

**راهنمای کاربردی مدرک بین‌المللی لینوکس
LPIC-3 300(Part1:OpenLDAP 2.4)
(جلد دوم: خلاصه، مثال‌ها و سناریوهای عملی اجرا شده)**



مؤلف: مهندس سید حسین رجاء

Course Objectives	21
Introduction - Features	21
Installation Exploration	21
Introduction to SLAPD LDAP Configuration	21
LDAP Entries.....	22
Client Authentication	22
Debian CentOS Clients	23
LDAP Account Manager	23
Replication	23
TLS SSL Configuration.....	24
Chapter 1.....	25
OpenLDAP 2.4 Features	25
1. Current Major Release: 2.4x - in contrast to 2.3x	25
2. Industry Standard Directory Services via:	
Standalone LDAP Server: 'slapd'	25
3. Centralized access to common information:.....	25
4. Facilitates the current Virtualization trend, whereby the ability to spawn numerous instances of OSes is the norm. Saves time in referencing common data- sets: users, groups, machines, application data, other key-value pairs (associated attributes).....	26
5. Provides fast searches of such data.....	26
6. Quite scalable at providing access to key data....	26

4 LPIC-3 300(Part1:OpenLDAP 2.4) راهنمای سریع مدرک بین‌المللی

7. Replication (distribution) of content (data) across N nodes as needed.....	26
Note: 'slurpd' is no longer used for replication - 'slapd' handles replication	26
8. Consistent presentation of Directory Information Tree (DIT) across ALL: 'slapd' instances	26
9. Simpler configuration.....	26
Note: 'slapd-config' influences dedicated configuration DIT instead of standalone configuration file: 'slapd.conf'	27
Note: Configuration is still largely the same, just stored inside of LDAP instead of outside in a configuration file.....	27
10. In-built support to convert from: 'slapd.conf' to 'slapd-config' - auto-updated on Debian Ubuntu if exists: 'slapd.conf'	27
11. Services driven primarily by: 'slapd'.....	27
12. LDAP Entries (Unique amalgamations of values) consist of:.....	27
13. Common implementations follow DNS: i.e. raja.internal => i.e. dc=raja,dc=internal,o=raja,ou=training	28
14. It is common internally to use a sub-domain of Internet-routable naming scheme: i.e. raja.com, ad.raja.com, it.ad.raja.com.....	28
15. Entries are referenced using: Distinguished Names (DNs) - Concatenations of entries' attributes	28

16. Directory Information Tree (DIT) - maintained by 'slapd' instances	28
17. Single configuration via - 'slapd-config'	28
18. Ability to dynamically configure: 'slapd' instances - sans server restart	28
19. Support for a variety of back-ends: BDB, HDB(Default), Custom (i.e. scripts, etc.), other DBMSs (MySQL, Oracle)	29
20. Referrals - LDAP can refer client requests to appropriate 'slapd' instance(s)	29
21. SASL Support for Authentication	29
22. TLS SSL Support for Encryption - Confidentiality & Integrity - 'ldaps://' - TCP:636	29
23. Unix Domain Sockets (UDS) Support - 'ldapi://' - local access via UDS	29
24. Logging is configurable and defaults to: LOCAL429	
25. Overlays - Additional (modular) functionality providing hooks to various behaviors: i.e. logging....	29
Chapter 2.....	31
Installation, Exploration and Environment.....	31
Topology:	31
Features:	32
1. Primary daemon: 'slapd'	32
2. Configured dynamically via: 'slapd.d/' - 'ldiff' entries - these reflect configurations maintained in new 'slapd' DIT configuration	32

6 LPIC-3 300(Part1:OpenLDAP 2.4) راهنمای سریع مدرک بین‌المللی

Note: This gives us a file system (FS) view of the current configuration..... 32

Note: These files (beneath: slapd.d/) are NOT to be modified directly, but rather via DTI configuration: 'cn=config' (DIT) 32

Execution:..... 32

Note: If necessary, provide directives via: 'slapd.conf' 34

Note: Do NOT modify LDIF entries directly - Use: 'ldapadd, ldapmodify, ldapdelete' 34

3. Dynamic Configuration Engine - requires fewer server restarts 34

4. 'slapd.conf' - deprecated - Use: 'slapd-config' command to effect changes dynamically 34

Tasks:..... 34

1. Install 'slapd' on both servers - rajaopenldap[12] 34

--For ubuntu(a,b)..... 34

Note: If installer does NOT prompt for 'Admin' password and domain info, then run: 'dpkg-reconfigure -plow slapd' - permits defaults..... 34

-- From Document:
<http://www.openldap.org/doc/admin24/install.html>

--not work on CentOS6 35

a. Get the software 35

b. Unpack the distribution 35

Execution:..... 36

c. Run configure 36

d. Build the software..... 37

e. Test the build.	37
f. Install the software.	38
g. Edit the configuration file.	38
Execution:.....	41
g. Import the configuration database.....	46
command:	46
Execution:.....	47
Notice:Not work!!!!!! on Centos 6.....	47
Installing and configuring OpenLDAP on Centos 6: .	47
i) Run the following command:	47
ii) Generate a password hash to be used as the admin password. This password hash will be used when you create the root user for your LDAP installation. For example:.....	48
iii) While editing this file, change the distinguished name (DN) of the olcSuffix to something appropriate. The suffix typically corresponds to your DNS domain name, and it will be appended to the DN of every other LDAP entry in your LDAP tree.	48
Note: If the olcRootPW attribute does not already exist, create it. Then set the value to be the hash you created from slappasswd. For example:.....	48
iv) Modify the DN of the root user in the olcDatabase={1}monitor.ldif file to match the olcRootDN line in the olcDatabase={2}bdb.ldif file. Do the following:	49
v) Hide the password hashes from users who should not have permission to view them.	49

8 راهنمای سریع مدرک بین‌المللی (LPIC-3 300(Part1:OpenLDAP 2.4))

vi)Make sure that OpenLDAP is configured to start when the machine starts up, and start the OpenLDAP service.	50
h.Start SLAPD.	50
Note: the use of single quotes around command parameters to prevent special characters from being	50
Execution:.....	51
i.Add initial entries to your directory.....	52
i. create an LDIF file.....	52
ii. run ldapadd	52
Execution:.....	54
k.See if it works.	56
l.You are now ready to add more entries using ldapadd(1) or another LDAP client, experiment with various configuration options, backend arrangements, etc.....	56
Execution:.....	56
##### Add a use to LDAP	58
##### Adding a user to a group	64
2. Confirm running 'slapd'	67
3. Install Jxplorer for graphical use	68
4. Explore configuration.....	69
Execution:.....	69
Execution:.....	70
Execution:.....	71
Execution:.....	73
Execution:.....	83

Index	9
Execution:.....	86
Execution:.....	87
Execution for client utilities:	99
Chapter 3.....	101
'slapd-config' - Configuration	101
Features:	101
1. LDAP-stored and driven configuration	101
2. Reduces the likelihood of a damaged configuration due to human error, because changes must be effected via front-end tools: i.e.	
'ldap[add modify delete] - 'slapd-config'	101
3. 'cn=config' - root of configuration of LDAP instance - server-wide configuration attributes.....	101
4. 'slapd.conf' - still supported, but deprecated - Debian-systems (Ubuntu Debian) auto-migrate entries from: 'slapd.conf'	102
Configuration - 'slapd-config'	102
Tasks:.....	102
1. Explore 'slapd-config' hierarchy.....	102
Execution:.....	102
Execution:.....	106
Note: If you need to implement feature in OpenLDAP via 'cn=config' mechanism, you will often prefix the directive with: 'olc' to indicate OpenLDAP	
Configuration entry: i.e. 'slapd.conf' supported directive would usually be prefixed with:	
'olcNameOfDirective'	107

10	LPIC-3 300(Part1:OpenLDAP 2.4) راهنمای سریع مدرک بین‌المللی	
	Execution:.....	107
	2. Dump Default Configuration - Fully-amalgamated	
	108
	Solve the problem:.....	109
	Execution:.....	110
	3. Enable logging with: 'cn=config'	111
	Execution:.....	112
	Note: This is a realtime, configuration change sans	
	need to restart 'slapd'	112
	Note: Base of interest in new configuration is:	
	'cn=config' - change keys/values that drive server	
	behavior here.....	112
	Execution:.....	113
	Chapter 4.....	115
	LDAP Entries and Commands.....	115
	dc=raja,dc=internal, o, ou, users, machines, groups,	
	etc.	115
	Tasks:.....	115
	1. Create basic top-level entries	
	in:dc=raja,dc=internal	115
	Execution:.....	116
	Execution:.....	117
	Note: 'ldapadd' permits multiple records sans	
	delimiting '-' unlike 'ldapmodify'.....	120
	Note: '-c' option will skip errors pertaining to existing	
	records	120
	Current Structure:.....	120

Index	11
2. Search for objects	121
Execution:.....	121
Note: Default search from: 'dc=raja,dc=internal' reveals ALL objects in DIT (dc=raja,dc=internal)....	125
3. Filter Results.....	125
Execution:.....	125
4. Add Users	127
Execution:.....	128
Execution:.....	130
Execution:.....	130
5. Change Users' Passwords.....	139
Execution:.....	139
4. Modify Users' details	149
Note: When modifying records with: 'ldapmodify', separate actions (add,replace,delete) with '-', but separate records (LDAP DN's) with whitespace	149
Execution:.....	149
5. Delete User	150
Execution:.....	150
Chapter 5.....	153
LDAP Authentication	153
# LDAP AUTH - Centralized Accounts #.....	153
Definition:	153
1. Centralized accounts.....	153
2. Centralized configuration data for applications: i.e. MySQL, Postfix, Apache, etc.	153
3. Reduced administrative overhead.....	153

12 راهنمای سریع مدرک بین‌المللی (LPIC-3 300(Part1:OpenLDAP 2.4))

Typical Stack:	153
1. AUTH Client (LDAP Client).....	153
2. PAM Hook	153
3. NSS Hook.....	154
#RedHat CentOS Clients - LDAP AUTH #	154
Features:	154
1. Uses: sssd to cache and interact with directory services: i.e. LDAP, NIS, ADS, etc.	154
2. Stack:.....	154
Tasks:.....	154
1. Review Build stack.....	154
Execution:.....	155
Note: 'authconfig' is \$SHELL alternative to updating CLIENT AUTH mechanism of CentOS RedHat	
instances	161
Execution:.....	161
2. Test access to LDAP Directory Users.....	162
Execution:.....	162
Note: If this fails, re-run: 'system-config- authentication' and check settings	175
3. Update PAM config to auto-create \$HOME	176
Execution:.....	176
4. Update using 'ldapmodify' cn=raja3 to have 'loginShell' attribute.....	178
Execution:.....	178
Note: new login session may be required	182
Tasks:.....	182
1. Configure Ubuntu to use LDAP AUTH.....	182

Note: 'nscd' - will cache lookups of: passwd, group, hosts.....	183
Note: UDS 'ldapi://' - requires no AUTH to view entries in LDAP	183
Note: If problems accessing LDAP, re-configure with: 'dpkg-reconfigure ldap-auth-config'	183
2. Configure dependent LDAP client components	183
Note: prepend: 'passwd', 'group', and 'shadow' with: 'ldap ' - to allow NSSWITCH to search LDAP for results	183
3. Prepare for new AUTH environment	184
4. SSH to local LDAP clients as LDAP users	184
5. Ensure that: rajaubudesk2 also uses common LDAP	184
6. Confirm current LDAP client access	184
Note: On CentOS RedHat systems - check: /etc/openldap/ldap.conf to ensure appropriate LDAP URI(s)	185
Note: If LDAP users have: 'uid=raja' (existing user: i.e. raja), there will be ambiguity upon login. Ensure that LDAP users do NOT use uid=existing users.....	185
Note: LDAP permits each user object to have multiple 'uid' values, which may conflict with: /etc/passwd users	185
#Debian Clients - LDAP AUTH #	185
Tasks:.....	185
1. Configure Debian clients to use LDAP servers as AUTH sources	185

14 LPIC-3 300(Part1:OpenLDAP 2.4) راهنمای سریع مدرک بین‌المللی

Note: Password AUTH issues often relate to mismatch in LDAP client algorithm default: i.e. Server uses: SHA256, client supports MD5..... 186

Note: Ensure that ALL LDAP clients use matching algors with LDAP server 186

Chapter 6..... 187

LDAP Account Manager - Enterprise LDAP

Administration 187

Features: 187

1. Web GUI to assist with LDAP DIT Management 187

2. Schema Browser 187

Note : I use jxplorer for LDAP DIT Management. ... 187

Tasks:..... 187

1. Install & Explore 187

2. Use Interface - Update defaults..... 188

3. Clean-up existing users 188

4. Create new users 188

5. Test connectivity 188

Note: Now that MD5 algo is part-and-parcel of ALL users, AUTH issues should be fixed 189

6. Further exploration 189

Note: Use: 'slappasswd' to generate password strings for user accounts when using LDAP client utilities 189

Note: By default, pam_mkhome.so will apply the \$USER as the owner of their \$HOME. This may not be desirable for some applications: i.e. 'sftp' in restricted, high-security mode. In this case, tweak

pam_mkhome.so accordingly to flag permissions as: i.e. 'root.root'.....	189
Note: Default LDAP implementation permits ALL users, including anonymous, access to 'read' contents of Default DIT - dc=raja,dc=internal.....	190
Chapter 7.....	191
Replication.....	191
Features:	191
1. New model: Provider Consumer - instead of Master Slave.....	191
2. Providers (Masters) and Consumers (Slaves) can interchange roles	191
3. Syncrepl.....	191
Note: If connections are unstable, then use: 'refreshOnly'(pull) synchronization.....	191
4. Synchs are provided via special searches by consumer to provider: i.e. 'ldapsearch...'	192
5. Each synched object(record) has unique: entryUUID attribute - more unique than DN because DN is subject to change	192
6. Single-Master && Multi-Master Replication Supported	192
7. Replicas can be built from backups or using syncrepl (auto-converges)	192
8. Replication configuration is made directly to DIT DBs	192
Tasks:.....	192

16	LPIC-3 300(Part1:OpenLDAP 2.4) راهنمای سریع مدرک بین‌المللی	
	Execution:.....	193
	1. Server Configuration	193
	Execution:.....	193
	Note: We will assume for now that 'cn=repl' has access to read DIT	196
	2. Client Configuration	197
	3. Create Dummy POSIX accounts and ensure replication	200
	4. Add: 'rajabuild2' as Consumer of: 'rajaopenldap1'	200
	Note: 'usermod', 'userdel', and 'useradd' do NOT update LDAP by default	202
	Note: 'passwd' command has special hook for LDAP and local users	202
	Execution:.....	202
	1)Configure LDAP Provider. Add syncprov module.	203
	2) Configure LDAP Consumer.....	204
	Note: spaces are important	204
	3) Configure LDAP Client to bind LDAP Consumer, too.....	205
	Very Important Note: after ldapsearch the consumer or slave(rajaopenldap2.raja.internal) you not receive updates and it seem replication not work.....	205
	The Provider or Master result:.....	209
	Chapter 8.....	237
	LDAP over TLS - Secure Communications	237

Features:	237
1. Secure communications over standard LDAP port of: TCP:389 (Default).....	237
Note: Traditionally, LDAP functioned over 2-ports: TCP:389(Clear-text) && TCP:636(Secure)(-H ldaps:///)	237
Note: (ldaps://) - considered deprecated - use: LDAP over TLS via TCP:389	237
Note: With this model, clients will attempt to use: TLS if available, with clear-text if unavailable.....	237
Tasks:.....	237
1. Examine default connection	237
2. Install TLS support on servers: rajaopenldap[12]	238
Note: '/etc/ssl/private/cakey.pem' && '/etc/ssl/certs/cacert.pem' - form the keypair for the self-signed CA server.....	239
# TLS Client Configuration #.....	241
Features:	241
1. Secure client communications with LDAP Servers - Not Default.....	241
2. Clear-text is a fallback for default connections using TLS: i.e. '-Z'	241
Tasks:.....	241
1. Update 'ldap.conf' client configuration file	241
Note: Default Linux bundle containing numerous certs except internal, self-signed certs.....	242

18 راهنمای سریع مدرک بین‌المللی (LPIC-3 300(Part1:OpenLDAP 2.4))

Note: One tactic is to append OpenLDAP TLS cert to generic: '/etc/ssl/certs/ca-certificates.crt' 242

Note: Another tactic, is to create a new, OpenLDAP-specific bundle file: i.e. '/etc/ssl/certs/cacert.pem' 242

Note: TLS | SSL clients auto-cycle through available certs in bundle files 242

2. Test Default Connection to Server 242

Note: Ensure that '/etc/hosts' && | | DNS are updated accordingly to fulfill extra check of: '-ZZ'. 243

Note: At this point, both LDAP servers still support clear-text communications 243

3. Force TLS | SSL Connection 243

Note: Applied per-database | | globally (systemwide) 243

Note: Replication MUST be updated to support TLS if DB requires confidentiality 244

URL:
<https://help.ubuntu.com/12.04/serverguide/openldap-server.html> 244