses X.509 certificates to carry client and server identities. All servers are required to have valid certificates, whereas client certificates are optional. Clients must have a valid certificate in order to authenticate via SASL EXTERNAL. For more information on creating and managing certificates, see the OpenSSL documentation.

14.1.1. Server Certificates

The DN of a server certificate must use the CN attribute to name the server, and the CN must carry the server's fully qualified domain name. Additional alias names and wildcards may be present in the subjectAltName certificate extension. More details on server certificate names are in RFC4513.

14.1.2. Client Certificates

The DN of a client certificate can be used directly as an authentication DN. Since X.509 is a part of the X.500 standard and LDAP is also based on X.500, both use the same DN formats and generally the DN in a user's X.509 certificate should be identical to the DN of their LDAP entry. However, sometimes the DNs may not be exactly the same, and so the mapping facility described in Mapping Authentication Identities can be applied to these DNs as well.

14.2. TLS Configuration

After obtaining the required certificates, a number of options must be configured on both the client and the server to enable TLS and make use of the certificates. At a minimum, the clients must be configured with the name of the file containing all of the Certificate Authority (CA) certificates it will trust. The server must be configured with the CA certificates and also its own server certificate and private key.

Typically a single CA will have issued the server certificate and all of the trusted client certificates, so the server only needs to trust that one signing CA. However, a client may wish to connect to a variety of secure servers managed by different organizations, with server certificates generated by many different CAs. As such, a client is likely to need a list of many different trusted CAs in its configuration.

14.2.1. Server Configuration

The configuration directives for slapd belong in the global directives section of slapd.conf(5).
14.2.1.1. TLSCACertificateFile <filename>

This directive specifies the PEM-format file containing certificates for the CA's that slapd will trust. The certificate for the CA that signed the server certificate must be included among these certificates. If the signing CA was not a top-level (root) CA, certificates for the entire sequence of CA's from the signing CA to the top-level CA should be present. Multiple certificates are simply appended to the file; the order is not significant.

14.2.1.2. TLSCACertificatePath <path>

This directive specifies the path of a directory that contains individual CA certificates in separate files. In addition, this directory must be specially managed using the OpenSSL c_rehash utility. When using this feature, the OpenSSL library will attempt to locate certificate files based on a hash of their name and serial number. The c_rehash utility is used to generate symbolic links with the hashed names that point to the actual certificate files. As such, this option can only be used with a filesystem that actually supports symbolic links. In general, it is simpler to use the TLSCACertificateFile directive instead.

14.2.1.3. TLSCertificateFile <filename>

This directive specifies the file that contains the slapd server certificate. Certificates are generally public information and require no special protection.

14.2.1.4. TLSCertificateKeyFile <filename>

This directive specifies the file that contains the private key that matches the certificate stored in the TLSCertificateFile file. Private keys themselves are sensitive data and are usually password encrypted for protection. However, the current implementation doesn't support encrypted keys so the key must not be encrypted and the file itself must be protected carefully.

14.2.1.5. TLSCipherSuite <cipher-suite-spec>

This directive configures what ciphers will be accepted and the preference order. <cipher-suite-spec> should be a cipher specification for OpenSSL. You can use the command

```
openssl ciphers -v ALL
```

to obtain a verbose list of available cipher specifications. Besides the individual cipher names, the specifiers HIGH, MEDIUM, LOW, EXPORT, and EXPORT40 may be helpful, along with TLSv1, SSLv3, and SSLv2.

14.2.1.6. TLSRandFile <filename>

This directive specifies the file to obtain random bits from when /dev/urandom is not available. If the system provides /dev/urandom then this option is not needed, otherwise a source of random data must be configured. Some systems (e.g. Linux) provide /dev/urandom by default, while others (e.g. Solaris) require the installation of a patch to provide it, and others may not support it at all. In the latter case, EGD or PRNGD should be installed, and this directive should specify the name of the EGD/PRNGD socket. The environment variable RANDFILE can also be used to specify the filename. Also, in the absence of these options, the .rnd file in the slapd user's home directory may be used if it exists. To use the .rnd file, just create the file and copy a few hundred bytes of arbitrary data into the file. The file is only used to provide a seed for the pseudo-random number generator, and it doesn't need very much data to work.
14.2.1.7. TLSEphemeralDHParamFile <filename>

This directive specifies the file that contains parameters for Diffie-Hellman ephemeral key exchange. This is required in order to use a DSA certificate on the server side (i.e. TLSCertificateKeyFile points to a DSA key). Multiple sets of parameters can be included in the file; all of them will be processed. Parameters can be generated using the following command:

```
openssl dhparam [-dsaparam] -out <filename> <numbits>
```

14.2.1.8. TLSVerifyClient { never | allow | try | demand }

This directive specifies what checks to perform on client certificates in an incoming TLS session, if any. This option is set to **never** by default, in which case the server never asks the client for a certificate. With a setting of **allow** the server will ask for a client certificate; if none is provided the session proceeds normally. If a certificate is provided but the server is unable to verify it, the certificate is ignored and the session proceeds normally, as if no certificate had been provided. With a setting of **try** the certificate is requested, and if none is provided, the session proceeds normally. If a certificate is provided and it cannot be verified, the session is immediately terminated. With a setting of **demand** the certificate is requested and a valid certificate must be provided, otherwise the session is immediately terminated.

**Note:** The server must request a client certificate in order to use the SASL EXTERNAL authentication mechanism with a TLS session. As such, a non-default TLSVerifyClient setting must be configured before SASL EXTERNAL authentication may be attempted, and the SASL EXTERNAL mechanism will only be offered to the client if a valid client certificate was received.

14.2.2. Client Configuration

Most of the client configuration directives parallel the server directives. The names of the directives are different, and they go into `ldap.conf(5)` instead of `slapd.conf(5)`, but their functionality is mostly the same. Also, while most of these options may be configured on a system-wide basis, they may all be overridden by individual users in their `.ldaprc` files.

The LDAP Start TLS operation is used in LDAP to initiate TLS negotiation. All OpenLDAP command line tools support a `-Z` and `-ZZ` flag to indicate whether a Start TLS operation is to be issued. The latter flag indicates that the tool is to cease processing if TLS cannot be started while the former allows the command to continue.

In LDAPv2 environments, TLS is normally started using the LDAP Secure URI scheme (`ldaps://`) instead of the normal LDAP URI scheme (`ldap://`). OpenLDAP command line tools allow either scheme to be used with the `-H` flag and with the `URI ldap.conf(5)` option.

14.2.2.1. TLS_CACERT <filename>

This is equivalent to the server's `TLSCACertificateFile` option. As noted in the TLS Configuration section, a client typically may need to know about more CAs than a server, but otherwise the same considerations apply.
14.2.2.2. TLS_CACERTDIR <path>

This is equivalent to the server's TLSCACertificatePath option. The specified directory must be managed with the OpenSSL c_rehash utility as well.

14.2.2.3. TLS_CERT <filename>

This directive specifies the file that contains the client certificate. This is a user-only directive and can only be specified in a user's .ldaprc file.

14.2.2.4. TLS_KEY <filename>

This directive specifies the file that contains the private key that matches the certificate stored in the TLS_CERT file. The same constraints mentioned for TLSCertificateKeyFile apply here. This is also a user-only directive.

14.2.2.5. TLS_RANDFILE <filename>

This directive is the same as the server's TLSRandFile option.

14.2.2.6. TLS_REQCERT { never | allow | try | demand }

This directive is equivalent to the server's TLSVerifyClient option. However, for clients the default value is demand and there generally is no good reason to change this setting.
15. Constructing a Distributed Directory Service

For many sites, running one or more `slapd(8)` that hold an entire subtree of data is sufficient. But often it is desirable to have one `slapd` refer to other directory services for a certain part of the tree (which may or may not be running `slapd`).

`slapd` supports subordinate and superior knowledge information. Subordinate knowledge information is held in referral objects (RFC3296).

15.1. Subordinate Knowledge Information

Subordinate knowledge information may be provided to delegate a subtree. Subordinate knowledge information is maintained in the directory as a special referral object at the delegate point. The referral object acts as a delegation point, gluing two services together. This mechanism allows for hierarchical directory services to be constructed.

A referral object has a structural object class of referral and has the same Distinguished Name as the delegated subtree. Generally, the referral object will also provide the auxiliary object class extensibleObject. This allows the entry to contain appropriate Relative Distinguished Name values. This is best demonstrated by example.

If the server `a.example.net` holds `dc=example,dc=net` and wished to delegate the subtree `ou=subtree,dc=example,dc=net` to another server `b.example.net`, the following named referral object would be added to `a.example.net`:

```
dn: dc=subtree,dc=example,dc=net
objectClass: referral
objectClass: extensibleObject
dc: subtree
ref: ldap://b.example.net/dc=subtree,dc=example,dc=net
```

The server uses this information to generate referrals and search continuations to subordinate servers.

For those familiar with X.500, a named referral object is similar to an X.500 knowledge reference held in a subr DSE.

15.2. Superior Knowledge Information

Superior knowledge information may be specified using the referral directive. The value is a list of URIs referring to superior directory services. For servers without immediate superiors, such as for `a.example.net` in the example above, the server can be configured to use a directory service with global knowledge, such as the OpenLDAP Root Service (http://www.openldap.org/faq/index.cgi?file=393).

```
referral ldap://root.openldap.org/
```

However, as `a.example.net` is the immediate superior to `b.example.net`, `b.example.net` would be configured as follows:

```
referral ldap://a.example.net/
```
The server uses this information to generate referrals for operations acting upon entries not within or subordinate to any of the naming contexts held by the server.

For those familiar with X.500, this use of the `ref` attribute is similar to an X.500 knowledge reference held in a *Supr DSE*.

### 15.3. The ManageDsaIT Control

Adding, modifying, and deleting referral objects is generally done using `ldapmodify(1)` or similar tools which support the ManageDsaIT control. The ManageDsaIT control informs the server that you intend to manage the referral object as a regular entry. This keeps the server from sending a referral result for requests which interrogate or update referral objects.

The ManageDsaIT control should not be specified when managing regular entries.

The `−M` option of `ldapmodify(1)` (and other tools) enables ManageDsaIT. For example:

```
ldapmodify -M -f referral.ldif -x -D "cn=Manager,dc=example,dc=net" -W
```

or with `ldapsearch(1)`:  
```
ldapsearch -M -b "dc=example,dc=net" -x "(objectclass=referral)" '*' ref
```

**Note:** the `ref` attribute is operational and must be explicitly requested when desired in search results.

**Note:** the use of referrals to construct a Distributed Directory Service is extremely clumsy and not well supported by common clients. If an existing installation has already been built using referrals, the use of the *chain* overlay to hide the referrals will greatly improve the usability of the Directory system. A better approach would be to use explicitly defined local and proxy databases in *subordinate* configurations to provide a seamless view of the Distributed Directory.
16. Replication

Replicated directories are a fundamental requirement for delivering a resilient enterprise deployment.

OpenLDAP has various configuration options for creating a replicated directory. The following sections will discuss these.

16.1. Replication Strategies

16.1.1. Push Based

16.1.1.1. Replacing Slurpd

Slurpd replication has been deprecated in favor of Syncrepl replication and has been completely removed from OpenLDAP 2.4.

Why was it replaced?

The slurpd daemon was the original replication mechanism inherited from UMich's LDAP and operates in push mode: the master pushes changes to the slaves. It has been replaced for many reasons, in brief:

- It is not reliable
- It is extremely sensitive to the ordering of records in the replog
- It can easily go out of sync, at which point manual intervention is required to resync the slave database with the master directory
- It isn't very tolerant of unavailable servers. If a slave goes down for a long time, the replog may grow to a size that's too large for slurpd to process

What was it replaced with?

Syncrepl

Why is Syncrepl better?

- Syncrepl is self-synchronizing; you can start with a database in any state from totally empty to fully synced and it will automatically do the right thing to achieve and maintain synchronization
- Syncrepl can operate in either direction
- Data updates can be minimal or maximal

How do I implement a pushed based replication system using Syncrepl?

The easiest way is to point an LDAP backend (Backends and slapd-ldap(8)) to your slave directory and setup Syncrepl to point to your Master database.

REFERENCE test045/048 for better explanation of above.

If you imagine Syncrepl pulling down changes from the Master server, and then pushing those changes out to your slave servers via slapd-ldap(8). This is called proxy mode (elaborate/confirm?).

DIAGRAM HERE
OpenLDAP Software 2.4 Administrator's Guide

BETTER EXAMPLE here from test045/048 for different push/multiproxy examples.

Here's an example:

```
include ./schema/core.schema
include ./schema/cosine.schema
include ./schema/inetorgperson.schema
include ./schema/openldap.schema
include ./schema/nis.schema

pidfile /home/ghenry/openldap/ldap/tests/testrun/slapd.3.pid
argsfile /home/ghenry/openldap/ldap/tests/testrun/slapd.3.args

modulepath ../servers/slapd/back-bdb/
moduleload back_bdb.la
modulepath ../servers/slapd/back-monitor/
moduleload back_monitor.la
modulepath ../servers/slapd/overlays/
moduleload syncprov.la
modulepath ../servers/slapd/back-ldap/
moduleload back_ldap.la

# We don't need any access to this DSA
restrict all

#######################################################################
# consumer proxy database definitions
#######################################################################

database ldap
suffix "dc=example,dc=com"
rootdn "cn=Whoever"
uri ldap://localhost:9012/

lastmod on

# HACK: use the RootDN of the monitor database as UpdateDN so ACLs apply
# without the need to write the UpdateDN before starting replication
acl-bind bindmethod=simple
binddn="cn=Monitor"
credentials=monitor

# HACK: use the RootDN of the monitor database as UpdateDN so ACLs apply
# without the need to write the UpdateDN before starting replication
syncrepl rid=1
provider=ldap://localhost:9011/
binddn="cn=Manager,dc=example,dc=com"
bindmethod=simple
credentials=secret
searchbase="dc=example,dc=com"
filter="(objectClass=*)"
attrs="*,structuralObjectClass,entryUUID,entryCSN,creatorsName,createTimestamp,modifiersName,modifyTimestamp"
schemachecking=off
scope=sub
type=refreshAndPersist
retry="5 5 300 5"

overlay syncprov

database monitor
```
As you can see, you can let your imagination go wild using Syncrepl and slapd-ldap(8) tailoring your replication to fit your specific network topology.

### 16.1.2. Pull Based

#### 16.1.2.1. syncrepl replication

#### 16.1.2.2. delta-syncrepl replication

### 16.2. Replication Types

#### 16.2.1. syncrepl replication

#### 16.2.2. delta-syncrepl replication

#### 16.2.3. N-Way Multi-Master

http://www.connexitor.com/blog/pivot/entry.php?id=105#body

http://www.openldap.org/lists/openldap-software/200702/msg00006.html

http://www.openldap.org/lists/openldap-software/200602/msg00064.html

#### 16.2.4. MirrorMode

MirrorMode is a hybrid configuration that provides all of the consistency guarantees of single-master replication, while also providing the high availability of multi-master. In MirrorMode two masters are set up to replicate from each other (as a multi-master configuration) but an external frontend is employed to direct all writes to only one of the two servers. The second master will only be used for writes if the first master crashes, at which point the frontend will switch to directing all writes to the second master. When a crashed master is repaired and restarted it will automatically catch up to any changes on the running master and resync.

This is discussed in full in the MirrorMode section below

### 16.3. LDAP Sync Replication

The LDAP Sync Replication engine, syncrepl for short, is a consumer-side replication engine that enables the consumer LDAP server to maintain a shadow copy of a DIT fragment. A syncrepl engine resides at the consumer-side as one of the slapd(8) threads. It creates and maintains a consumer replica by connecting to the replication provider to perform the initial DIT content load followed either by periodic content polling or by timely updates upon content changes.

Syncrepl uses the LDAP Content Synchronization (or LDAP Sync for short) protocol as the replica synchronization protocol. It provides a stateful replication which supports both pull-based and push-based synchronization and does not mandate the use of a history store.
Syncrepl keeps track of the status of the replication content by maintaining and exchanging synchronization cookies. Because the syncrepl consumer and provider maintain their content status, the consumer can poll the provider content to perform incremental synchronization by asking for the entries required to make the consumer replica up-to-date with the provider content. Syncrepl also enables convenient management of replicas by maintaining replica status. The consumer replica can be constructed from a consumer-side or a provider-side backup at any synchronization status. Syncrepl can automatically resynchronize the consumer replica up-to-date with the current provider content.

Syncrepl supports both pull-based and push-based synchronization. In its basic refreshOnly synchronization mode, the provider uses pull-based synchronization where the consumer servers need not be tracked and no history information is maintained. The information required for the provider to process periodic polling requests is contained in the synchronization cookie of the request itself. To optimize the pull-based synchronization, syncrepl utilizes the present phase of the LDAP Sync protocol as well as its delete phase, instead of falling back on frequent full reloads. To further optimize the pull-based synchronization, the provider can maintain a per-scope session log as a history store. In its refreshAndPersist mode of synchronization, the provider uses a push-based synchronization. The provider keeps track of the consumer servers that have requested a persistent search and sends them necessary updates as the provider replication content gets modified.

With syncrepl, a consumer server can create a replica without changing the provider's configurations and without restarting the provider server, if the consumer server has appropriate access privileges for the DIT fragment to be replicated. The consumer server can stop the replication also without the need for provider-side changes and restart.

Syncrepl supports both partial and sparse replications. The shadow DIT fragment is defined by a general search criteria consisting of base, scope, filter, and attribute list. The replica content is also subject to the access privileges of the bind identity of the syncrepl replication connection.

16.3.1. The LDAP Content Synchronization Protocol

The LDAP Sync protocol allows a client to maintain a synchronized copy of a DIT fragment. The LDAP Sync operation is defined as a set of controls and other protocol elements which extend the LDAP search operation. This section introduces the LDAP Content Sync protocol only briefly. For more information, refer to RFC4533.

The LDAP Sync protocol supports both polling and listening for changes by defining two respective synchronization operations: refreshOnly and refreshAndPersist. Polling is implemented by the refreshOnly operation. The client copy is synchronized to the server copy at the time of polling. The server finishes the search operation by returning SearchResultDone at the end of the search operation as in the normal search. The listening is implemented by the refreshAndPersist operation. Instead of finishing the search after returning all entries currently matching the search criteria, the synchronization search remains persistent in the server. Subsequent updates to the synchronization content in the server cause additional entry updates to be sent to the client.

The refreshOnly operation and the refresh stage of the refreshAndPersist operation can be performed with a present phase or a delete phase.

In the present phase, the server sends the client the entries updated within the search scope since the last synchronization. The server sends all requested attributes, be it changed or not, of the updated entries. For each unchanged entry which remains in the scope, the server sends a present message consisting only of the name of the entry and the synchronization control representing state present. The present message does not
contain any attributes of the entry. After the client receives all update and present entries, it can reliably
determine the new client copy by adding the entries added to the server, by replacing the entries modified at
the server, and by deleting entries in the client copy which have not been updated nor specified as being
present at the server.

The transmission of the updated entries in the delete phase is the same as in the present phase. The server
sends all the requested attributes of the entries updated within the search scope since the last synchronization
to the client. In the delete phase, however, the server sends a delete message for each entry deleted from the
search scope, instead of sending present messages. The delete message consists only of the name of the entry
and the synchronization control representing state delete. The new client copy can be determined by adding,
modifying, and removing entries according to the synchronization control attached to the SearchResultEntry
message.

In the case that the LDAP Sync server maintains a history store and can determine which entries are scoped
out of the client copy since the last synchronization time, the server can use the delete phase. If the server does
not maintain any history store, cannot determine the scoped-out entries from the history store, or the history
store does not cover the outdated synchronization state of the client, the server should use the present phase.
The use of the present phase is much more efficient than a full content reload in terms of the synchronization
traffic. To reduce the synchronization traffic further, the LDAP Sync protocol also provides several
optimizations such as the transmission of the normalized entryUUIDs and the transmission of multiple
entryUUIDs in a single syncIdSet message.

At the end of the refreshOnly synchronization, the server sends a synchronization cookie to the client as a
state indicator of the client copy after the synchronization is completed. The client will present the received
cookie when it requests the next incremental synchronization to the server.

When refreshAndPersist synchronization is used, the server sends a synchronization cookie at the end of the
refresh stage by sending a Sync Info message with TRUE refreshDone. It also sends a synchronization cookie
by attaching it to SearchResultEntry generated in the persist stage of the synchronization search. During the
persist stage, the server can also send a Sync Info message containing the synchronization cookie at any time
the server wants to update the client-side state indicator. The server also updates a synchronization indicator
of the client at the end of the persist stage.

In the LDAP Sync protocol, entries are uniquely identified by the entryUUID attribute value. It can function
as a reliable identifier of the entry. The DN of the entry, on the other hand, can be changed over time and
hence cannot be considered as the reliable identifier. The entryUUID is attached to each SearchResultEntry
or SearchResultReference as a part of the synchronization control.

### 16.3.2. Syncrepl Details

The syncrepl engine utilizes both the refreshOnly and the refreshAndPersist operations of the LDAP Sync
protocol. If a syncrepl specification is included in a database definition, slapd(8) launches a syncrepl engine as
a slapd(8) thread and schedules its execution. If the refreshOnly operation is specified, the syncrepl engine
will be rescheduled at the interval time after a synchronization operation is completed. If the
refreshAndPersist operation is specified, the engine will remain active and process the persistent
synchronization messages from the provider.

The syncrepl engine utilizes both the present phase and the delete phase of the refresh synchronization. It is
possible to configure a per-scope session log in the provider server which stores the entryUUIDs of a finite
number of entries deleted from a replication content. Multiple replicas of single provider content share the
same per-scope session log. The syncrepl engine uses the delete phase if the session log is present and the
state of the consumer server is recent enough that no session log entries are truncated after the last
synchronization of the client. The syncrepl engine uses the present phase if no session log is configured for
the replication content or if the consumer replica is too outdated to be covered by the session log. The current
design of the session log store is memory based, so the information contained in the session log is not
persistent over multiple provider invocations. It is not currently supported to access the session log store by
using LDAP operations. It is also not currently supported to impose access control to the session log.

As a further optimization, even in the case the synchronization search is not associated with any session log,
no entries will be transmitted to the consumer server when there has been no update in the replication context.

The syncrepl engine, which is a consumer-side replication engine, can work with any backends. The LDAP
Sync provider can be configured as an overlay on any backend, but works best with the back-bdb or back-hdb
backend.

The LDAP Sync provider maintains a contextCSN for each database as the current synchronization state
indicator of the provider content. It is the largest entryCSN in the provider context such that no transactions
for an entry having smaller entryCSN value remains outstanding. The contextCSN could not just be set to
the largest issued entryCSN because entryCSN is obtained before a transaction starts and transactions are
not committed in the issue order.

The provider stores the contextCSN of a context in the contextCSN attribute of the context suffix entry.
The attribute is not written to the database after every update operation though; instead it is maintained
primarily in memory. At database start time the provider reads the last saved contextCSN into memory and
uses the in-memory copy exclusively thereafter. By default, changes to the contextCSN as a result of
database updates will not be written to the database until the server is cleanly shut down. A checkpoint facility
exists to cause the contextCSN to be written out more frequently if desired.

Note that at startup time, if the provider is unable to read a contextCSN from the suffix entry, it will scan
the entire database to determine the value, and this scan may take quite a long time on a large database. When
a contextCSN value is read, the database will still be scanned for any entryCSN values greater than it, to
make sure the contextCSN value truly reflects the greatest committed entryCSN in the database. On
databases which support inequality indexing, setting an eq index on the entryCSN attribute and configuring
contextCSN checkpoints will greatly speed up this scanning step.

If no contextCSN can be determined by reading and scanning the database, a new value will be generated.
Also, if scanning the database yielded a greater entryCSN than was previously recorded in the suffix entry's
contextCSN attribute, a checkpoint will be immediately written with the new value.

The consumer also stores its replica state, which is the provider's contextCSN received as a synchronization
cookie, in the contextCSN attribute of the suffix entry. The replica state maintained by a consumer server is
used as the synchronization state indicator when it performs subsequent incremental synchronization with the
provider server. It is also used as a provider-side synchronization state indicator when it functions as a
secondary provider server in a cascading replication configuration. Since the consumer and provider state
information are maintained in the same location within their respective databases, any consumer can be
promoted to a provider (and vice versa) without any special actions.

Because a general search filter can be used in the syncrepl specification, some entries in the context may be
omitted from the synchronization content. The syncrepl engine creates a glue entry to fill in the holes in the
replica context if any part of the replica content is subordinate to the holes. The glue entries will not be
returned in the search result unless ManageDsaIT control is provided.
Also as a consequence of the search filter used in the syncrepl specification, it is possible for a modification to remove an entry from the replication scope even though the entry has not been deleted on the provider. Logically the entry must be deleted on the consumer but in refreshOnly mode the provider cannot detect and propagate this change without the use of the session log.

### 16.3.3. Configuring Syncrepl

Because syncrepl is a consumer-side replication engine, the syncrepl specification is defined in `slapd.conf(5)` of the consumer server, not in the provider server's configuration file. The initial loading of the replica content can be performed either by starting the syncrepl engine with no synchronization cookie or by populating the consumer replica by adding an LDIF file dumped as a backup at the provider.

When loading from a backup, it is not required to perform the initial loading from the up-to-date backup of the provider content. The syncrepl engine will automatically synchronize the initial consumer replica to the current provider content. As a result, it is not required to stop the provider server in order to avoid the replica inconsistency caused by the updates to the provider content during the content backup and loading process.

When replicating a large scale directory, especially in a bandwidth constrained environment, it is advised to load the consumer replica from a backup instead of performing a full initial load using syncrepl.

#### 16.3.3.1. Set up the provider slapd

The provider is implemented as an overlay, so the overlay itself must first be configured in `slapd.conf(5)` before it can be used. The provider has only two configuration directives, for setting checkpoints on the contextCSN and for configuring the session log. Because the LDAP Sync search is subject to access control, proper access control privileges should be set up for the replicated content.

The contextCSN checkpoint is configured by the

```
 syncprov-checkpoint <ops> <minutes>
```

directive. Checkpoints are only tested after successful write operations. If `<ops>` operations or more than `<minutes>` time has passed since the last checkpoint, a new checkpoint is performed.

The session log is configured by the

```
 syncprov-sessionlog <size>
```

directive, where `<size>` is the maximum number of session log entries the session log can record. When a session log is configured, it is automatically used for all LDAP Sync searches within the database.

Note that using the session log requires searching on the `entryUUID` attribute. Setting an eq index on this attribute will greatly benefit the performance of the session log on the provider.

A more complete example of the `slapd.conf(5)` content is thus:

```
database bdb
suffix dc=Example,dc=com
rootdn dc=Example,dc=com
directory /var/ldap/db
index objectclass,entryCSN,entryUUID eq
```
16.3.3.2. Set up the consumer slapd

The syncrepl replication is specified in the database section of slapd.conf(5) for the replica context. The syncrepl engine is backend independent and the directive can be defined with any database type.

database hdb
suffix dc=Example,dc=com
rootdn dc=Example,dc=com
directory /var/ldap/db
index objectclass,entryCSN,entryUUID eq

syncrepl rid=123
  provider=ldap://provider.example.com:389
  type=refreshOnly
  interval=01:00:00:00
  searchbase="dc=example,dc=com"
  filter="(objectClass=organizationalPerson)"
  scope=sub
  attrs="cn,sn,ou,telephoneNumber,title,l"
  schemachecking=off
  bindmethod=simple
  binddn="cn=syncuser,dc=example,dc=com"
  credentials=secret

In this example, the consumer will connect to the provider slapd(8) at port 389 of ldap://provider.example.com to perform a polling (refreshOnly) mode of synchronization once a day. It will bind as cn=syncuser,dc=example,dc=com using simple authentication with password "secret". Note that the access control privilege of cn=syncuser,dc=example,dc=com should be set appropriately in the provider to retrieve the desired replication content. Also the search limits must be high enough on the provider to allow the syncuser to retrieve a complete copy of the requested content. The consumer uses the rootdn to write to its database so it always has full permissions to write all content.

The synchronization search in the above example will search for the entries whose objectClass is organizationalPerson in the entire subtree rooted at dc=example,dc=com. The requested attributes are cn, sn, ou, telephoneNumber, title, and l. The schema checking is turned off, so that the consumer slapd(8) will not enforce entry schema checking when it process updates from the provider slapd(8).

For more detailed information on the syncrepl directive, see the syncrepl section of The slapd Configuration File chapter of this admin guide.

16.3.3.3. Start the provider and the consumer slapd

The provider slapd(8) is not required to be restarted. contextCSN is automatically generated as needed: it might be originally contained in the LDIF file, generated by slapadd (8), generated upon changes in the context, or generated when the first LDAP Sync search arrives at the provider. If an LDIF file is being loaded which did not previously contain the contextCSN, the -w option should be used with slapadd (8) to cause it to be generated. This will allow the server to startup a little quicker the first time it runs.

When starting a consumer slapd(8), it is possible to provide a synchronization cookie as the -c cookie command line option in order to start the synchronization from a specific state. The cookie is a comma
separated list of name=value pairs. Currently supported syncrepl cookie fields are csn=<csn> and rid=<rid>. <csn> represents the current synchronization state of the consumer replica. <rid> identifies a consumer replica locally within the consumer server. It is used to relate the cookie to the syncrepl definition in slapd.conf(5) which has the matching replica identifier. The <rid> must have no more than 3 decimal digits. The command line cookie overrides the synchronization cookie stored in the consumer replica database.

16.4. N-Way Multi-Master

16.5. MirrorMode

16.5.1. Arguments for MirrorMode

- Provides a high-availability (HA) solution for directory writes (replicas handle reads)
- As long as one Master is operational, writes can safely be excepted
- Master nodes replicate from each other, so they are always up to date and can be ready to take over (hot standby)
- Syncrepl also allows the master nodes to re-synchronize after any downtime
- Delta-Syncrepl can be used

16.5.2. Arguments against MirrorMode

- MirrorMode is not what is termed as a Multi-Master solution. This is because writes have to go to one of the mirror nodes at a time
- MirrorMode can be termed as Active-Active Hot-Standby, therefore an external server (slapd in proxy mode) or device (hardware load balancer) to manage which master is currently active
- While syncrepl can recover from a completely empty database, slapadd is much faster
- Does not provide faster or more scalable write performance (neither could any Multi-Master solution)
- Backups are managed slightly differently
  - If backing up the Berkeley database itself and periodically backing up the transaction log files, then the same member of the mirror pair needs to be used to collect logfiles until the next database backup is taken
  - To ensure that both databases are consistent, each database might have to be put in read-only mode while performing a slapcat.
  - When using slapcat, the generated LDIF files can be rather large. This can happen with a non-MirrorMode deployment also.

16.5.3. MirrorMode Configuration

MirrorMode configuration is actually very easy. If you have ever setup a normal slapd syncrepl provider, then the only change is the directive:

```
mirrormode on
```

You also need to make you the rid of each mirror node pair is different and that the provider syncrepl directive points to the other mirror pair.
16.5.3.1. Mirror Node Configuration

This is the same as the Set up the provider slapd section, referencing delta-syncrepl replication if using `delta-syncrepl`.

Here's a specific cut down example using LDAP Sync Replication in `refreshAndPersist` mode (`delta-syncrepl` can be used also):

MirrorMode node 1:

```
# syncrepl directives
syncrepl     rid=1
    provider=ldap://ldap-rid2.example.com
    bindmethod=simple
    binddn="cn=mirrormode,dc=example,dc=com"
    credentials=mirrormode
    searchbase="dc=example,dc=com"
    schemachecking=on
    type=refreshAndPersist
    retry="60 +"

mirrormode on
```

MirrorMode node 2:

```
# syncrepl directives
syncrepl     rid=2
    provider=ldap://ldap-rid1.example.com
    bindmethod=simple
    binddn="cn=mirrormode,dc=example,dc=com"
    credentials=mirrormode
    searchbase="dc=example,dc=com"
    schemachecking=on
    type=refreshAndPersist
    retry="60 +"

mirrormode on
```

It's simple really; each MirrorMode node is setup exactly the same, except that the `provider` directive is set to point to the other MirrorMode node.

16.5.3.2. Failover Configuration

There are generally 2 choices for this; 1. Hardware proxies/load-balancing or dedicated proxy software, 2. using a Back-LDAP proxy as a syncrepl provider

MORE HERE and a nice PICTURE

16.5.3.3. Normal Consumer Configuration

This is exactly the same as the Set up the consumer slapd section. It can either setup in normal syncrepl replication mode, or in delta-syncrepl replication mode.
16.5.4. MirrorMode Summary

Hopefully you will now have a directory architecture that provides all of the consistency guarantees of single-master replication, whilst also providing the high availability of multi-master replication.
17. Maintenance

System Administration is all about maintenance, so it is only fair that we discuss how to correctly maintain an OpenLDAP deployment.

17.1. Directory Backups

Backup strategies largely depend on the amount of change in the database and how much of that change an administrator might be willing to lose in a catastrophic failure. There are two basic methods that can be used:

1. Backup the Berkeley database itself and periodically back up the transaction log files:

   Berkeley DB produces transaction logs that can be used to reconstruct changes from a given point in time. For example, if an administrator were willing to only lose one hour's worth of changes, they could take down the server in the middle of the night, copy the Berkeley database files offsite, and bring the server back online. Then, on an hourly basis, they could force a database checkpoint, capture the log files that have been generated in the past hour, and copy them offsite. The accumulated log files, in combination with the previous database backup, could be used with db_recover to reconstruct the database up to the time the last collection of log files was copied offsite. This method affords good protection, with minimal space overhead.

2. Periodically run slapcat and back up the LDIF file:

   Slapcat can be run while slapd is active. However, one runs the risk of an inconsistent database— not from the point of slapd, but from the point of the applications using LDAP. For example, if a provisioning application performed tasks that consisted of several LDAP operations, and the slapcat took place concurrently with those operations, then there might be inconsistencies in the LDAP database from the point of view of that provisioning application and applications that depended on it. One must, therefore, be convinced something like that won't happen. One way to do that would be to put the database in read-only mode while performing the slapcat. The other disadvantage of this approach is that the generated LDIF files can be rather large and the accumulation of the day's backups could add up to a substantial amount of space.

   You can use `slapcat(8)` to generate an LDIF file for each of your `slapd(8)` back-bdb or back-hdb databases.

   ```
   slapcat -f slapd.conf -b "dc=example,dc=com"
   ```

   For back-bdb and back-hdb, this command may be ran while slapd(8) is running.

   MORE on actual Berkeley DB backups later covering db_recover etc.

17.2. Berkeley DB Logs

Berkeley DB log files grow, and the administrator has to deal with it. The procedure is known as log file archival or log file rotation.

---

**Note:** The actual log file rotation is handled by the Berkeley DB engine.

Logs of current transactions need to be stored into files so that the database can be recovered in the event of an application crash. Administrators can change the size limit of a single log file (by default 10MB), and have old log files removed automatically, by setting up DB environment (see below). The reason Berkeley DB
never deletes any log files by default is that the administrator may wish to backup the log files before removal to make database recovery possible even after a catastrophic failure, such as file system corruption.

Log file names are log.XXXXXXXXX (X is a digit). By default the log files are located in the BDB backend directory. The db_archive tool knows what log files are used in current transactions, and what are not. Administrators can move unused log files to a backup media, and delete them. To have them removed automatically, place set_flags DB_LOG_AUTOREMOVE directive in DB_CONFIG.

Note: If the log files are removed automatically, recovery after a catastrophic failure is likely to be impossible.

The files with names __db.001, __db.002, etc are just shared memory regions (or whatever). These ARE NOT 'logs', they must be left alone. Don't be afraid of them, they do not grow like logs do.

To understand the db_archive interface, the reader should refer to chapter 9 of the Berkeley DB guide. In particular, the following chapters are recommended:

- Database and log file archival
- Log file removal
- Recovery procedures
- Hot failover

Advanced installations can use special environment settings to fine-tune some Berkeley DB options (change the log file limit, etc). This can be done by using the DB_CONFIG file. This magic file can be created in BDB backend directory set up by slapd.conf(5). More information on this file can be found in File naming chapter. Specific directives can be found in C Interface, look for DB_ENV->set_XXXX calls.

Note: options set in DB_CONFIG file override options set by OpenLDAP. Use them with extreme caution. Do not use them unless You know what You are doing.

The advantages of DB_CONFIG usage can be the following:

- to keep data files and log files on different mediums (i.e. disks) to improve performance and/or reliability;
- to fine-tune some specific options (such as shared memory region sizes);
- to set the log file limit (please read Log file limits before doing this).

To figure out the best-practice BDB backup scenario, the reader is highly recommended to read the whole Chapter 9: Berkeley DB Transactional Data Store Applications. This chapter is a set of small pages with examples in C language. Non-programming people can skip this examples without loss of knowledge.

17.3. Checkpointing

MORE/TIDY

If you put "checkpoint 1024 5" in slapd.conf (to checkpoint after 1024kb or 5 minutes, for example), this does not checkpoint every 5 minutes as you may think. The explanation from Howard is:

'In OpenLDAP 2.1 and 2.2 the checkpoint directive acts as follows - *when there is a write operation*, and more than <check> minutes have occurred since the last checkpoint, perform the checkpoint. If more than
<check> minutes pass after a write without any other write operations occurring, no checkpoint is performed, so it's possible to lose the last write that occurred."

In other words, a write operation occurring less than "check" minutes after the last checkpoint will not be checkpointed until the next write occurs after "check" minutes have passed since the checkpoint.

This has been modified in 2.3 to indeed checkpoint every so often; in the meantime a workaround is to invoke "db_checkpoint" from a cron script every so often, say 5 minutes.

17.4. Migration

Exporting to a new system......
18. Monitoring

`slapd`(8) supports an optional LDAP monitoring interface you can use to obtain information regarding the current state of your `slapd` instance. For instance, the interface allows you to determine how many clients are connected to the server currently. The monitoring information is provided by a specialized backend, the `monitor` backend. A manual page, `slapd-monitor`(5) is available.

When the monitoring interface is enabled, LDAP clients may be used to access information provided by the `monitor` backend, subject to access and other controls.

When enabled, the `monitor` backend dynamically generates and returns objects in response to search requests in the `cn=Monitor` subtree. Each object contains information about a particular aspect of the server. The information is held in a combination of user applications and operational attributes. This information can be access with `ldapsearch(1)`, with any general-purpose LDAP browser, or with specialized monitoring tools. The Accessing Monitoring Information section provides a brief tutorial on how to use `ldapsearch(1)` to access monitoring information, while the Monitor information section details monitoring information base and its organization.

While support for the monitor backend is included in default builds of `slapd`(8), this support requires some configuration to become active. This may be done using either `cn=config` or `slapd.conf`(5). The former is discussed in the Monitor configuration via `cn=config` section of this chapter. The latter is discussed in the Monitor configuration via `slapd.conf`(5) section of this chapter. These sections assume monitor backend is built into `slapd` (e.g., `--enable-monitor=yes`, the default). If the monitor backend was built as a module (e.g., `--enable-monitor=mod`, this module must loaded. Loading of modules is discussed in the Configuring slapd and The slapd Configuration File chapters.

18.1. Monitor configuration via `cn=config`(5)

*This section has yet to be written.*

18.2. Monitor configuration via `slapd.conf`(5)

Configuration of the `slapd.conf`(5) to support LDAP monitoring is quite simple.

First, ensure `core.schema` schema configuration file is included by your `slapd.conf`(5) file. The `monitor` backend requires it.

Second, instantiate the `monitor backend` by adding a `database monitor` directive below your existing database sections. For instance:

```
database monitor
```

Lastly, add additional global or database directives as needed.

Like most other database backends, the monitor backend does honor `slapd`(8) access and other administrative controls. As some monitor information may be sensitive, it is generally recommend access to `cn=monitor` be restricted to directory administrators and their monitoring agents. Adding an `access` directive immediately below the `database monitor` directive is a clear and effective approach for controlling access. For instance, the addition of the following `access` directive immediately below the `database monitor` directive restricts access to

131
monitoring information to the specified directory manager.

```
access to *
    by dn.exact="cn=Manager,dc=example,dc=com"
    by * none
```

More information on `slapd(8)` access controls, see *The access Control Directive* section of the The slapd Configuration File chapter and `slapd.access(5)`.

After restarting `slapd(8)`, you are ready to start exploring the monitoring information provided in `cn=config` as discussed in the Accessing Monitoring Information section of this chapter.

One can verify `slapd(8)` is properly configured to provide monitoring information by attempting to read the `cn=monitor` object. For instance, if the following `ldapsearch(1)` command returns the `cn=monitor` object (with, as requested, no attributes), it's working.

```
ldapsearch -x -D 'cn=Manager,dc=example,dc=com' -W \
    -b 'cn=Monitor' -s base 1.1
```

Note that unlike general purpose database backends, the database suffix is hardcoded. It's always `cn=Monitor`. So no `suffix` directive should be provided. Also note that general purpose database backends, the monitor backend cannot be instantiated multiple times. That is, there can only be one (or zero) occurrences of database monitor in the server's configuration.

### 18.3. Accessing Monitoring Information

As previously discussed, when enabled, the `monitor` backend dynamically generates and returns objects in response to search requests in the `cn=Monitor` subtree. Each object contains information about a particular aspect of the server. The information is held in a combination of user applications and operational attributes. This information can be access with `ldapsearch(1)`, with any general-purpose LDAP browser, or with specialized monitoring tools.

This section provides a provides a brief tutorial on how to use `ldapsearch(1)` to access monitoring information.

To inspect any particular monitor object, one performs search operation on the object with a baseObject scope and a `(objectClass=*)` filter. As the monitoring information is contained in a combination of user applications and operational attributes, the return all user applications attributes (e.g., `'*'`) and all operational attributes (e.g., `'+'`) should be requested. For instance, to read the `cn=Monitor` object itself, the `ldapsearch(1)` command (modified to fit your configuration) can be used:

```
ldapsearch -x -D 'cn=Manager,dc=example,dc=com' -W \
    -b 'cn=Monitor' -s base '(objectClass=*)' '*+'
```

When run against your server, this should produce output similar to:

```
dn: cn=Monitor
objectClass: monitorServer
structuralObjectClass: monitorServer
cn: Monitor
creatorsName: 
modifiersName: 
createTimestamp: 20061208223558Z
```
To reduce the number of uninteresting attributes returned, one can be more selective when requesting which attributes are to be returned. For instance, one could request the return of all attributes allowed by the monitorServer object class (e.g., @objectClass) instead of all user and all operational attributes:

```
ldapsearch -x -D 'cn=Manager,dc=example,dc=com' -W -b 'cn=Monitor' -s base '(objectClass=*)' '@monitorServer'
```

This limits the output as follows:

```
 dn: cn=Monitor
 objectClass: monitorServer
 cn: Monitor
 description: This subtree contains monitoring/managing objects.
 description: This object contains information about this server.
 description: Most of the information is held in operational attributes, which
 must be explicitly requested.
 monitoredInfo: OpenLDAP: slapd 2.X (Dec 7 2006 17:30:29)
```

To return the names of all the monitoring objects, one performs a search of cn=Monitor with subtree scope and (objectClass=*) filter and requesting no attributes (e.g., 1.1) be returned.

```
ldapsearch -x -D 'cn=Manager,dc=example,dc=com' -W -b 'cn=Monitor' -s sub 1.1
```

If you run this command you will discover that there are many objects in the cn=Monitor subtree. The following section describes some of the commonly available monitoring objects.

### 18.4. Monitor Information

The monitor backend provides a wealth of information useful for monitoring the slapd(8) contained in set of monitor objects. Each object contains information about a particular aspect of the server, such as a backends, a connection, or a thread. Some objects serve as containers for other objects and used to construct a hierarchy of objects.

In this hierarchy, the most superior object is {cn=Monitor}. While this object primarily serves as a container for other objects, most of which are containers, this object provides information about this server. In particular, it provides the slapd(8) version string. Example:

```
 dn: cn=Monitor
 monitoredInfo: OpenLDAP: slapd 2.X (Dec 7 2006 17:30:29)
```

**Note:** Examples in this section (and its subsections) have been trimmed to show only key information.
18.4.1. Backends

The `cn=Backends,cn=Monitor` object, itself, provides a list of available backends. The list of available backends all built-in backends, as well as backends loaded by modules. For example:

```
dn: cn=Backends,cn=Monitor
  monitoredInfo: config
  monitoredInfo: ldif
  monitoredInfo: monitor
  monitoredInfo: bdb
  monitoredInfo: hdb
```

This indicates the `config`, `ldif`, `monitor`, `bdb`, and `hdb` backends are available.

The `cn=Backends,cn=Monitor` object is also a container for available backend objects. Each available backend object contains information about a particular backend. For example:

```
dn: cn=Backend 0,cn=Backends,cn=Monitor
  monitoredInfo: config
  monitorRuntimeConfig: TRUE
  supportedControl: 2.16.840.1.113730.3.4.2
  seeAlso: cn=Database 0,cn=Databases,cn=Monitor

dn: cn=Backend 1,cn=Backends,cn=Monitor
  monitoredInfo: ldif
  monitorRuntimeConfig: TRUE
  supportedControl: 2.16.840.1.113730.3.4.2

dn: cn=Backend 2,cn=Backends,cn=Monitor
  monitoredInfo: monitor
  monitorRuntimeConfig: TRUE
  supportedControl: 2.16.840.1.113730.3.4.2
  seeAlso: cn=Database 2,cn=Databases,cn=Monitor

dn: cn=Backend 3,cn=Backends,cn=Monitor
  monitoredInfo: bdb
  monitorRuntimeConfig: TRUE
  supportedControl: 1.3.6.1.1.12
  supportedControl: 2.16.840.1.113730.3.4.2
  supportedControl: 1.3.6.1.4.1.4203.666.5.2
  supportedControl: 1.2.840.113556.1.4.319
  supportedControl: 1.3.6.1.1.13.1
  supportedControl: 1.3.6.1.1.13.2
  supportedControl: 1.3.6.1.4.1.4203.1.10.1
  supportedControl: 1.2.840.113556.1.4.1413
  supportedControl: 1.3.6.1.4.1.4203.666.11.7.2
  seeAlso: cn=Database 1,cn=Databases,cn=Monitor

dn: cn=Backend 4,cn=Backends,cn=Monitor
  monitoredInfo: hdb
  monitorRuntimeConfig: TRUE
  supportedControl: 1.3.6.1.1.12
  supportedControl: 2.16.840.1.113730.3.4.2
  supportedControl: 1.3.6.1.4.1.4203.666.5.2
  supportedControl: 1.2.840.113556.1.4.319
  supportedControl: 1.3.6.1.1.13.1
  supportedControl: 1.3.6.1.1.13.2
  supportedControl: 1.3.6.1.4.1.4203.1.10.1
  supportedControl: 1.2.840.113556.1.4.1413
  supportedControl: 1.3.6.1.4.1.4203.666.11.7.2
  seeAlso: cn=Database 1,cn=Databases,cn=Monitor
```
For each of these objects, `monitorInfo` indicates which backend the information in the object is about. For instance, the `cn=Backend 3,cn=Backends,cn=Monitor` object contains (in the example) information about the `bdb` backend.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitoredInfo</td>
<td>Name of backend</td>
</tr>
<tr>
<td>supportedControl</td>
<td>supported LDAP control extensions</td>
</tr>
<tr>
<td>seeAlso</td>
<td>Database objects of instances of this backend</td>
</tr>
</tbody>
</table>

### 18.4.2. Connections

The main entry is empty; it should contain some statistics on the number of connections.

Dynamic child entries are created for each open connection, with stats on the activity on that connection (the format will be detailed later). There are two special child entries that show the number of total and current connections respectively.

For example:

**Total Connections:**

```
    dn: cn=Total,cn=Connections,cn=Monitor
    structuralObjectClass: monitorCounterObject
    monitorCounter: 4
    entryDN: cn=Total,cn=Connections,cn=Monitor
    subschemaSubentry: cn=Subschema
    hasSubordinates: FALSE
```

**Current Connections:**

```
    dn: cn=Current,cn=Connections,cn=Monitor
    structuralObjectClass: monitorCounterObject
    monitorCounter: 2
    entryDN: cn=Current,cn=Connections,cn=Monitor
    subschemaSubentry: cn=Subschema
    hasSubordinates: FALSE
```

### 18.4.3. Databases

The main entry contains the naming context of each configured database; the child entries contain, for each database, the type and the naming context.

For example:

```
    dn: cn=Database 2,cn=Databases,cn=Monitor
    structuralObjectClass: monitoredObject
    monitoredInfo: monitor
    monitorIsShadow: FALSE
    monitorContext: cn=Monitor
    readOnly: FALSE
    entryDN: cn=Database 2,cn=Databases,cn=Monitor
    subschemaSubentry: cn=Subschema
```
18.4.4. Listener

It contains the description of the devices the server is currently listening on:

```
 dn: cn=Listener 0,cn=Listeners,cn=Monitor  
 structuralObjectClass: monitoredObject  
 monitorConnectionLocalAddress: IP=0.0.0.0:389  
 entryDN: cn=Listener 0,cn=Listeners,cn=Monitor  
 subschemaSubentry: cn=Subschema  
 hasSubordinates: FALSE
```
There are too many types to list example here, so please try for yourself using Monitor search example

### 18.4.7. Overlays

The main entry contains the type of overlays available at run-time; the child entries, for each overlay, contain the type of the overlay.

It should also contain the modules that have been loaded if dynamic overlays are enabled:

```bash
# Overlays, Monitor
dn: cn=Overlays,cn=Monitor
structuralObjectClass: monitorContainer
monitoredInfo: syncprov
monitoredInfo: accesslog
monitoredInfo: glue
entryDN: cn=Overlays,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: TRUE
```

### 18.4.8. SASL

Currently empty.

### 18.4.9. Statistics

It shows some statistics on the data sent by the server:

```bash
# Entries, Statistics, Monitor
dn: cn=Entries,cn=Statistics,cn=Monitor
structuralObjectClass: monitorCounterObject
monitorCounter: 612248
entryDN: cn=Entries,cn=Statistics,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE
```

### 18.4.10. Threads

It contains the maximum number of threads enabled at startup and the current backload.

```bash
# Max, Threads, Monitor
dn: cn=Max,cn=Threads,cn=Monitor
structuralObjectClass: monitoredObject
monitoredInfo: 16
entryDN: cn=Max,cn=Threads,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE
```
18.4.11. Time

It contains two child entries with the start time and the current time of the server.

e.g.

Start time:

dn: cn=Start,cn=Time,cn=Monitor
structuralObjectClass: monitoredObject
monitorTimestamp: 20061205124040Z
entryDN: cn=Start,cn=Time,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE

Current time:

dn: cn=Current,cn=Time,cn=Monitor
structuralObjectClass: monitoredObject
monitorTimestamp: 20061207120624Z
entryDN: cn=Current,cn=Time,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE

18.4.12. TLS

Currently empty.

18.4.13. Waiters

It contains the number of current read waiters.

e.g.

Read waiters:

dn: cn=Read,cn=Waiters,cn=Monitor
structuralObjectClass: monitorCounterObject
monitorCounter: 7
entryDN: cn=Read,cn=Waiters,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE

Write waiters:

dn: cn=Write,cn=Waiters,cn=Monitor
structuralObjectClass: monitorCounterObject
monitorCounter: 0
entryDN: cn=Write,cn=Waiters,cn=Monitor
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE

Add new monitored things here and discuss, referencing man pages and present examples
19. Tuning

This is perhaps one of the most important chapters in the guide, because if you have not tuned *slapd*(8) correctly or grasped how to design your directory and environment, you can expect very poor performance.

Reading, understanding and experimenting using the instructions and information in the following sections, will enable you to fully understand how to tailor your directory server to your specific requirements.

It should be noted that the following information has been collected over time from our community based FAQ. So obviously the benefit of this real world experience and advice should be of great value to the reader.

19.1. Performance Factors

Various factors can play a part in how your directory performs on your chosen hardware and environment. We will attempt to discuss these here.

19.1.1. Memory

Scale your cache to use available memory and increase system memory if you can.

More info here.

19.1.2. Disks

Use fast subsystems. Put each database and logs on separate disks.

Example showing config settings

19.1.3. Network Topology

http://www.openldap.org/faq/data/cache/363.html

Drawing here.

19.1.4. Directory Layout Design

Reference to other sections and good/bad drawing here.

19.1.5. Expected Usage

Discussion.

19.2. Indexes

19.2.1. Understanding how a search works

If you're searching on a filter that has been indexed, then the search reads the index and pulls exactly the entries that are referenced by the index. If the filter term has not been indexed, then the search must read every
single entry in the target scope and test to see if each entry matches the filter. Obviously indexing can save a lot of work when it's used correctly.

19.2.2. What to index

You should create indices to match the actual filter terms used in search queries.

    index cn,sn,givenname,mail eq

Each attribute index can be tuned further by selecting the set of index types to generate. For example, substring and approximate search for organizations (o) may make little sense (and isn't like done very often). And searching for userPassword likely makes no sense what so ever.

General rule: don't go overboard with indexes. Unused indexes must be maintained and hence can only slow things down.

See slapd.conf(8) and slapdindex(8) for more information

19.2.3. Presence indexing

If your client application uses presence filters and if the target attribute exists on the majority of entries in your target scope, then all of those entries are going to be read anyway, because they are valid members of the result set. In a subtree where 100% of the entries are going to contain the same attributes, the presence index does absolutely NOTHING to benefit the search, because 100% of the entries match that presence filter.

So the resource cost of generating the index is a complete waste of CPU time, disk, and memory. Don't do it unless you know that it will be used, and that the attribute in question occurs very infrequently in the target data.

Almost no applications use presence filters in their search queries. Presence indexing is pointless when the target attribute exists on the majority of entries in the database. In most LDAP deployments, presence indexing should not be done, it's just wasted overhead.

See the Logging section below on what to watch our for if you have a frequently searched for attribute that is unindexed.

19.3. Logging

19.3.1. What log level to use

The default of loglevel 256 is really the best bet. There's a corollary to this when problems *do* arise, don't try to trace them using syslog. Use the debug flag instead, and capture slapd's stderr output. syslog is too slow for debug tracing, and it's inherently lossy - it will throw away messages when it can't keep up.

Contrary to popular belief, loglevel 0 is not ideal for production as you won't be able to track when problems first arise.
19.3.2. What to watch out for

The most common message you'll see that you should pay attention to is:

```
"<= bdb_equality_candidates: (foo) index_param failed (18)"
```

That means that some application tried to use an equality filter (foo=<somevalue>) and attribute foo does not have an equality index. If you see a lot of these messages, you should add the index. If you see one every month or so, it may be acceptable to ignore it.

The default syslog level is 256 which logs the basic parameters of each request; it usually produces 1-3 lines of output. On Solaris and systems that only provide synchronous syslog, you may want to turn it off completely, but usually you want to leave it enabled so that you'll be able to see index messages whenever they arise. On Linux you can configure syslogd to run asynchronously, in which case the performance hit for moderate syslog traffic pretty much disappears.

19.3.3. Improving throughput

You can improve logging performance on some systems by configuring syslog not to sync the file system with every write (man syslogd/syslog.conf). In Linux, you can prepend the log file name with a "-" in syslog.conf. For example, if you are using the default LOCAL4 logging you could try:

```
# LDAP logs
LOCAL4.*               -/var/log/ldap
```

For syslog-ng, add or modify the following line in syslog-ng.conf:

```
options { sync(n); }; 
```

where n is the number of lines which will be buffered before a write.

19.4. BDB/HDB Database Caching

We all know what caching is, don't we?

In brief, "A cache is a block of memory for temporary storage of data likely to be used again" - http://en.wikipedia.org/wiki/Cache

There are 3 types of caches, BerkeleyDB's own cache, slapd(8) entry cache and IDL (IDL) cache.

19.4.1. Berkeley DB Cache

BerkeleyDB's own data cache operates on page-sized blocks of raw data.

Note that while the BDB cache is just raw chunks of memory and configured as a memory size, the slapd(8) entry cache holds parsed entries, and the size of each entry is variable.

There is also an IDL cache which is used for Index Data Lookups. If you can fit all of your database into slapd's entry cache, and all of your index lookups fit in the IDL cache, that will provide the maximum throughput.
If not, but you can fit the entire database into the BDB cache, then you should do that and shrink the slapd entry cache as appropriate.

Failing that, you should balance the BDB cache against the entry cache.

It is worth noting that it is not absolutely necessary to configure a BerkeleyDB cache equal in size to your entire database. All that you need is a cache that's large enough for your "working set."

That means, large enough to hold all of the most frequently accessed data, plus a few less-frequently accessed items.

ORACLE LINKS HERE

19.4.1.1. Calculating Cachesize

The back-bdb database lives in two main files, `dn2id.bdb` and `id2entry.bdb`. These are B-tree databases. We have never documented the back-bdb internal layout before, because it didn't seem like something anyone should have to worry about, nor was it necessarily cast in stone. But here's how it works today, in OpenLDAP 2.4.

A B-tree is a balanced tree; it stores data in its leaf nodes and bookkeeping data in its interior nodes (If you don't know what tree data structures look like in general, Google for some references, because that's getting far too elementary for the purposes of this discussion).

For decent performance, you need enough cache memory to contain all the nodes along the path from the root of the tree down to the particular data item you're accessing. That's enough cache for a single search. For the general case, you want enough cache to contain all the internal nodes in the database.

```
  db_stat -d
```

will tell you how many internal pages are present in a database. You should check this number for both `dn2id` and `id2entry`.

Also note that `id2entry` always uses 16KB per "page", while `dn2id` uses whatever the underlying filesystem uses, typically 4 or 8KB. To avoid thrashing the, your cache must be at least as large as the number of internal pages in both the `dn2id` and `id2entry` databases, plus some extra space to accommodate the actual leaf data pages.

For example, in my OpenLDAP 2.4 test database, I have an input LDIF file that's about 360MB. With the back-hdb backend this creates a `dn2id.bdb` that's 68MB, and an `id2entry` that's 800MB. `db_stat` tells me that `dn2id` uses 4KB pages, has 433 internal pages, and 6378 leaf pages. The `id2entry` uses 16KB pages, has 52 internal pages, and 45912 leaf pages. In order to efficiently retrieve any single entry in this database, the cache should be at least

```
(433+1) * 4KB + (52+1) * 16KB in size: 1736KB + 848KB =~ 2.5MB.
```

This doesn't take into account other library overhead, so this is even lower than the barest minimum. The default cache size, when nothing is configured, is only 256KB.

This 2.5MB number also doesn't take indexing into account. Each indexed attribute uses another database file of its own, using a Hash structure.
Unlike the B-trees, where you only need to touch one data page to find an entry of interest, doing an index lookup generally touches multiple keys, and the point of a hash structure is that the keys are evenly distributed across the data space. That means there's no convenient compact subset of the database that you can keep in the cache to insure quick operation, you can pretty much expect references to be scattered across the whole thing. My strategy here would be to provide enough cache for at least 50% of all of the hash data.

\[
(Number \text{ of hash buckets } + \text{ number of overflow pages } + \text{ number of duplicate pages}) \times \text{ page size} / 2.
\]

The objectClass index for my example database is 5.9MB and uses 3 hash buckets and 656 duplicate pages. So:

\[
(3 + 656) \times 4\text{KB} / 2 \approx 1.3\text{MB}.
\]

With only this index enabled, I'd figure at least a 4MB cache for this backend. (Of course you're using a single cache shared among all of the database files, so the cache pages will most likely get used for something other than what you accounted for, but this gives you a fighting chance.)

With this 4MB cache I can slapcat this entire database on my 1.3GHz PIII in 1 minute, 40 seconds. With the cache doubled to 8MB, it still takes the same 1:40s. Once you've got enough cache to fit the B-tree internal pages, increasing it further won't have any effect until the cache really is large enough to hold 100% of the data pages. I don't have enough free RAM to hold all the 800MB id2entry data, so 4MB is good enough.

With back-bdb and back-hdb you can use "db_stat -m" to check how well the database cache is performing.

**19.4.2. slapd(8) Entry Cache**

The slapd(8) entry cache operates on decoded entries. The rationale - entries in the entry cache can be used directly, giving the fastest response. If an entry isn't in the entry cache but can be extracted from the BDB page cache, that will avoid an I/O but it will still require parsing, so this will be slower.

If the entry is in neither cache then BDB will have to flush some of its current cached pages and bring in the needed pages, resulting in a couple of expensive I/Os as well as parsing.

As far as balancing the entry cache vs the BDB cache - parsed entries in memory are generally about twice as large as they are on disk.

As we have already mentioned, not having a proper database cache size will cause performance issues. These issues are not an indication of corruption occurring in the database. It is merely the fact that the cache is thrashing itself that causes performance/response time to slowdown.

**MOVE BELOW AROUND:**

If you want to setup the cache size, please read:

(Xref) How do I configure the BDB backend? (Xref) What are the DB_CONFIG configuration directives?
http://www.sleepycat.com/docs/utility/db_recover.html

A default config can be found in the answer:

(Xref) What are the DB_CONFIG configuration directives?
just change the set_lg_dir to point to your .log directory or comment that line.

Quick guide:

- Create a DB_CONFIG file in your ldap home directory (/var/lib/ldap/DB_CONFIG) with the correct "set_cachesize" value
- stop your ldap server and run db_recover -h /var/lib/ldap
- start your ldap server and check the new cache size with:

  db_stat -h /var/lib/ldap -m | head -n 2

- this procedure is only needed if you use OpenLDAP 2.2 with the BDB or HDB backends; In OpenLDAP 2.3 DB recovery is performed automatically whenever the DB_CONFIG file is changed or when an unclean shutdown is detected.

◊ On Tuesday, February 22, 2005 12:15 PM -0500 Dusty Doris <openldap@mail.doris.cc> wrote:

Few questions, if you change the cachesize and idlecachesize entries, do you have to do anything special aside from restarting slapd, such as run slapindex or db_recover?

Also, is there any way to tell how much memory these caches are taking up to make sure they are not set too large? What happens if you set your cachesize too large and you don’t have enough available memory to store these? Will that cause an issue with openldap, or will it just not cache those entries that would make it exceed its available memory. Will it just use some sort of FIFO on those caches?

It will consume the memory resources of your system, and likely cause issues.

Finally, what do most people try to achieve with these values? Would the goal be to make these as big as the directory? So, if I have 400,000 dn's in my directory, would it be safe to set these at 400000 or would something like 20,000 be good enough to get a nice performance increase?

I try to cache the most actively used entries. Unless you expect all 400,000 entries of your DB to be accessed regularly, there is no need to cache that many entries. My entry cache is set to 20,000 (out of a little over 400,000 entries).

The idlcache has to do with how many unique result sets of searches you want to store in memory. Setting up this cache will allow your most frequently placed searches to get results much faster, but I doubt you want to try and cache the results of every search that hits your system. ;)

◊ Quanah

19.4.3. IDL Cache

http://www.openldap.org/faq/data/cache/1076.html
20. Troubleshooting

If you're having trouble using OpenLDAP, get onto the OpenLDAP-Software mailing list, or:

- Browse the list archives at http://www.openldap.org/lists/#archives
- Search the FAQ at http://www.openldap.org/faq/
- Search the Issue Tracking System at http://www.openldap.org/its/

Chances are the problem has been solved and explained in detail many times before.

20.1. User or Software errors?

More often than not, an error is caused by a configuration problem or a misunderstanding of what you are trying to implement and/or achieve.

We will now attempt to discuss common user errors.

20.2. Checklist

The following checklist can help track down your problem. Please try to use if before posting to the list, or in the rare circumstances of reporting a bug.

1. Use the slaptest tool to verify configurations before starting slapd

2. Verify that slapd is listening to the specified port(s) (389 and 636, generally) before trying the ldapsearch

3. Can you issue an ldapsearch?

4. If not, have you enabled complex ACLs without fully understanding them?

5. Do you have a system wide LDAP setting pointing to the wrong LDAP Directory?

6. Are you using TLS?

7. Have your certificates expired?

20.3. OpenLDAP Bugs

Sometimes you may encounter an actual OpenLDAP bug, in which case please visit our Issue Tracking system http://www.openldap.org/its/ and report it. However, make sure it's not already a known bug or a common user problem.

- bugs in historic versions of OpenLDAP will not be considered;
- bugs in released versions that are no longer present in HEAD code, either because they have been fixed or because they no longer apply, will not be considered as well;
• bugs in distributions of OpenLDAP software that are not related to the software as provided by OpenLDAP will not be considered; in those cases please refer to the distributor.

Note: Our Issue Tracking system is NOT for OpenLDAP Support, please join our mailing Lists: http://www.openldap.org/lists/ for that.

The information you should provide in your bug report is discussed in our FAQ-O-MATIC at http://www.openldap.org/faq/data/cache/59.html

20.4. 3rd party software error

The OpenLDAP Project only supports OpenLDAP software.

You may however seek commercial support (http://www.openldap.org/support/) or join the general LDAP forum for non-commercial discussions and information relating to LDAP at: http://www.umich.edu/~dirsvcs/ldap/mailinglist.html

20.5. How to contact the OpenLDAP Project

• Mailing Lists: http://www.openldap.org/lists/
• Project: http://www.openldap.org/project/
• Issue Tracking: http://www.openldap.org/its/

20.6. How to present your problem

20.7. Debugging *slapd*(8)

After reading through the above sections and before e-mailing the OpenLDAP lists, you might want to try out some of the following to track down the cause of your problems:

• Loglevel 256 is generally a good first loglevel to try for getting information useful to list members on issues
• Running *slapd* -d -1 can often track down fairly simple issues, such as missing schemas and incorrect file permissions for the *slapd* user to things like certs
• Check your logs for errors, as discussed at http://www.openldap.org/faq/data/cache/358.html

20.8. Commercial Support

The firms listed at http://www.openldap.org/support/ offer technical support services catering to OpenLDAP community.

The listing of any given firm should not be viewed as an endorsement or recommendation of any kind, nor as otherwise indicating there exists a business relationship or an affiliation between any listed firm and the OpenLDAP Foundation or the OpenLDAP Project or its contributors.
A. Changes Since Previous Release

The following sections attempt to summarize the new features and changes in OpenLDAP software since the 2.3.x release and the OpenLDAP Admin Guide.

A.1. New Guide Sections

In order to make the Admin Guide more thorough and cover the majority of questions asked on the OpenLDAP mailing lists and scenarios discussed there, we have added the following new sections:

- When should I use LDAP?
- When should I not use LDAP?
- LDAP vs RDBMS
- Backends
- Overlays
- Replication
- Maintenance
- Monitoring
- Tuning
- Troubleshooting
- Changes Since Previous Release
- Upgrading from 2.3.x
- Common errors encountered when using OpenLDAP Software
- Recommended OpenLDAP Software Dependency Versions
- Real World OpenLDAP Deployments and Examples
- OpenLDAP Software Contributions
- Configuration File Examples
- LDAP Result Codes
- Glossary

Also, the table of contents is now 3 levels deep to ease navigation.

A.2. New Features and Enhancements in 2.4

A.2.1. Better cn=config functionality

There is a new slapd-config(5) manpage for the **cn=config** backend. The original design called for auto-renaming of config entries when you insert or delete entries with ordered names, but that was not implemented in 2.3. It is now in 2.4. This means, e.g., if you have

```plaintext
olcDatabase={1}bdb, cn=config
olcSuffix: dc=example, dc=com
```

and you want to add a new subordinate, now you can ldapadd:

```plaintext
olcDatabase={1}bdb, cn=config
olcSuffix: dc=foo, dc=example, dc=com
```

This will insert a new BDB database in slot 1 and bump all following databases down one, so the original BDB database will now be named:
A.2.2. Better cn=schema functionality

In 2.3 you were only able to add new schema elements, not delete or modify existing elements. In 2.4 you can modify schema at will. (Except for the hardcoded system schema, of course.)

A.2.3. More sophisticated Syncrepl configurations

The original implementation of Syncrepl in OpenLDAP 2.2 was intended to support multiple consumers within the same database, but that feature never worked and was removed from OpenLDAP 2.3; you could only configure a single consumer in any database.

In 2.4 you can configure multiple consumers in a single database. The configuration possibilities here are quite complex and numerous. You can configure consumers over arbitrary subtrees of a database (disjoint or overlapping). Any portion of the database may in turn be provided to other consumers using the Syncprov overlay. The Syncprov overlay works with any number of consumers over a single database or over arbitrarily many glued databases.

A.2.4. N-Way Multimaster Replication

As a consequence of the work to support multiple consumer contexts, the syncrepl system now supports full N-Way multimaster replication with entry-level conflict resolution. There are some important constraints, of course: In order to maintain consistent results across all servers, you must maintain tightly synchronized clocks across all participating servers (e.g., you must use NTP on all servers).

The entryCSNs used for replication now record timestamps with microsecond resolution, instead of just seconds. The delta-syncrepl code has not been updated to support multimaster usage yet, that will come later in the 2.4 cycle.

A.2.5. Replicating slapd Configuration (syncrepl and cn=config)

Syncrepl was explicitly disabled on cn=config in 2.3. It is now fully supported in 2.4; you can use syncrepl to replicate an entire server configuration from one server to arbitrarily many other servers. It's possible to clone an entire running slapd using just a small (less than 10 lines) seed configuration, or you can just replicate the schema subtrees, etc. Tests 049 and 050 in the test suite provide working examples of these capabilities.

A.2.6. Push-Mode Replication

In 2.3 you could configure syncrepl as a full push-mode replicator by using it in conjunction with a back-ldap pointed at the target server. But because the back-ldap database needs to have a suffix corresponding to the target's suffix, you could only configure one instance per slapd.

In 2.4 you can define a database to be "hidden", which means that its suffix is ignored when checking for name collisions, and the database will never be used to answer requests received by the frontend. Using this "hidden" database feature allows you to configure multiple databases with the same suffix, allowing you to set up multiple back-ldap instances for pushing replication of a single database to multiple targets. There may be other uses for hidden databases as well (e.g., using a syncrepl consumer to maintain a *local* mirror of a database on a separate filesystem).
A.2.7. More extensive TLS configuration control

In 2.3, the TLS configuration in slapd was only used by the slapd listeners. For outbound connections used by e.g. back-ldap or syncrepl their TLS parameters came from the system's ldap.conf file.

In 2.4 all of these sessions inherit their settings from the main slapd configuration, but settings can be individually overridden on a per-config-item basis. This is particularly helpful if you use certificate-based authentication and need to use a different client certificate for different destinations.

A.2.8. Performance enhancements

Too many to list. Some notable changes - ldapadd used to be a couple of orders of magnitude slower than "slapadd -q". It's now at worst only about half the speed of slapadd -q. Some comparisons of all the 2.x OpenLDAP releases are available at http://www.openldap.org/pub/hyc/scale2007.pdf

That compared 2.0.27, 2.1.30, 2.2.30, 2.3.33, and HEAD). Toward the latter end of the "Cached Search Performance" chart it gets hard to see the difference because the run times are so small, but the new code is about 25% faster than 2.3, which was about 20% faster than 2.2, which was about 100% faster than 2.1, which was about 100% faster than 2.0, in that particular search scenario. That test basically searched a 1.3GB DB of 380836 entries (all in the slapd entry cache) in under 1 second. i.e., on a 2.4GHz CPU with DDR400 ECC/Registered RAM we can search over 500 thousand entries per second. The search was on an unindexed attribute using a filter that would not match any entry, forcing slapd to examine every entry in the DB, testing the filter for a match.

Essentially the slapd entry cache in back-bdb/back-hdb is so efficient the search processing time is almost invisible; the runtime is limited only by the memory bandwidth of the machine. (The search data rate corresponds to about 3.5GB/sec; the memory bandwidth on the machine is only about 4GB/sec due to ECC and register latency.)

A.2.9. New overlays

- slapo-constraint (Attribute value constraints)
- slapo-dds (Dynamic Directory Services, RFC 2589)
- slapo-memberof (reverse group membership maintenance)

A.2.10. New features in existing Overlays

- slapo-pcache
  - Inspection/Maintenance
    - the cache database can be directly accessed via LDAP by adding a specific control to each LDAP request; a specific extended operation allows to consistently remove cached entries and entire cached queries
  - Hot Restart
    - cached queries are saved on disk at shutdown, and reloaded if not expired yet at subsequent restart
- slapo-rwm can safely interoperable with other overlays
- Dyningroup/Dynlist merge, plus security enhancements
  - added dgIdentity support (draft-haripriya-dynamicgroup)
A.2.11. New features in slapd

- monitoring of back-{b,h}db: cache fill-in, non-indexed searches,
- session tracking control (draft-wahl-ldap-session)
- subtree delete in back-sql (draft-armijo-ldap-treedelete)

A.2.12. New features in libldap

- ldap_sync client API (LDAP Content Sync Operation, RFC 4533)

A.2.13. New clients, tools and tool enhancements

- ldapexop for arbitrary extended operations
- Complete support of controls in request/response for all clients
- LDAP Client tools now honor SRV records

A.2.14. New build options

- Support for building against GnuTLS

A.3. Obsolete Features Removed From 2.4

These features were strongly deprecated in 2.3 and removed in 2.4.

A.3.1. Slurpd

Please read the Replication section as to why this is no longer in OpenLDAP

A.3.2. back-ldbm

back-ldbm was both slow and unreliable. Its byzantine indexing code was prone to spontaneous corruption, as were the underlying database libraries that were commonly used (e.g. GDBM or NDBM). back-bdb and back-hdb are superior in every aspect, with simplified indexing to avoid index corruption, fine-grained locking for greater concurrency, hierarchical caching for greater performance, streamlined on-disk format for greater efficiency and portability, and full transaction support for greater reliability.
B. Upgrading from 2.3.x

The following sections attempt to document the steps you will need to take in order to upgrade from the latest 2.3.x OpenLDAP version.

The normal upgrade procedure, as discussed in the Maintenance section, should of course still be followed prior to doing any of this.

B.1. Monitor Backend

Note: This is a temporary requirement and is subject to change over the next 2.4.x beta release cycle

A monitor (slapd-monitor(5)) now needs a rootdn entry. If you do not have one, slapd will fail to start up with an error message like so:

```
monitor_back_register_entry_attrs("": base="cn=databases,cn=monitor" scope=one
filter="(namingContexts:distinguishedNameMatch:=dc=example,dc=com)": unable to find
backend_startup_one: bi_db_open failed! (1)
slap_startup failed (test would succeed using the -u switch)
```

Here is a complete database monitor example:

```
database monitor
rootdn cn=monitor
rootpw change_me
```

B.2. cn=config olc* attributes

Quite a few olc* attributes have now become obsolete, if you see in your logs entries like below, just remove them from the relevant ldif file.

```
olcReplicationInterval: value #0: <olcReplicationInterval> keyword is obsolete (ignore)
```

ADD MORE HERE
C. Common errors encountered when using OpenLDAP Software

The following sections attempt to summarize the most common causes of LDAP errors when using OpenLDAP.

C.1. Common causes of LDAP errors

C.1.1. ldap_*: Can’t contact LDAP server

The error is usually returned when the LDAP server cannot be contacted. This may occur for many reasons:

- the LDAP server is not running; this can be checked by running, for example,

  telnet <host> <port>

  replacing <host> and <port> with the hostname and the port the server is supposed to listen on.

- the client has not been instructed to contact a running server; with OpenLDAP command-line tools this is accomplished by providing the -H switch, whose argument is a valid LDAP url corresponding to the interface the server is supposed to be listening on.

C.1.2. ldap_*: No such object

The error is generally returned when the target DN of the operation cannot be located. This section details reasons common to all operations. You should also look for answers specific to the operation (as indicated in the error message).

The most common reason for this error is non-existence of the named object. First, check for typos.

Also note that, by default, a new directory server holds no objects (except for a few system entries). So, if you are setting up a new directory server and get this message, it may simply be that you have yet to add the object you are trying to locate.

The error commonly occurs because a DN was not specified and a default was not properly configured.

If you have a suffix specified in slapd.conf eg.

  suffix "dc=example,dc=com"

You should use

  ldapsearch -b 'dc=example,dc=com' '(cn=jane*)'

to tell it where to start the search.

The -b should be specified for all LDAP commands unless you have an ldap.conf(5) default configured.
See `ldapsearch(1), ldapmodify(1)`

Also, `slapadd(8)` and its ancillary programs are very strict about the syntax of the LDIF file.

Some liberties in the LDIF file may result in an apparently successful creation of the database, but accessing some parts of it may be difficult.

One known common error in database creation is putting a blank line before the first entry in the LDIF file. **There must be no leading blank lines in the LDIF file.**

It is generally recommended that `ldapadd(1)` be used instead of `slapadd(8)` when adding new entries your directory. `slapadd(8)` should be used to bulk load entries known to be valid.

Another cause of this message is a referral (:{SECT:Constructing a Distributed Directory Service}) entry to an unpopulated directory.

Either remove the referral, or add a single record with the referral base DN to the empty directory.

This error may also occur when slapd is unable to access the contents of its database because of file permission problems. For instance, on a Red Hat Linux system, slapd runs as user 'ldap'. When slapadd is run as root to create a database from scratch, the contents of `/var/lib/ldap` are created with user and group root and with permission 600, making the contents inaccessible to the slapd server.

### C.1.3. ldap_*: Can't chase referral

This is caused by the line

```
referral        ldap://root.openldap.org
```

In `slapd.conf`, it was provided as an example for how to use referrals in the original file. However if your machine is not permanently connected to the Internet, it will fail to find the server, and hence produce an error message.

To resolve, just place a # in front of line and restart slapd or point it to an available ldap server.

See also: `ldapadd(1), ldapmodify(1)` and `slapd.conf(5)`

### C.1.4. ldap_*: server is unwilling to perform

slapd will return an unwilling to perform error if the backend holding the target entry does not support the given operation.

The password backend is only willing to perform searches. It will return an unwilling to perform error for all other operations.

The shell backend is configurable and may support a limited subset of operations. Check for other errors indicating a shortage of resources required by the directory server. i.e. you may have a full disk etc
C.1.5. ldap_*: Insufficient access

This error occurs when server denies the operation due to insufficient access. This is usually caused by binding to a DN with insufficient privileges (or binding anonymously) to perform the operation.

You can bind as the rootdn/rootpw specified in slapd.conf(5) to gain full access. Otherwise, you must bind to an entry which has been granted the appropriate rights through access controls.

C.1.6. ldap_*: Invalid DN syntax

The target (or other) DN of the operation is invalid. This implies that either the string representation of the DN is not in the required form, one of the types in the attribute value assertions is not defined, or one of the values in the attribute value assertions does not conform to the appropriate syntax.

C.1.7. ldap_*: Referral hop limit exceeded

This error generally occurs when the client chases a referral which refers itself back to a server it already contacted. The server responds as it did before and the client loops. This loop is detected when the hop limit is exceeded.

This is most often caused through misconfiguration of the server’s default referral. The default referral should not be itself:

That is, on ldap://myldap/ the default referral should not be ldap://myldap/ (or any hostname/ip which is equivalent to myldap).

C.1.8. ldap_*: operations error

In some versions of slapd(8), operationsError was returned instead of other.

C.1.9. ldap_*: other error

The other result code indicates an internal error has occurred. While the additional information provided with the result code might provide some hint as to the problem, often one will need to consult the server’s log files.

C.1.10. ldap_add/modify: Invalid syntax

This error is reported when a value of an attribute does not conform to syntax restrictions. Additional information is commonly provided stating which value of which attribute was found to be invalid. Double check this value and other values (the server will only report the first error it finds).

Common causes include:

- extraneous white space (especially trailing white space)
- improperly encoded characters (LDAPv3 uses UTF-8 encoded Unicode)
- empty values (few syntaxes allow empty values)

For certain syntax, like OBJECT IDENTIFIER (OID), this error can indicate that the OID descriptor (a "short name") provided is unrecognized. For instance, this error is returned if the objectClass value provided is unrecognized.
C.1.11. ldap_add/modify: Object class violation

This error is returned with the entry to be added or the entry as modified violates the object class schema rules. Normally additional information is returned the error detailing the violation. Some of these are detailed below.

Violations related to the entry's attributes:

- **Attribute not allowed**
  
  A provided attribute is not allowed by the entry's object class(es).

- **Missing required attribute**
  
  An attribute required by the entry's object class(es) was not provided.

Violations related to the entry's class(es):

- **Entry has no objectClass attribute**
  
  The entry did not state which object classes it belonged to.

- **Unrecognized objectClass**
  
  One (or more) of the listed objectClass values is not recognized.

- **No structural object class provided**
  
  None of the listed objectClass values is structural.

- **Invalid structural object class chain**
  
  Two or more structural objectClass values are not in same structural object class chain.

- **Structural object class modification**
  
  Modify operation attempts to change the structural class of the entry.

- **Instantiantiation of abstract objectClass**
  
  An abstract class is not subordinate to any listed structural or auxiliary class.

- **Invalid structural object class**
  
  Other structural object class problem.

- **No structuralObjectClass operational attribute**
  
  This is commonly returned when a shadow server is provided an entry which does not contain the structuralObjectClass operational attribute.
Note that the above error messages as well as the above answer assumes basic knowledge of LDAP/X.500 schema.

**C.1.12. ldap_add: No such object**

The "ldap_add: No such object" error is commonly returned if parent of the entry being added does not exist. Add the parent entry first...

For example, if you are adding "cn=bob,dc=domain,dc=com" and you get:

```
ldap_add: No such object
```

The entry "dc=domain,dc=com" likely doesn't exist. You can use ldapsearch to see if does exist:

```
ldapsearch -b 'dc=domain,dc=com' -s base '(objectclass=*)'
```

If it doesn't, add it. See A Quick-Start Guide for assistance.

**Note:** if the entry being added is the same as database suffix, it's parent isn't required. i.e.: if your suffix is "dc=domain,dc=com", "dc=com" doesn't need to exist to add "dc=domain,dc=com".

This error will also occur if you try to add any entry that the server is not configured to hold.

For example, if your database suffix is "dc=domain,dc=com" and you attempt to add "dc=domain2,dc=com", "dc=com", "dc=domain,dc=org", "o=domain,c=us", or an other DN in the "dc=domain,dc=com" subtree, the server will return a "No such object" (or referral) error.

*sldapd*(8) will generally return "no global superior knowledge" as additional information indicating its return noSuchObject instead of a referral as the server is not configured with knowledge of a global superior server.

**C.1.13. ldap add: invalid structural object class chain**

This particular error refers to the rule about STRUCTURAL objectclasses, which states that an object is of one STRUCTURAL class, the structural class of the object. The object is said to belong to this class, zero or more auxiliaries classes, and their super classes.

While all of these classes are commonly listed in the objectClass attribute of the entry, one of these classes is the structural object class of the entry. Thus, it is OK for an objectClass attribute to contain inetOrgPerson, organizationalPerson, and person because they inherit one from another to form a single super class chain. That is, inetOrgPerson SUPs organizationPerson SUPs person. On the other hand, it is invalid for both inetOrgPerson and account to be listed in objectClass as inetOrgPerson and account are not part of the same super class chain (unless some other class is also listed with is a subclass of both).

To resolve this problem, one must determine which class will better serve structural object class for the entry, adding this class to the objectClass attribute (if not already present), and remove any other structural class from the entry's objectClass attribute which is not a super class of the structural object class.

Which object class is better depends on the particulars of the situation. One generally should consult the documentation for the applications one is using for help in making the determination.
C.1.14. ldap_add: no structuralObjectClass operational attribute

ldapadd(1) may error:

```plaintext
adding new entry "uid=XXX,ou=People,o=campus,c=ru"
ldap_add: Internal (implementation specific) error (80)
   additional info: no structuralObjectClass operational attribute
```

dn: dc=example,dc=com
objectClass: organization
o: Example
# note: "dc: example" is missing

when slapd(8) cannot determine, based upon the contents of the objectClass attribute, what the structural class of the object should be.

C.1.15. ldap_add/modify/rename: Naming violation

OpenLDAP's slapd checks for naming attributes and distinguished values consistency, according to RFC 4512.

Naming attributes are those attributeTypes that appear in an entry's RDN; distinguished values are the values of the naming attributes that appear in an entry's RDN, e.g, in

```plaintext
cn=Someone+mail=someone@example.com,dc=example,dc=com
```

the naming attributes are cn and mail, and the distinguished values are Someone and someone@example.com.

OpenLDAP's slapd checks for consistency when:

- adding an entry
- modifying an entry, if the values of the naming attributes are changed
- renaming an entry, if the RDN of the entry changes

Possible causes of error are:

- the naming attributes are not present in the entry; for example:
  ```plaintext
dn: dc=example,dc=com
objectClass: organization
o: Example
# note: "dc: example" is missing
```

- the naming attributes are present in the entry, but in the attributeType definition they are marked as:
  - collective
  - operational
  - obsolete

- the naming attributes are present in the entry, but the distinguished values are not; for example:

  ```plaintext
dn: dc=example,dc=com
objectClass: domain
dc: foobar
# note: "dc" is present, but the value is not "example"
```

- the naming attributes are present in the entry, with the distinguished values, but the naming attributes:
  - do not have an equality field, so equality cannot be asserted
  - the matching rule is not supported (yet)
♦ the matching rule is not appropriate
• the given distinguished values do not comply with their syntax
• other errors occurred during the validation/normalization/match process; this is a catchall: look at previous logs for details in case none of the above apply to your case.

In any case, make sure that the attributeType definition for the naming attributes contains an appropriate EQUALITY field; or that of the superior, if they are defined based on a superior attributeType (look at the SUP field). See RFC 4512 for details.

C.1.16. ldap_add/delete/modify/rename: no global superior knowledge

If the target entry name places is not within any of the databases the server is configured to hold and the server has no knowledge of a global superior, the server will indicate it is unwilling to perform the operation and provide the text "no global superior knowledge" as additional text.

Likely the entry name is incorrect, or the server is not properly configured to hold the named entry, or, in distributed directory environments, a default referral was not configured.

C.1.17. ldap_bind: Insufficient access

Current versions of slapd(8) requires that clients have authentication permission to attribute types used for authentication purposes before accessing them to perform the bind operation. As all bind operations are done anonymously (regardless of previous bind success), the auth access must be granted to anonymous.

In the example ACL below grants the following access:

• to anonymous users:
  ♦ permission to authenticate using values of userPassword
• to authenticated users:
  ♦ permission to update (but not read) their userPassword
  ♦ permission to read any object excepting values of userPassword

All other access is denied.

```plaintext
access to attr=userPassword
by self =w
by anonymous auth
access *
by self write
by users read
```

C.1.18. ldap_bind: Invalid credentials

The error usually occurs when the credentials (password) provided does not match the userPassword held in entry you are binding to.

The error can also occur when the bind DN specified is not known to the server.

Check both! In addition to the cases mentioned above you should check if the server denied access to userPassword on selected parts of the directory. In fact, slapd always returns "Invalid credentials" in case of failed bind, regardless of the failure reason, since other return codes could reveal the validity of the user's
name.

To debug access rules defined in slapd.conf, add "ACL" to log level.

**C.1.19. ldap_bind: Protocol error**

There error is generally occurs when the LDAP version requested by the client is not supported by the server.

The OpenLDAP Software 2.x server, by default, only accepts version 3 LDAP Bind requests but can be configured to accept a version 2 LDAP Bind request.

---

**Note:** The 2.x server expects LDAPv3 [RFC4510] to be used when the client requests version 3 and expects a limited LDAPv3 variant (basically, LDAPv3 syntax and semantics in an LDAPv2 PDUs) to be used when version 2 is expected.

This variant is also sometimes referred to as LDAPv2+, but differs from the U-Mich LDAP variant in a number of ways.

---

**C.1.20. ldap_modify: cannot modify object class**

This message is commonly returned when attempting to modify the objectClass attribute in a manner inconsistent with the LDAP/X.500 information model. In particular, it commonly occurs when one tries to change the structure of the object from one class to another, for instance, trying to change an 'apple' into a 'pear' or a 'fruit' into a 'pear'.

Such changes are disallowed by the slapd(8) in accordance with LDAP and X.500 restrictions.

---

**C.1.21. ldap_sasl_interactive_bind_s: ...**

If you intended to bind using a DN and password and get an error from ldap_sasl_interactive_bind_s, you likely forgot to provide a '-x' option to the command. By default, SASL authentication is used. '-x' is necessary to select "simple" authentication.

---

**C.1.22. ldap_sasl_interactive_bind_s: No such Object**

This indicates that LDAP SASL authentication function could not read the Root DSE. The error will occur when the server doesn't provide a root DSE. This may be due to access controls.

---

**C.1.23. ldap_sasl_interactive_bind_s: No such attribute**

This indicates that LDAP SASL authentication function could read the Root DSE but it contained no supportedSASLMechanism attribute.

The supportedSASLMechanism attribute lists mechanisms currently available. The list may be empty because none of the supported mechanisms are currently available. For example, EXTERNAL is listed only if the client has established its identity by authenticating at a lower level (e.g. TLS).

---

**Note:** the attribute may not be visible due to access controls
Note: SASL bind is the default for all OpenLDAP tools, e.g. ldapsearch(1), ldapmodify(1). To force use of "simple" bind, use the "-x" option. Use of "simple" bind is not recommended unless one has adequate confidentiality protection in place (e.g. TLS/SSL, IPSEC).

C.1.24. ldap_sasl_interactive_bind_s: Unknown authentication method

This indicates that none of the SASL authentication supported by the server are supported by the client, or that they are too weak or otherwise inappropriate for use by the client. Note that the default security options disallows the use of certain mechanisms such as ANONYMOUS and PLAIN (without TLS).

Note: SASL bind is the default for all OpenLDAP tools. To force use of "simple" bind, use the "-x" option. Use of "simple" bind is not recommended unless one has adequate confidentiality protection in place (e.g. TLS/SSL, IPSEC).

C.1.25. ldap_sasl_interactive_bind_s: Local error (82)

Apparently not having forward and reverse DNS entries for the LDAP server can result in this error.

C.1.26. ldap_search: Partial results and referral received

This error is returned with the server responses to an LDAPv2 search query with both results (zero or more matched entries) and references (referrals to other servers). See also: ldapsearch(1).

If the updatedn on the replica does not exist, a referral will be returned. It may do this as well if the ACL needs tweaking.

C.1.27. ldap_start_tls: Operations error

ldapsearch(1) and other tools will return

```plaintext
ldap_start_tls: Operations error (1)
   additional info: TLS already started
```

When the user (though command line options and/or ldap.conf(5)) has requested TLS (SSL) be started twice. For instance, when specifying both "-H ldaps://server.do.main" and "-ZZ".

C.2. Other Errors

C.2.1. ber_get_next on fd X failed errno=34 (Numerical result out of range)

This slapd error generally indicates that the client sent a message that exceeded an administrative limit. See sockbuf_max_incoming and sockbuf_max_incoming_auth configuration directives in slapd.conf(5).

C.2.2. ber_get_next on fd X failed errno=11 (Resource temporarily unavailable)

This message is not indicative of abnormal behavior or error. It simply means that expected data is not yet available from the resource, in this context, a network socket. slapd(8) will process the data once it does
becomes available.

**C.2.3. daemon: socket() failed errno=97 (Address family not supported)**

This message indicates that the operating system does not support one of the (protocol) address families which slapd(8) was configured to support. Most commonly, this occurs when slapd(8) was configured to support IPv6 yet the operating system kernel wasn't. In such cases, the message can be ignored.

**C.2.4. GSSAPI: gss_acquire_cred: Miscellaneous failure; Permission denied**

This message means that slapd is not running as root and, thus, it cannot get its Kerberos 5 key from the keytab, usually file /etc/krb5.keytab.

A keytab file is used to store keys that are to be used by services or daemons that are started at boot time. It is very important that these secrets are kept beyond reach of intruders.

That's why the default keytab file is owned by root and protected from being read by others. Do not mess with these permissions, build a different keytab file for slapd instead.

To do this, start kadmin, and enter the following commands:

```
addprinc -randkey ldap/ldap.example.com@EXAMPLE.COM
ktadd -k /etc/openldap/ldap.keytab ldap/ldap.example.com@EXAMPLE.COM
```

Then, on the shell, do:

```
chown ldap ldap /etc/openldap/ldap.keytab
chmod 600 /etc/openldap/ldap.keytab
```

Now you have to tell slapd (well, actually tell the gssapi library in Kerberos 5 that is invoked by Cyrus SASL) where to find the new keytab. You do this by setting the environment variable KRB5_KTNAME like this:

```
export KRB5_KTNAME="FILE:/etc/openldap/ldap.keytab"
```

Set that environment variable on the slapd start script (Red Hat users might find /etc/sysconfig/ldap a perfect place).

This only works if you are using MIT kerberos. It doesn't work with Heimdal, for instance.

In Heimdal there is a function gsskrb5_register_acceptor_identity() that sets the path of the keytab file you want to use. In Cyrus SASL 2 you can add

```
keytab: /path/to/file
```

to your application's SASL config file to use this feature. This only works with Heimdal.

**C.2.5. access from unknown denied**

This related to TCP wrappers. See hosts_access(5) for more information. in the log file: "access from unknown denied" This related to TCP wrappers. See hosts_access(5) for more information. for example: add the line "slapd: .hosts.you.want.to.allow" in /etc/hosts.allow to get rid of the error.
C.2.6. `ldap_read': want=# error=Resource temporarily unavailable

This message occurs normally. It means that pending data is not yet available from the resource, a network socket. slapd(8) will process the data once it becomes available.

C.2.7. `make test' fails

Some times, `make test' fails at the very first test with an obscure message like

```
make test
make[1]: Entering directory `/ldap_files/openldap-2.4.6/tests'
make[2]: Entering directory `/ldap_files/openldap-2.4.6/tests'
Initiating LDAP tests for BDB...
Cleaning up test run directory leftover from previous run.
Running ./scripts/all...
>>>>> Executing all LDAP tests for bdb
>>>>> Starting test000-rootdse ...
running defines.sh
Starting slapd on TCP/IP port 9011...
Using ldapsearch to retrieve the root DSE...
Waiting 5 seconds for slapd to start...
./scripts/test000-rootdse: line 40: 10607 Segmentation fault $SLAPD -f $CONF1 -h $URI1 -d $LVL $TIMING >$LOG1 2>&1
Waiting 5 seconds for slapd to start...
Waiting 5 seconds for slapd to start...
Waiting 5 seconds for slapd to start...
Waiting 5 seconds for slapd to start...
./scripts/test000-rootdse: kill: (10607) - No such pid
ldap_sasl_bind_s: Can't contact LDAP server (-1)
>>>>> Test failed
>>>>> ./scripts/test000-rootdse failed (exit 1)
make[2]: *** [bdb-yes] Error 1
make[2]: Leaving directory `/ldap_files/openldap-2.4.6/tests'
make[1]: *** [test] Error 2
make[1]: Leaving directory `/ldap_files/openldap-2.4.6/tests'
make: *** [test] Error 2
```

or so. Usually, the five lines indicate that slapd didn't start at all.

In tests/testrun/slapd.1.log there is a full log of what slapd wrote while trying to start. The log level can be increased by setting the environment variable SLAPD_DEBUG to the corresponding value; see loglevel in slapd.conf(5) for the meaning of log levels.

A typical reason for this behavior is a runtime link problem, i.e. slapd cannot find some dynamic libraries it was linked against. Try running ldd(1) on slapd (for those architectures that support runtime linking).

There might well be other reasons; the contents of the log file should help clarifying them.

Tests that fire up multiple instances of slapd typically log to tests/testrun/slapd.<n>.log, with a distinct <n> for each instance of slapd; list tests/testrun/ for possible values of <n>.
C.2.8. *ldap_*: Internal (implementation specific) error (80) - additional info:
entry index delete failed

This seems to be related with wrong ownership of the BDB's dir (/var/lib/ldap) and files.

    chmod -R openldap:openldap /var/lib/ldap

fixes it in Debian

C.2.9. *ldap_sasl_interactive_bind_s*: Can't contact LDAP server (-1)

Using SASL, when a client contacts LDAP server, the slapd service dies immediately and client gets an error:

    SASL/GSSAPI authentication started ldap_sasl_interactive_bind_s: Can't contact LDAP server (-1)

Then check the slapd service, it stopped.

This may come from incompatible of using different versions of BerkeleyDB for installing of SASL and installing of OpenLDAP. The problem arises in case of using multiple version of BerkeleyDB. Solution:
- Check which version of BerkeleyDB when install Cyrus SASL.

Reinstall OpenLDAP with the version of BerkeleyDB above.
## D. Recommended OpenLDAP Software Dependency Versions

This appendix details the recommended versions of the software that OpenLDAP depends on.

Please read the Prerequisite software section for more information on the following software dependencies.

### D.1. Dependency Versions

Table 8.5: OpenLDAP Software Dependency Versions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Layer Security:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenSSL</td>
<td>0.9.7+</td>
</tr>
<tr>
<td></td>
<td>GnuTLS</td>
<td>2.0.1</td>
</tr>
<tr>
<td>Simple Authentication and Security Layer</td>
<td>Cyrus SASL</td>
<td>2.1.21+</td>
</tr>
<tr>
<td>Kerberos Authentication Service:</td>
<td>Heimdal</td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td>MIT Kerberos</td>
<td>Version</td>
</tr>
<tr>
<td>Database Software</td>
<td>Berkeley DB:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.6</td>
</tr>
<tr>
<td></td>
<td>Note: It is highly recommended to apply the patches from for a given release.</td>
<td></td>
</tr>
<tr>
<td>Threads:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>POSIX pthreads</td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td>Mach CThreads</td>
<td>Version</td>
</tr>
<tr>
<td>TCP Wrappers</td>
<td>Name</td>
<td>Version</td>
</tr>
</tbody>
</table>
E. Real World OpenLDAP Deployments and Examples

Examples and discussions
F. OpenLDAP Software Contributions

The following sections attempt to summarize the various contributions in OpenLDAP software, as found in openldap_src/contrib

F.1. Client APIs

Intro and discuss

F.1.1. ldapc++

Intro and discuss

F.1.2. ldaptcl

Intro and discuss

F.2. Overlays

Intro and complete/expand correct names for below:

F.2.1. acl
F.2.2. addpartial
F.2.3. allopl
F.2.4. comp_match
F.2.5. dentity
F.2.6. dsaschema
F.2.7. lastmod
F.2.8. passwd
F.2.9. proxyOld
F.2.10. smbk5pwd
F.2.11. trace

F.3. Tools

Intro and discuss
F.3.1. Statistic Logging

statslog

F.4. SLAPI Plugins

Intro and discuss

F.4.1. addrdnvalues

More
G. Configuration File Examples

G.1. slapd.conf
G.2. ldap.conf
G.3. a-n-other.conf
H. LDAP Result Codes

For the purposes of this guide, we have incorporated the standard LDAP result codes from Appendix A. LDAP Result Codes of rfc4511. A copy of which can be found in doc/rfc of the OpenLDAP source code.

We have expanded the description of each error in relation to the OpenLDAP toolsets.

H.1. Non-Error Result Codes

These result codes (called "non-error" result codes) do not indicate an error condition:

- success (0),
- compareFalse (5),
- compareTrue (6),
- referral (10), and
- saslBindInProgress (14).

The success, compareTrue, and compareFalse result codes indicate successful completion (and, hence, are referred to as "successful" result codes).

The referral and saslBindInProgress result codes indicate the client needs to take additional action to complete the operation.

H.2. Result Codes

Existing LDAP result codes are described as follows:

H.3. success (0)

Indicates the successful completion of an operation.

**Note:** this code is not used with the Compare operation. See compareFalse (5) and compareTrue (6).

H.4. operationsError (1)

Indicates that the operation is not properly sequenced with relation to other operations (of same or different type).

For example, this code is returned if the client attempts to StartTLS [RFC4346] while there are other uncompleted operations or if a TLS layer was already installed.

H.5. protocolError (2)

Indicates the server received data that is not well-formed.

For Bind operation only, this code is also used to indicate that the server does not support the requested protocol version.
For Extended operations only, this code is also used to indicate that the server does not support (by design or configuration) the Extended operation associated with the requestName.

For request operations specifying multiple controls, this may be used to indicate that the server cannot ignore the order of the controls as specified, or that the combination of the specified controls is invalid or unspecified.

H.6. timeLimitExceeded (3)
Indicates that the time limit specified by the client was exceeded before the operation could be completed.

H.7. sizeLimitExceeded (4)
Indicates that the size limit specified by the client was exceeded before the operation could be completed.

H.8. compareFalse (5)
Indicates that the Compare operation has successfully completed and the assertion has evaluated to FALSE or Undefined.

H.9. compareTrue (6)
Indicates that the Compare operation has successfully completed and the assertion has evaluated to TRUE.

H.10. authMethodNotSupported (7)
Indicates that the authentication method or mechanism is not supported.

H.11. strongerAuthRequired (8)
Indicates the server requires strong(er) authentication in order to complete the operation.

When used with the Notice of Disconnection operation, this code indicates that the server has detected that an established security association between the client and server has unexpectedly failed or been compromised.

H.12. referral (10)
Indicates that a referral needs to be chased to complete the operation (see Section 4.1.10).

H.13. adminLimitExceeded (11)
Indicates that an administrative limit has been exceeded.

H.14. unavailableCriticalExtension (12)
Indicates a critical control is unrecognized (see Section 4.1.11).
H.15. confidentialityRequired (13)
Indicates that data confidentiality protections are required.

H.16. saslBindInProgress (14)
Indicates the server requires the client to send a new bind request, with the same SASL mechanism, to continue the authentication process (see Section 4.2).

H.17. noSuchAttribute (16)
Indicates that the named entry does not contain the specified attribute or attribute value.

H.18. undefinedAttributeType (17)
Indicates that a request field contains an unrecognized attribute description.

H.19. inappropriateMatching (18)
Indicates that an attempt was made (e.g., in an assertion) to use a matching rule not defined for the attribute type concerned.

H.20. constraintViolation (19)
Indicates that the client supplied an attribute value that does not conform to the constraints placed upon it by the data model.

For example, this code is returned when multiple values are supplied to an attribute that has a SINGLE-VALUE constraint.

H.21. attributeOrValueExists (20)
Indicates that the client supplied an attribute or value to be added to an entry, but the attribute or value already exists.

H.22. invalidAttributeSyntax (21)
Indicates that a purported attribute value does not conform to the syntax of the attribute.

H.23. noSuchObject (32)
Indicates that the object does not exist in the DIT.

H.24. aliasProblem (33)
Indicates that an alias problem has occurred. For example, the code may used to indicate an alias has been dereferenced that names no object.

**H.25. invalidDNSyntax (34)**

Indicates that an LDAPDN or RelativeLDAPDN field (e.g., search base, target entry, ModifyDN newrdn, etc.) of a request does not conform to the required syntax or contains attribute values that do not conform to the syntax of the attribute’s type.

**H.26. aliasDereferencingProblem (36)**

Indicates that a problem occurred while dereferencing an alias. Typically, an alias was encountered in a situation where it was not allowed or where access was denied.

**H.27. inappropriateAuthentication (48)**

Indicates the server requires the client that had attempted to bind anonymously or without supplying credentials to provide some form of credentials.

**H.28. invalidCredentials (49)**

Indicates that the provided credentials (e.g., the user's name and password) are invalid.

**H.29. insufficientAccessRights (50)**

Indicates that the client does not have sufficient access rights to perform the operation.

**H.30. busy (51)**

Indicates that the server is too busy to service the operation.

**H.31. unavailable (52)**

Indicates that the server is shutting down or a subsystem necessary to complete the operation is offline.

**H.32. unwillingToPerform (53)**

Indicates that the server is unwilling to perform the operation.

**H.33. loopDetect (54)**

Indicates that the server has detected an internal loop (e.g., while dereferencing aliases or chaining an operation).
H.34. *namingViolation (64)*

Indicates that the entry's name violates naming restrictions.

H.35. *objectClassViolation (65)*

Indicates that the entry violates object class restrictions.

H.36. *notAllowedOnNonLeaf (66)*

Indicates that the operation is inappropriately acting upon a non-leaf entry.

H.37. *notAllowedOnRDN (67)*

Indicates that the operation is inappropriately attempting to remove a value that forms the entry's relative distinguished name.

H.38. *entryAlreadyExists (68)*

Indicates that the request cannot be fulfilled (added, moved, or renamed) as the target entry already exists.

H.39. *objectClassModsProhibited (69)*

Indicates that an attempt to modify the object class(es) of an entry's 'objectClass' attribute is prohibited.

For example, this code is returned when a client attempts to modify the structural object class of an entry.

H.40. *affectsMultipleDSAs (71)*

Indicates that the operation cannot be performed as it would affect multiple servers (DSAs).

H.41. *other (80)*

Indicates the server has encountered an internal error.
# I. Glossary

## I.1. Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple DES</td>
</tr>
<tr>
<td>ABNF</td>
<td>Augmented Backus-Naur Form</td>
</tr>
<tr>
<td>ACDF</td>
<td>Access Control Decision Function</td>
</tr>
<tr>
<td>ACE</td>
<td>ASCII Compatible Encoding</td>
</tr>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ACID</td>
<td>Atomicity, Consistency, Isolation, and Durability</td>
</tr>
<tr>
<td>ACI</td>
<td>Access Control Information</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AES</td>
<td>Advance Encryption Standard</td>
</tr>
<tr>
<td>ABI</td>
<td>Application Binary Interface</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>ASN.1</td>
<td>Abstract Syntax Notation - One</td>
</tr>
<tr>
<td>AVA</td>
<td>Attribute Value Assertion</td>
</tr>
<tr>
<td>AuthcDN</td>
<td>Authentication DN</td>
</tr>
<tr>
<td>AuthcId</td>
<td>Authentication Identity</td>
</tr>
<tr>
<td>AuthzDN</td>
<td>Authorization DN</td>
</tr>
<tr>
<td>AuthzId</td>
<td>Authorization Identity</td>
</tr>
<tr>
<td>BCP</td>
<td>Best Current Practice</td>
</tr>
<tr>
<td>BDB</td>
<td>Berkeley DB (Backend)</td>
</tr>
<tr>
<td>BER</td>
<td>Basic Encoding Rules</td>
</tr>
<tr>
<td>BNF</td>
<td>Backus-Naur Form</td>
</tr>
<tr>
<td>C</td>
<td>The C Programming Language</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CER</td>
<td>Canonical Encoding Rules</td>
</tr>
<tr>
<td>CLDAP</td>
<td>Connection-less LDAP</td>
</tr>
<tr>
<td>CN</td>
<td>Common Name</td>
</tr>
<tr>
<td>CRAM-MD5</td>
<td>SASL MD5 Challedge/Response Authentication Mechanism</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>DAP</td>
<td>Directory Access Protocol</td>
</tr>
<tr>
<td>DC</td>
<td>Domain Component</td>
</tr>
<tr>
<td>DER</td>
<td>Distinguished Encoding Rules</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DIB</td>
<td>Directory Information Base</td>
</tr>
<tr>
<td>DIGEST-MD5</td>
<td>SASL Digest MD5 Authentication Mechanism</td>
</tr>
<tr>
<td>DISP</td>
<td>Directory Information Shadowing Protocol</td>
</tr>
<tr>
<td>DIT</td>
<td>Directory Information Tree</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>DOP</td>
<td>Directory Operational Binding Management Protocol</td>
</tr>
<tr>
<td>DSAIT</td>
<td>DSA Information Tree</td>
</tr>
<tr>
<td>DSA</td>
<td>Directory System Agent</td>
</tr>
<tr>
<td>DSE</td>
<td>DSA-specific Entry</td>
</tr>
<tr>
<td>DSP</td>
<td>Directory System Protocol</td>
</tr>
<tr>
<td>DS</td>
<td>Draft Standard</td>
</tr>
<tr>
<td>DUA</td>
<td>Directory User Agent</td>
</tr>
<tr>
<td>EXTERNAL</td>
<td>SASL External Authentication Mechanism</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>FYI</td>
<td>For Your Information</td>
</tr>
<tr>
<td>GSER</td>
<td>Generic String Encoding Rules</td>
</tr>
<tr>
<td>GSS-API</td>
<td>Generic Security Service Application Program Interface</td>
</tr>
<tr>
<td>GSSAPI</td>
<td>SASL Kerberos V GSS-API Authentication Mechanism</td>
</tr>
<tr>
<td>HDB</td>
<td>Hierarchical Database (Backend)</td>
</tr>
<tr>
<td>I-D</td>
<td>Internet-Draft</td>
</tr>
<tr>
<td>IA5</td>
<td>International Alphabet 5</td>
</tr>
<tr>
<td>IDNA</td>
<td>Internationalized Domain Names in Applications</td>
</tr>
<tr>
<td>IDN</td>
<td>Internationalized Domain Name</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier</td>
</tr>
<tr>
<td>IDL</td>
<td>Index Data Lookups</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPC</td>
<td>Inter-process communication</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol, version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol, version 6</td>
</tr>
<tr>
<td>ITS</td>
<td>Issue Tracking System</td>
</tr>
<tr>
<td>JPEG</td>
<td>Joint Photographic Experts Group</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos Authentication Service</td>
</tr>
<tr>
<td>LBER</td>
<td>Lightweight BER</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LDAP Sync</td>
<td>LDAP Content Sychronization</td>
</tr>
<tr>
<td>LDAPv3</td>
<td>LDAP, version 3</td>
</tr>
<tr>
<td>LDIF</td>
<td>LDAP Data Interchange Format</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MODDN</td>
<td>Modify DN</td>
</tr>
<tr>
<td>MODRDN</td>
<td>Modify RDN</td>
</tr>
<tr>
<td>NSSR</td>
<td>Non-specific Subordinate Reference</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
</tbody>
</table>
OSI  Open Systems Interconnect
OTP  One Time Password
PDU  Protocol Data Unit
PEM  Privacy Enhanced eMail
PEN  Private Enterprise Number
PKCS Public Key Cryptosystem
PKI  Public Key Infrastructure
PKIX Public Key Infrastructure (X.509)
PLAIN  SASL Plaintext Password Authentication Mechanism
POSIX Portable Operating System Interface
PS  Proposed Standard
RDN  Relative Distinguished Name
RFC Request for Comments
RPC  Remote Procedure Call
RXER Robust XML Encoding Rules
SASL Simple Authentication and Security Layer
SDF Simple Document Format
SDSE Shadowed DSE
SHA1 Secure Hash Algorithm 1
SLAPD Standalone LDAP Daemon
SLURPD Standalone LDAP Update Replication Daemon
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
SQL Structured Query Language
SRP Secure Remote Password
SSF Security Strength Factor
SSL Secure Socket Layer
STD Internet Standard
TCP Transmission Control Protocol
TLS Transport Layer Security
UCS Universal Multiple-Octet Coded Character Set
UDP User Datagram Protocol
UID User Identifier
Unicode The Unicode Standard
UNIX Unix
URI Uniform Resource Identifier
URL Uniform Resource Locator
URN Uniform Resource Name
UTF-8 8-bit UCS/Unicode Transformation Format
UTR Unicode Technical Report
UUID Universally Unique Identifier
WWW World Wide Web
OpenLDAP Software 2.4 Administrator's Guide

X.500 X.500 Directory Services
X.509 X.509 Public Key and Attribute Certificate Frameworks
XED XML Enabled Directory
XER XML Encoding Rules
XML Extensible Markup Language
syncrepl LDAP Sync-based Replication

## 1.2. Related Organizations

<table>
<thead>
<tr>
<th>Name</th>
<th>Long</th>
<th>Jump</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
<td><a href="http://www.ansi.org/">http://www.ansi.org/</a></td>
</tr>
<tr>
<td>BSI</td>
<td>British Standards Institute</td>
<td><a href="http://www.bsi-global.com/">http://www.bsi-global.com/</a></td>
</tr>
<tr>
<td>COSINE</td>
<td>Co-operation and Open Systems Interconnection in Europe</td>
<td></td>
</tr>
<tr>
<td>CPAN</td>
<td>Comprehensive Perl Archive Network</td>
<td><a href="http://cpan.org/">http://cpan.org/</a></td>
</tr>
<tr>
<td>Cyrus</td>
<td>Project Cyrus</td>
<td><a href="http://cyrusimap.web.cmu.edu/">http://cyrusimap.web.cmu.edu/</a></td>
</tr>
<tr>
<td>FSF</td>
<td>Free Software Foundation</td>
<td><a href="http://www.fsf.org/">http://www.fsf.org/</a></td>
</tr>
<tr>
<td>GNU</td>
<td>GNU Not Unix Project</td>
<td><a href="http://www.gnu.org/">http://www.gnu.org/</a></td>
</tr>
<tr>
<td>IAB</td>
<td>Internet Architecture Board</td>
<td><a href="http://www.iab.org/">http://www.iab.org/</a></td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
<td><a href="http://www.iana.org/">http://www.iana.org/</a></td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
<td><a href="http://www.ieee.org">http://www.ieee.org</a></td>
</tr>
<tr>
<td>IESG</td>
<td>Internet Engineering Steering Group</td>
<td><a href="http://www.ietf.org/iesg/">http://www.ietf.org/iesg/</a></td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
<td><a href="http://www.ietf.org/">http://www.ietf.org/</a></td>
</tr>
<tr>
<td>IRTF</td>
<td>Internet Research Task Force</td>
<td><a href="http://www.irtf.org/">http://www.irtf.org/</a></td>
</tr>
<tr>
<td>ISOC</td>
<td>Internet Society</td>
<td><a href="http://www.isoc.org/">http://www.isoc.org/</a></td>
</tr>
<tr>
<td>ITU</td>
<td>International Telephone Union</td>
<td><a href="http://www.itu.int/">http://www.itu.int/</a></td>
</tr>
<tr>
<td>OLF</td>
<td>OpenLDAP Foundation</td>
<td><a href="http://www.openldap.org/foundation/">http://www.openldap.org/foundation/</a></td>
</tr>
<tr>
<td>OLP</td>
<td>OpenLDAP Project</td>
<td><a href="http://www.openldap.org/project/">http://www.openldap.org/project/</a></td>
</tr>
<tr>
<td>OpenSSL</td>
<td>OpenSSL Project</td>
<td><a href="http://www.openssl.org/">http://www.openssl.org/</a></td>
</tr>
<tr>
<td>RFC Editor</td>
<td>RFC Editor</td>
<td><a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a></td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Corporation</td>
<td><a href="http://www.oracle.com/">http://www.oracle.com/</a></td>
</tr>
<tr>
<td>UM</td>
<td>University of Michigan</td>
<td><a href="http://www.umich.edu/">http://www.umich.edu/</a></td>
</tr>
<tr>
<td>UMLDAP</td>
<td></td>
<td><a href="http://www.umich.edu/~dirsvcs/ldap/ldap.html">http://www.umich.edu/~dirsvcs/ldap/ldap.html</a></td>
</tr>
</tbody>
</table>
I.3. Related Products

<table>
<thead>
<tr>
<th>Name</th>
<th>Jump</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVS</td>
<td><a href="http://www.cvshome.org/">http://www.cvshome.org/</a></td>
</tr>
<tr>
<td>Cyrus</td>
<td><a href="http://cyrusimap.web.cmu.edu/generalinfo.html">http://cyrusimap.web.cmu.edu/generalinfo.html</a></td>
</tr>
<tr>
<td>Cyrus SASL</td>
<td><a href="http://asg.web.cmu.edu/sasl/sasl-library.html">http://asg.web.cmu.edu/sasl/sasl-library.html</a></td>
</tr>
<tr>
<td>GNU</td>
<td><a href="http://www.gnu.org/software/">http://www.gnu.org/software/</a></td>
</tr>
<tr>
<td>GnuTLS</td>
<td><a href="http://www.gnu.org/software/gnutls/">http://www.gnu.org/software/gnutls/</a></td>
</tr>
<tr>
<td>Heimdal</td>
<td><a href="http://www.pdc.kth.se/heimdal/">http://www.pdc.kth.se/heimdal/</a></td>
</tr>
<tr>
<td>JLDAP</td>
<td><a href="http://www.openldap.org/jldap/">http://www.openldap.org/jldap/</a></td>
</tr>
<tr>
<td>MIT Kerberos</td>
<td><a href="http://web.mit.edu/kerberos/www/">http://web.mit.edu/kerberos/www/</a></td>
</tr>
<tr>
<td>OpenLDAP</td>
<td><a href="http://www.openldap.org/">http://www.openldap.org/</a></td>
</tr>
<tr>
<td>OpenLDAP FAQ</td>
<td><a href="http://www.openldap.org/faq/">http://www.openldap.org/faq/</a></td>
</tr>
<tr>
<td>OpenLDAP ITS</td>
<td><a href="http://www.openldap.org/its/">http://www.openldap.org/its/</a></td>
</tr>
<tr>
<td>OpenLDAP Software</td>
<td><a href="http://www.openldap.org/software/">http://www.openldap.org/software/</a></td>
</tr>
<tr>
<td>OpenSSL</td>
<td><a href="http://www.openssl.org/">http://www.openssl.org/</a></td>
</tr>
<tr>
<td>Perl</td>
<td><a href="http://www.perl.org/">http://www.perl.org/</a></td>
</tr>
<tr>
<td>UMLDAP</td>
<td><a href="http://www.umich.edu/~dirsvcs/ldap/ldap.html">http://www.umich.edu/~dirsvcs/ldap/ldap.html</a></td>
</tr>
</tbody>
</table>

I.4. References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document</th>
<th>Status</th>
<th>Jump</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC2079</td>
<td>Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers</td>
<td>PS</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc2079.txt">http://www.rfc-editor.org/rfc/rfc2079.txt</a></td>
</tr>
<tr>
<td>RFC2296</td>
<td>Use of Language Codes in LDAP An Approach for Using LDAP as a Network Information Service</td>
<td>PS</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc2296.txt">http://www.rfc-editor.org/rfc/rfc2296.txt</a></td>
</tr>
<tr>
<td>RFC2307</td>
<td>Definition of the inetOrgPerson LDAP Object Class</td>
<td>X</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc2307.txt">http://www.rfc-editor.org/rfc/rfc2307.txt</a></td>
</tr>
<tr>
<td>RFC2798</td>
<td></td>
<td>I</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc2798.txt">http://www.rfc-editor.org/rfc/rfc2798.txt</a></td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
<td>Status</td>
<td>Document URL</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>RFC2831</td>
<td>Using Digest Authentication as a SASL Mechanism</td>
<td>PS</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc2831.txt">http://www.rfc-editor.org/rfc/rfc2831.txt</a></td>
</tr>
<tr>
<td>RFC2849</td>
<td>The LDAP Data Interchange Format</td>
<td>PS</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc2849.txt">http://www.rfc-editor.org/rfc/rfc2849.txt</a></td>
</tr>
<tr>
<td>RFC3088</td>
<td>OpenLDAP Root Service</td>
<td>X</td>
<td><a href="http://www.rfc-editor.org/rfc/rfc3088.txt">http://www.rfc-editor.org/rfc/rfc3088.txt</a></td>
</tr>
<tr>
<td>RFC4346</td>
<td>PS</td>
<td></td>
<td><a href="http://www.rfc-editor.org/rfc/rfc4346.txt">http://www.rfc-editor.org/rfc/rfc4346.txt</a></td>
</tr>
<tr>
<td>RFC4422</td>
<td>PS</td>
<td></td>
<td><a href="http://www.rfc-editor.org/rfc/rfc4422.txt">http://www.rfc-editor.org/rfc/rfc4422.txt</a></td>
</tr>
<tr>
<td>RFC4510</td>
<td>PS</td>
<td></td>
<td><a href="http://www.rfc-editor.org/rfc/rfc4510.txt">http://www.rfc-editor.org/rfc/rfc4510.txt</a></td>
</tr>
<tr>
<td>RFC4511</td>
<td>PS</td>
<td></td>
<td><a href="http://www.rfc-editor.org/rfc/rfc4511.txt">http://www.rfc-editor.org/rfc/rfc4511.txt</a></td>
</tr>
<tr>
<td>RFC4512</td>
<td>PS</td>
<td></td>
<td><a href="http://www.rfc-editor.org/rfc/rfc4512.txt">http://www.rfc-editor.org/rfc/rfc4512.txt</a></td>
</tr>
<tr>
<td>RFC4513</td>
<td>PS</td>
<td></td>
<td><a href="http://www.rfc-editor.org/rfc/rfc4513.txt">http://www.rfc-editor.org/rfc/rfc4513.txt</a></td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
<td>Mechanism</td>
<td>Location</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td></td>
<td>of Distinguished Names</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>of Search Filters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Locator</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>String Preparation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Applications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
J. Generic configure Instructions

Basic Installation
==================

These are generic installation instructions.

The `configure' shell script attempts to guess correct values for various system-dependent variables used during compilation. It uses those values to create a `Makefile' in each directory of the package. It may also create one or more `.h' files containing system-dependent definitions. Finally, it creates a shell script `config.status' that you can run in the future to recreate the current configuration, a file `config.cache' that saves the results of its tests to speed up reconfiguring, and a file `config.log' containing compiler output (useful mainly for debugging `configure').

If you need to do unusual things to compile the package, please try to figure out how `configure' could check whether to do them, and mail diffs or instructions to the address given in the `README' so they can be considered for the next release. If at some point `config.cache' contains results you don't want to keep, you may remove or edit it.

The file `configure.in' is used to create `configure' by a program called `autoconf'. You only need `configure.in' if you want to change it or regenerate `configure' using a newer version of `autoconf'.

The simplest way to compile this package is:

1. `cd' to the directory containing the package's source code and type `./configure' to configure the package for your system. If you're using `csh' on an old version of System V, you might need to type `sh ./configure' instead to prevent `csh' from trying to execute `configure' itself.

   Running `configure' takes awhile. While running, it prints some messages telling which features it is checking for.

2. Type `make' to compile the package.

3. Optionally, type `make check' to run any self-tests that come with the package.

4. Type `make install' to install the programs and any data files and documentation.

5. You can remove the program binaries and object files from the source code directory by typing `make clean'. To also remove the files that `configure' created (so you can compile the package for a different kind of computer), type `make distclean'. There is also a `make maintainer-clean' target, but that is intended mainly for the package's developers. If you use it, you may have to get all sorts of other programs in order to regenerate files that came with the distribution.

Compilers and Options
=====================

Some systems require unusual options for compilation or linking that the `configure' script does not know about. You can give `configure'
initial values for variables by setting them in the environment. Using a Bourne-compatible shell, you can do that on the command line like this:

```
CC=c89 CFLAGS=-O2 LIBS=-lposix ./configure
```

Or on systems that have the `env' program, you can do it like this:

```
env CPPFLAGS=-I/usr/local/include LDFLAGS=-s ./configure
```

Compiling For Multiple Architectures
====================================

You can compile the package for more than one kind of computer at the same time, by placing the object files for each architecture in their own directory. To do this, you must use a version of `make' that supports the `VPATH' variable, such as GNU `make'. `cd' to the directory where you want the object files and executables to go and run the `configure' script. `configure' automatically checks for the source code in the directory that `configure' is in and in `.\..'.

If you have to use a `make' that does not supports the `VPATH' variable, you have to compile the package for one architecture at a time in the source code directory. After you have installed the package for one architecture, use `make distclean' before reconfiguring for another architecture.

Installation Names
==================

By default, `make install' will install the package's files in `\usr/local/bin', `\usr/local/man', etc. You can specify an installation prefix other than `\usr/local' by giving `configure' the option `--prefix=PATH'.

You can specify separate installation prefixes for architecture-specific files and architecture-independent files. If you give `configure' the option `--exec-prefix=PATH', the package will use PATH as the prefix for installing programs and libraries. Documentation and other data files will still use the regular prefix.

In addition, if you use an unusual directory layout you can give options like `--bindir=PATH' to specify different values for particular kinds of files. Run `configure --help' for a list of the directories you can set and what kinds of files go in them.

If the package supports it, you can cause programs to be installed with an extra prefix or suffix on their names by giving `configure' the option `--program-prefix=PREFIX' or `--program-suffix=SUFFIX'.

Optional Features
=================

Some packages pay attention to `--enable-FEATURE' options to `configure', where FEATURE indicates an optional part of the package. They may also pay attention to `--with-PACKAGE' options, where PACKAGE is something like `gnu-as' or `x' (for the X Window System). The `README' should mention any `--enable-' and `--with-' options that the package recognizes.

For packages that use the X Window System, `configure' can usually find the X include and library files automatically, but if it doesn't, you can use the `configure' options `--x-includes=DIR' and
`--x-libraries=DIR' to specify their locations.

Specifying the System Type
==========================

There may be some features `configure' can not figure out automatically, but needs to determine by the type of host the package will run on. Usually `configure' can figure that out, but if it prints a message saying it can not guess the host type, give it the `--host=TYPE' option. TYPE can either be a short name for the system type, such as `sun4', or a canonical name with three fields: CPU-COMPANY-SYSTEM

See the file `config.sub' for the possible values of each field. If `config.sub' isn't included in this package, then this package doesn't need to know the host type.

If you are building compiler tools for cross-compiling, you can also use the `--target=TYPE' option to select the type of system they will produce code for and the `--build=TYPE' option to select the type of system on which you are compiling the package.

Sharing Defaults
================

If you want to set default values for `configure' scripts to share, you can create a site shell script called `config.site' that gives default values for variables like `CC', `cache_file', and `prefix'. `configure' looks for `PREFIX/share/config.site' if it exists, then `PREFIX/etc/config.site' if it exists. Or, you can set the `CONFIG_SITE' environment variable to the location of the site script. A warning: not all `configure' scripts look for a site script.

Operation Controls
==================

`configure' recognizes the following options to control how it operates.

`--cache-file=FILE'
Use and save the results of the tests in FILE instead of `./config.cache'. Set FILE to `/dev/null' to disable caching, for debugging `configure'.

`--help'
Print a summary of the options to `configure', and exit.

`--quiet'
`--silent'
`-q'
Do not print messages saying which checks are being made. To suppress all normal output, redirect it to `/dev/null' (any error messages will still be shown).

`--srcdir=DIR'
Look for the package's source code in directory DIR. Usually `configure' can determine that directory automatically.

`--version'
Print the version of Autoconf used to generate the `configure' script, and exit.
'configure' also accepts some other, not widely useful, options.
K. OpenLDAP Software Copyright Notices

K.1. OpenLDAP Copyright Notice

Copyright 1998-2007 The OpenLDAP Foundation.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and their use subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources.

Additional information about OpenLDAP software can be obtained at <http://www.OpenLDAP.org/>.

K.2. Additional Copyright Notice

Portions Copyright 2001-2006 IBM Corporation.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

Portions Copyright 1999-2007 Symas Corporation.
Portions Copyright 2007 Gavin Henry
Portions Copyright 2007 Suretec Systems
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided “as is” without express or implied warranty.
K.3. University of Michigan Copyright Notice

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided ``as is'' without express or implied warranty.
L. OpenLDAP Public License

The OpenLDAP Public License
Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation
("Software"), with or without modification, are permitted provided
that the following conditions are met:

1. Redistributions in source form must retain copyright statements
   and notices,

2. Redistributions in binary form must reproduce applicable copyright
   statements and notices, this list of conditions, and the following
   disclaimer in the documentation and/or other materials provided
   with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.
Each revision is distinguished by a version number. You may use
this Software under terms of this license revision or under the
terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS
CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S)
OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in
advertising or otherwise to promote the sale, use or other dealing
in this Software without specific, written prior permission. Title
copyright in this Software shall at all times remain with copyright
holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA. All Rights Reserved. Permission to copy and
distribute verbatim copies of this document is granted.