

**راهنمای کاربردی مدرک بین‌المللی لینوکس  
LPIC-3 301(OpenLDAP 2.3)  
(جلد دوم: خلاصه، مثال‌ها و سناریوهای عملی اجرا شده)**



**مؤلف: مهندس سید حسین رجاء**



## Index

|   |           |
|---|-----------|
| <b>Course Objectives .....</b>                | <b>21</b> |
| Introduction - Features.....                  | 21        |
| LDAP Concepts .....                           | 21        |
| Master Server Configuration .....             | 21        |
| Define Directory Information Tree (DIT) ..... | 22        |
| Configure Replication.....                    | 22        |
| LDAP Add.....                                 | 23        |
| LDAP Delete.....                              | 23        |
| LDAP Modify.....                              | 23        |
| LDAP Search.....                              | 24        |
| Logging .....                                 | 24        |
| LDIF.....                                     | 25        |
| LDAP Schemas .....                            | 25        |
| Migrate to LDAP Authentication .....          | 25        |
| Syncrepl Replication .....                    | 26        |
| LDAP Security .....                           | 26        |
| <b>Chapter 1 .....</b>                        | <b>27</b> |
| <b>OpenLDAP Features .....</b>                | <b>27</b> |

4 راهنمای کاربردی مدرک بین‌المللی (OpenLDAP 2.3) LPIC-3 301 جلد ۲

|   |           |
|---|-----------|
| 1. Centralized directory of useful information (user accounts, contacts, mail info, address, etc.) .....        | 27        |
| 2. Optimized for Reads.....   | 27        |
| 3. Redundant Configuration .....  | 28        |
| 4. Namespace is similar to DNS: i.e. dc=raja,dc=internal DNS(raja.internal) .....                               | 28        |
| 5. Supports AUTH encryption of clear-text AUTHs - LDAPS - TCP:636 .....   | 28        |
| 6. Supports StartTLS over regular TCP:389 LDAP port - secures entire connection.....                            | 28        |
| 7. Extensible - supports many attributes via schemas - /etc/openldap/schema : allows us to stretch schema ..... | 28        |
| 8. Data storage is independent of LDAP: default is DBM .....  | 28        |
| 9. Provides various tools: slap*(offline backend) - use when LDAP is NOT running .....                          | 29        |
| 10. Provides various tools: ldap*(online daily admin).....  | 29        |
| 11. Separates binaries for: LDAP daemon (slapd) and replication (slurpd).....                                   | 29        |
| <b>Chapter 2 .....</b>  | <b>31</b> |
| <b>LDAP Concepts .....</b>  | <b>31</b> |
| 1. Distinguished Names (DNs) .....  | 31        |
| 2. Object Class .....   | 33        |
| 3. Schemas - /etc/openldap/schema.....  | 34        |

|  |           |
|--|-----------|
| <b>Index</b>   | <b>5</b>  |
| 4. Attributes - Fields .....   | 34        |
| 5. PAM - authenticates users on behalf of<br>calling application - supports LDAP .....           | 35        |
| 6. Name Service Switch (NSS) - used by<br>applicatons to find common Unix databases:<br>.....    | 35        |
| 7. Both PAM & NSS work in conjunction to<br>authenticate using LDAP (/etc/ldap.conf) .....       | 35        |
| <b>Chapter 3 .....</b>   | <b>37</b> |
| <b>Config of LDAP .....</b>  | <b>37</b> |
| 1. Explore current auth environment.....   | 37        |
| 2. Setup LDAP Environment.....   | 37        |
| ###Key Online Management Utilities### .....  | 38        |
| ###Super-User Info### .....  | 39        |
| Execution: .....   | 40        |
| Execution: .....   | 42        |
| ###Search the DIT### .....   | 43        |
| ###LDAPSEARCH### .....   | 43        |
| ###LDAP BROWSER### .....   | 44        |
| <b>Chapter 4 .....</b>   | <b>45</b> |
| <b>DIT Creation .....</b>  | <b>45</b> |
| Task: Create a DIT .....   | 45        |
| 1. Create Root OU (Container) (DC) - using a<br>pre-defined LDIF file - build_root_ou.ldif ..... | 45        |
| 2. Create organizational units: people,<br>engineering, sales.....                               | 46        |

6 راهنمای کاربردی مدرک بین‌المللی (OpenLDAP 2.3) LPIC-3 301 جلد ۲

|  |           |
|--|-----------|
| Execution:.....  | 46        |
| 3. Create some users .....   | 48        |
| Export Full Table Tree LDIF with jxplorer .....                                      | 51        |
| <b>Chapter 5 .....</b>   | <b>55</b> |
| <b>Replication .....</b>   | <b>55</b> |
| Requires:.....   | 55        |
| Requirements: .....  | 55        |
| 1. OpenLDAP RPMs are installed - openldap*,<br>nss_ldap*(includes PAM support) ..... | 55        |
| Steps to replication (regardless of<br>distribution): .....                          | 55        |
| 1. Stop master LDAP server /etc/init.d/ldap<br>stop - takes offline .....            | 55        |
| 2. Export the contents of the primary(master<br>server) (DIT) to an LDIF file .....  | 56        |
| Execution.....   | 56        |
| Execution:.....  | 60        |
| 3. Update /etc/hosts on both machines.....   | 60        |
| a. Master .....  | 60        |
| Execution.....   | 60        |
| b. Slave.....  | 61        |
| Execution:.....  | 61        |
| 4. Update slapd.conf on the master(primary)<br>server to support replication.....    | 62        |
| #Replication.....  | 62        |
| --this is for redhat ,centos .....   | 62        |
| --this is for suse.....  | 62        |

|   |           |
|---|-----------|
| <b>Index</b>  | <b>7</b>  |
| Execution:.....   | 63        |
| 5. Install LDAP on Slave.....   | 63        |
| Execution.....  | 63        |
| 6. Copy and import DIT on slave server.....                                       | 65        |
| Execution:.....   | 65        |
| Execution.....  | 66        |
| Execution.....  | 68        |
| 7. Update slapd.conf on the slave(secondary) server.....                          | 70        |
| 8. start slapd(LDAP process) on the slave(secondary/replica) server.....          | 71        |
| 9. start slapd(LDAP process) on the master(primary) server.....                   | 71        |
| Execution.....  | 71        |
| 10. Ensure that services are set to start when the system reboots.....            | 72        |
| <b>Chapter 6 .....</b>  | <b>75</b> |
| <b>Confirm LDAP records on Primary(Master) and Secondary(Slave) systems .....</b> | <b>75</b> |
| Task: .....   | 75        |
| 1. Use 'ldapsearch' to confirm the existence of records on both systems.....      | 75        |
| Execution:.....   | 75        |
| Execution:.....   | 78        |
| <b>Chapter 7 .....</b>  | <b>81</b> |
| <b>LDAPADD .....</b>  | <b>81</b> |

8 راهنمای کاربردی مدرک بین‌المللی (OpenLDAP 2.3) LPIC-3 301 جلد ۲

|   |            |
|---|------------|
| LDAPADD Features:.....  | 81         |
| 1. Facilitates the addition of objects to the DIT<br>.....                                  | 81         |
| 2. 'ldapadd' is a symlink to 'ldapmodify -a' .....  | 81         |
| Execution: .....  | 81         |
| 3. Default invocation reads attributes from<br>STDIN .....                                  | 82         |
| Tasks: .....  | 82         |
| 1. Add user 'raja1' to remaining OUs.....   | 82         |
| Execution: .....  | 82         |
| #Add First User.....  | 82         |
| #Add 2nd User .....   | 83         |
| #Add 3rd User .....   | 84         |
| #Add fourth User.....   | 85         |
| Execution: .....  | 86         |
| Execution: .....  | 91         |
| 2. Add users 'raja3,raja4,raja5' to the DIT,<br>wholesale, via STDIN from slave server..... | 101        |
| Execution: .....  | 109        |
| 3. Use LDAP Browser to view DIT and to make<br>changes.....                                 | 116        |
| Execution: .....  | 116        |
| 4. Add 5 users to 2 OUs (Engineering & Sales)<br>via text file.....                         | 117        |
| 5. Confirm results using: .....   | 117        |
| Execution: .....  | 118        |
| <b>Chapter 8 .....</b>  | <b>145</b> |



|  |            |
|--|------------|
| <b>LDAP Delete</b> .....                       | <b>145</b> |
| LDAP Delete Features: .....                    | 145        |
| 1. A means to remove DIT objects .....         | 145        |
| Tasks: .....                                   | 145        |
| 1. Delete an object from the command line      | 145        |
| Execution: .....                               | 145        |
| 2. Delete objects wholesale from:              |            |
| ou=sales,dc=raja,dc=internal - via STDIN ..... | 147        |
| Execution: .....                               | 147        |
| 4. Delete remaining OUs and objects via file   |            |
| .....  | 148        |
| Execution: .....                               | 148        |
| <b>Chapter 9</b> .....                         | <b>151</b> |
| <b>LDAP Modify</b> .....                       | <b>151</b> |
| LDAP Modify Features: .....                    | 151        |
| 1. Functionality found in: .....               | 151        |
| 2. Manipulates objects in DIT .....            | 151        |
| Tasks: .....                                   | 151        |
| 1. Rebuild the DIT - create top-level OUs and  |            |
| users/OUs .....                                | 151        |
| 2. Modify Attributes .....                     | 152        |
| Execution: .....                               | 152        |
| 3. Delete Items .....                          | 153        |
| <b>Chapter 10</b> .....                        | <b>155</b> |
| <b>LDAP Search</b> .....                       | <b>155</b> |
| LDAP Search Features: .....                    | 155        |

10 راهنمای کاربردی مدرک بین‌المللی (OpenLDAP 2.3) LPIC-3 301 جلد ۲

|   |            |
|---|------------|
| 1. Ability to search the DIT.....   | 155        |
| 2. Supports Boolean Operators: &(AND),<br> (OR), !(NOT) - Using prefix notation ..... | 155        |
| 3. Supports Wildcards: *, +(internal<br>operations).....                              | 155        |
| Usage: .....  | 155        |
| 1. ldapsearch [options] "(attribute<br>filteroperator value)" .....                   | 155        |
| Filter Operators:.....  | 155        |
| Value(s): .....   | 156        |
| Tasks: .....  | 156        |
| 1. Search specifict OUs for information .....   | 156        |
| Execution.....  | 156        |
| 2. Search the DIT for Organizational Units<br>(OUs) .....                             | 160        |
| Execution: .....  | 160        |
| Execution: .....  | 163        |
| Execution: .....  | 174        |
| 3. Use Boolean Operators .....  | 180        |
| <b>Chapter 11.....</b>  | <b>201</b> |
| <b>Logging/Debugging.....</b>   | <b>201</b> |
| Features:.....  | 201        |
| 1. Logs using SysLog (defaults to: LOCAL4)...   | 201        |
| 2. Includes ldap searches as well as<br>starts/stops/etc. ....                        | 201        |
| Configuration: .....  | 201        |
| Debugging in Red Hat openldap v2.3: .....   | 201        |

|   |            |
|---|------------|
| Table 5.1: Debugging Levels Level Description                               | 202        |
| Example   | 203        |
| loglevel -1   | 203        |
| Default:  | 203        |
| loglevel 256  | 203        |
| Debugging in Suse openldap v2.3:  | 203        |
| Task:   | 204        |
| 1. Setup Syslog logging   | 204        |
| Execution:  | 205        |
| Task:   | 227        |
| 1. Purposely misname a slapd.conf directive                                 | 227        |
| <b>Chapter 12</b>   | <b>229</b> |
| <b>LDIF Format</b>  | <b>229</b> |
| Features:   | 229        |
| 1. Standard import/export format returned by LDAP tools (offline/online)    | 229        |
| 2. RFC-2849   | 229        |
| 3. Very similar to name/value pairs from programming/scripting environments | 229        |
| Tasks:  | 229        |
| 1. ldapsearch - dumps DIT to STDOUT   | 229        |
| 2. Add 'TestUser1' to the DIT   | 230        |
| <b>Chapter 13</b>   | <b>231</b> |
| <b>Schema</b>   | <b>231</b> |

12 راهنمای کاربردی مدرک بین‌المللی (LPIC-3 301(OpenLDAP 2.3) جلد ۲

|  |            |
|--|------------|
| Features:.....   | 231        |
| 1. The definition of fields that constitute an object.....   | 231        |
| Execution:.....  | 231        |
| Execution:.....  | 232        |
| Execution:.....  | 234        |
| 2. 'SUP name' means, the higher-level (parent) attribute 'name' governs 'st' attribute .....           | 234        |
| 3. LDAP objects support single-inheritances .....  | 235        |
| Task: .....  | 236        |
| 1. Created LDAP user based on additional: core.schema attributes.....                                  | 236        |
| Execution:.....  | 236        |
| <b>Chapter 14.....</b>   | <b>239</b> |
| <b>Setup to use LDAP and Migrate to LDAP from /etc/* Files .....</b>                                   | <b>239</b> |
| Features:.....   | 239        |
| 1. Ability to take advantage of LDAP authentication .....  | 239        |
| 2. Ability to support both local (/etc/passwd) and distributed (LDAP) users .....                      | 239        |
| 3. Facilitates the sharing of most /etc/* tabular databases (/etc/hosts /etc/group /etc/services etc.) | 239        |
| 4. Setup LDAP auth of users/groups.....  | 239        |

|   |     |
|---|-----|
| 5. Ability to migrate users/records from flat files to LDAP.....  | 239 |
| 6. <a href="http://www.padl.com/OSS/MigrationTools.html">http://www.padl.com/OSS/MigrationTools.html</a> (makers of: pam_ldap.so & nss_ldap.so) ..... | 239 |
| Task: .....   | 240 |
| 0. Setup LDAP .....   | 240 |
| Execution.....  | 241 |
| 2. /etc/ldap.conf (LDAP client configuration) .....   | 241 |
| Execution:.....   | 241 |
| 3. /etc/pam.d/system-auth-ac .....  | 244 |
| Execution:.....   | 244 |
| 2. Test LDAP connectivity using SSH from slave LDAP host.....   | 244 |
| Execution:.....   | 245 |
| Execution:.....   | 248 |
| Create organizational units: Group .....  | 254 |
| Results:.....   | 263 |
| 3. Create new LDAP user and authenticate to both hosts: linuxcent & linuxcent-slave .....   | 281 |
| Execution:.....   | 282 |
| Test from slave: .....  | 283 |
| Execution:.....   | 284 |
| Further work:.....  | 289 |
| 1. Create local users on linuxcent and linuxcent-slave boxes .....  | 289 |
| 2. Migrate those users to LDAP .....  | 289 |

|  |            |
|--|------------|
| <b>Chapter 15</b> .....  | <b>291</b> |
| <b>Migrate Other Tables</b> .....  | <b>291</b> |
| Task: .....  | 291        |
| 1. Shared records via LDAP DIT .....   | 291        |
| 2. Migrate: /etc/hosts to LDAP DIT .....   | 291        |
| 3. Migrate: /etc/services .....  | 292        |
| 4. Migrate: /etc/protocols .....   | 292        |
| <b>Chapter 16</b> .....  | <b>293</b> |
| <b>Rebuild of DIT</b> .....  | <b>293</b> |
| Tasks: .....   | 293        |
| 1. Purge existing DIT using 'ldapdelete' .....   | 293        |
| Execution: .....   | 293        |
| 2. Rebuild OUs (people & group) .....  | 294        |
| Execution: .....   | 294        |
| <b>Chapter 17</b> .....  | <b>311</b> |
| <b>Account Maintenance</b> .....   | <b>311</b> |
| Task: .....  | 311        |
| 1. Create a user named 'bagher' - derived from<br>LDIF output.....                     | 311        |
| Execution: .....   | 311        |
| 2. Create a group named 'bagher' - derived<br>from LDIF output .....                   | 314        |
| Execution: .....   | 314        |
| 3. Create a directory: /home/bagher - for<br>members of the LDAP group: 'bagher' ..... | 315        |
| Execution: .....   | 315        |

|   |            |
|---|------------|
| 4. Confirm user: bagher is unable to write to:<br>/home/bagher .....                                    | 316        |
| 5. Use: 'ldpasswd' to assign a password to the<br>user: 'bagher' .....                                  | 316        |
| Execution: .....  | 317        |
| 6. Add user: 'bagher' to group: 'bagher' .....  | 318        |
| Execution: .....  | 318        |
| 7. Change users' passwords: .....   | 319        |
| 8. Change Relative Distinguished Name (RDN)<br>of an object .....                                       | 319        |
| <b>Chapter 18</b> .....   | <b>321</b> |
| <b>Replication with SyncRepl</b> .....  | <b>321</b> |
| Features: .....   | 321        |
| 1. More efficient and reliable than SLUPD-<br>based replication .....                                   | 321        |
| 2. Implemented as a slapd thread .....  | 321        |
| 3. Push/Pulls are supported: .....  | 321        |
| 4. Provider (Master) & Consumers(clients)<br>relationship .....   | 322        |
| 5. Also supports cascading configurations:<br>Provider -> Secondary Provider(s) -><br>Consumer(s) ..... | 322        |
| 6. Configuration is defined primarily on<br>'consumer' servers, NOT the provider .....                  | 322        |
| 7. Specific queries(searches) can be replicated,<br>including specific attributes .....                 | 322        |

|  |            |
|--|------------|
| 8. SyncRepl is search-based - searches define what gets replicated - search criteria is identical to that of: 'ldapsearch' ..... | 322        |
| 9. Uses built-in LDAP Content Sync protocol .....  | 323        |
| 10. Replication is incremental .....   | 323        |
| Tasks: .....   | 323        |
| 1. Configure SyncRepl .....  | 323        |
| Execution: .....   | 323        |
| Execution: .....   | 324        |
| Execution: .....   | 326        |
| Execution: .....   | 331        |
| 2. Create new object on provider .....   | 335        |
| 3. Replicate SyncRepl configuration on Another client .....  | 335        |
| 4. Provider Configuration - update provider(master) in the DB section of: slapd.conf .....                                       | 336        |
| <b>Chapter 19</b> .....  | <b>337</b> |
| <b>ACLs with OpenLDAP</b> .....  | <b>337</b> |
| Features: .....  | 337        |
| 1. General and granular restrictions .....   | 337        |
| 2. First match wins (top-down) .....   | 337        |
| 3. Implicit: 'by * none' at the end of ACLs, which denies access .....   | 337        |
| 4. ACLs are stored in: slapd.conf .....  | 337        |
| Template: .....  | 337        |



|   |            |
|---|------------|
| <b>Index</b>  | <b>17</b>  |
| Task: .....   | 338        |
| 1. Examine the Default ACL.....   | 338        |
| Execution: .....  | 338        |
| I) non authenticated user or anonymous .....  | 340        |
| II) Authenticated user RootDN: .....  | 341        |
| III) Authenticated user bagher:.....  | 342        |
| 3. Allow 'anonymous' access to 'hosts' OU and<br>nothing else .....                       | 344        |
| 4. Restrict access on an attribute level .....  | 344        |
| Execution: .....  | 344        |
| <b>Chapter 20.....</b>  | <b>353</b> |
| <b>OpenLDAP with SSL/TLS Encryption .....</b>   | <b>353</b> |
| Features:.....  | 353        |
| 1. Encrypted communications (default LDAP<br>communications is sent via clear-text) ..... | 353        |
| 2. SSL binds, by default, to TCP:636 - i.e. URI:<br>ldaps://hostname .....                | 353        |
| 3. TLS uses the default TCP:389 (StartTLS) - i.e.<br>URI: ldap://hostname .....           | 353        |
| Tasks: .....  | 353        |
| 1. Launch an 'wireshark' session in conjunction<br>with 'tcpdump' .....                   | 353        |
| Execution: .....  | 354        |
| 2. Enable SSL/TLS Encryption on the primary<br>server.....                                | 356        |
| Execution: .....  | 356        |
| Execution: .....  | 358        |

18 راهنمای کاربردی مدرک بین‌المللی (OpenLDAP 2.3) LPIC-3 301 جلد ۲

|   |     |
|---|-----|
| Execution:.....                               | 359 |
| Execution:.....                               | 360 |
| Execution:.....                               | 360 |
| Execution.....                                | 363 |
| Execution on not configured server for tls:.. | 365 |