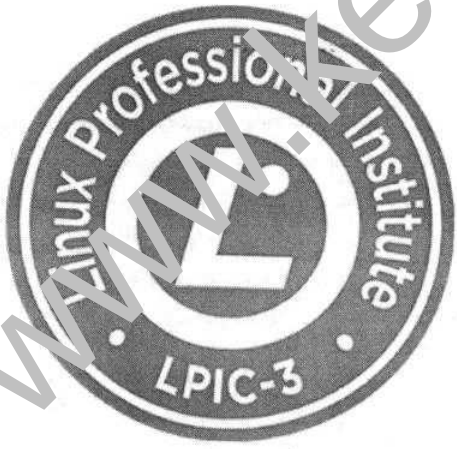
کانون نشر علوم

راهنمای کاربردی مدرک بین المللی

لینوکس

PIC-3 300 (Part1: OpenLDAP 2.4)

(جلد دوم، خلاصه، مثال‌ها و سناریوهای عملی اجرا شده)



مؤلف:

مهندس سید حسین رجاء

ناشر:
کانون نشر علوم

کانون نشرعلوم
www.nashreoloom.com
پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سرشناسه: رجاء، سیدحسین، ۱۳۶۲ -
عنوان و نام پدیدآور: راهنمای کاربردی مدرک بین‌المللی لینوکس LPIC-3 300 (OpenLDAP2.4)/ مولف سیدحسین رجاء
مشخصات نشر: تهران: انتشارات آترا: کانون نشر علوم، ۱۳۹۵.
مشخصات ظاهری: ۲ ج.: مصور، جدول، نمودار.
شابک: ۹۷۸۶۰۰۶۴۲۵۴۵۰: دوره؛ ۹۷۸۶۰۰۶۴۲۵۳۵۱:ج.۱؛ ۹۷۸۶۰۰۶۴۲۵۴۴۳:ج.۲
وضعیت فهرست‌نویسی: فیپا
مندرجات: ج. ۱. مفاهیم، نصب و راه‌اندازی، پیکربندی و مدیریت.- ج. ۲. خلاصه، مثال‌ها و سناریوهای عملی اجرا شده.
موضوع: سیستم‌عامل لینوکس
موضوع: Linux
موضوع: سیستم‌های عامل (کامپیوتر)
موضوع: Operating systems (Computers)
رده‌بندی کنگره: ۱۳۹۵ ۹۴ر۲۶۲ QA ۷۶/۷۶
رده‌بندی دیویی: ۰۰۵/۴۳۲
شماره کتابشناسی ملی: ۴۴۰۸۱۴۲

نام کتاب: راهنمای کاربردی مدرک بین‌المللی لینوکس LPIC-3 300 (Part1: OpenLDAP ...
(جلد دوم: خلاصه، مثال‌ها و سناریوهای عملی اجرا شده)
ناشر: آترا
ناشر همکار: کانون نشرعلوم
مؤلف: سید حسین رجاء
صفحه‌آرا: فاطمه آدیگوزل‌پور اردبیلی
طرح جلد: زهرا سلطان‌آبادی
چاپ اول: پاییز ۱۳۹۵
تیراژ: ۱۰۰۰
چاپ و صحافی: کانون نشر علوم
قیمت دوره دوجلدی: ۴۵۰۰۰ تومان
شابک جلد دوم: ۹۷۸۶۰۰۶۴۲۵۴۴۳
شابک دوره: ۹۷۸۶۰۰۶۴۲۵۴۵۰

مراکز پخش:
پخش علوم: خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد۱
تلفن: ۶۶۴۹۴۹۱۱-۶۶۹۶۱۵۶۸
نشر و پخش آترا: میدان انقلاب، خیابان جمالزاده جنوبی، کوچه شهید آقاصبوری، پلاک ۱۳
تلفن: ۶۶۹۲۲۰۸۲

سخن ناشر

به نام خداوند بخشنده و مهربان

گستره دانش بشری در برابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ همچنان که کریمه «و ما عطا نکردیم به شما علم را جز اندکی» شاهدی است بر ضعف معرفت انسانی نسبت به حکمت صَمَدانی. با این حال چه نیکو سفارش فرموده است خاتم انبیاء، حضرت محمد مصطفی (ص)، که «بجویید علم را اگر چه به سرزمین چین». این توصیه، تمامی پیروان راستین دین حنیف اسلام را به فراگیری و اکتساب علوم و فنون مختلف در همه زمان‌ها و همه مکان‌ها فرا خوانده است.

تلاش کانون نشر علوم، همراه مصروف به تولید آثار شایسته و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه دشواری‌ها و دشواری‌های فراوانی حادث شده و خواهد شد. این امر تا حدّی بسیار، تابعی از ماهیت رشته‌های فنی و مهندسی و معارف مربوط به آنهاست؛ چرا که این رشته‌ها به‌سرعت و بی‌وقفه در حال نوشدن می‌باشند. این امر رسالت کانون نشر علوم را در نشر آثار مربوطه، اعم از تألیف یا ترجمه، خطیر کرده و می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی در خور شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند منّان در این مهم مساعدت فرماید.

پایان سخن اینکه، کانون نشر علوم دست یاری و همّت تمامی مؤلفین و مترجمین علاقه‌مند در زمینه علوم فنی و مهندسی را به‌گرمی می‌فشارد و تمامی ایشان را خاضعانه و خاشعانه به همکاری فرا می‌خواند. همچنین این مجموعه از تمامی مخاطبین استدعا دارد که با نظرات صائب و راهگشای خود، در بهبود شکلی و محتوایی آثار منتشر شده مساعدت فرمایند؛ و صد البته که تمامی کاستی‌ها از این رهگذر تنها و تنها متوجه این مجموعه بوده و هست.

سید محمدحسین منوّری
کانون نشر علوم

فهرست مطالب

Course Objectives **13**
Introduction - Features 13
Installation | Exploration 13
Introduction to SLAPD LDAP Configuration 13
LDAP Entries 13
Client Authentication 13
Debian | CentOS Clients 14
LDAP Account Manager 14
Replication 14
TLS | SSL Configuration 14

Chaptert 1: OpenLDAP 2.4 Features **15**
1. Current Major Release: 2.4x - in contrast to 2.3x 15
2. Industry Standard Directory Services via: Standalone LDAP Server 'slapd' 15
3. Centralized access to common information: 15
4. Facilitates the current Virtulization 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) 15
5. Provides fast searches of such data 15
6. Quite scalable at providing access to key data 15
7. Replication (distribution) of content across N nodes as needed 15
Note: 'slurpd' is no longer used for replication - 'slapd' handles replication 15
8. Consistent presentation of Directory Information Tree (DIT) across ALL: 'slapd' instances 15
9. Simpler configuration 15
Note: 'slapd-config' influences dedicated configuration DIT instead of standalone configuration file: 'slapd.conf' 15
Note: Configuration is still largely the same, just stored inside of LDAP instead of outside in a configuration file 16
10. In-built support to convert from: 'slapd.conf' to 'slapd-config' - auto-updated on Debian | Ubuntu if exists: 'slapd.conf' 16
11. Services driven primarily by: 'slapd' 16
12. LDAP Entries (Unique amalgamations of values) consist of: 16
13. Common implementations follow DNS: i.e. raja.internal => i.e. dc=raja,dc=internal,o=raja,ou=training 16
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 16

15. Entries are referenced using: Distinguished Names (DNs) - Concatenations of entries' attributes 16
16. Directory Information Tree (DIT) - maintained by 'slapd' instances 16
17. Single configuration via - 'slapd-config' 16
18. Ability to dynamically configure: 'slapd' instances - sans server restart 16
19. Support for a variety of back-ends: BDB, HDB(Default), Custom (i.e. scripts, etc.), other DBMSs (MySQL, Oracle) 16
20. Referrals - LDAP can refer client requests to appropriate 'slapd' instance(s) 16
21. SASL Support for Authentication 16
22. TLS | SSL Support for Encryption - Confidentiality & Integrity - 'ldaps:' - TCP:636 16
23. Unix Domain Sockets (UDS) Support - 'ldapi://' - local access via UDS 16
24. Logging is configurable and defaults to: LOCAL4 16
25. Overlays - Additional (modular) functionality providing hooks to various behaiors: i.e. logging. 16

Chaptert 2: Installation,Exploration and Environment 17
Topology: 17
Features: 17
1. Primary daemon: 'slapd' 17
2. Configured dynamically via: 'slapd.d/' - 'ldiff' entries - these reflect configurations maintained in new 'slapd' DIT configuration 17
Note: This gives a file system (FS) view of the current configuration 17
Note: These files (beneath: slapd.d/) are NOT to be modified directly, but rather via DTI configuration 'cn=config' (DIT) 17
Execution: 17
Note: If necessary, provide directives via: 'slapd.conf' 18
Note: DO NOT modify LDIFF entries directly - Use: 'ldapadd, ldapmodify, ldapdelete'. 18
3. Dynamic Configuration Engine - requires fewer server restarts 18
4. 'slapd.conf' - deprecated - Use: 'slapd-config' command to effect changes dynamically 18
Tasks: 18
1. Install 'slapd' on both servers - rajaopenldap[12] 18
--For ubuntu(a,b) 18
Note: If installer does NOT prompt for 'Admin' password and domain info, then run: 'dpkg-reconfigure -plow slapd' - permits defaults 18
-- From Document: http://www.openldap.org/doc/admin24/install.html --not work on CentOS6 19
a.Get the software 19
b.Unpack the distribution 19
Execution: 19
c.Run configure 19
d.Build the software. 20

e.Test the build. 20
f. Install the software 20
g. Edit the configuration file. 21
Execution: 22
g. Import the configuration database 26
command: 26
Execution: 26
Notice:Not work!!!!!! on Centos 6 26
Installing and configuring OpenLDAP on Centos 6: 26
i) Run the following command: 26
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: 26
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 will be appended to the DN of every other LDAP entry in your LDAP tree. 27
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: 27
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. Enter the following: 27
v) Hide the password hashes from users who should not have permission to view them. 27
vi) Make sure that OpenLDAP is configured to start when the machine starts up, and start the OpenLDAP service. 28
h. Start SLAPD. 28
Note: the use of single quotes around command parameters to prevent special characters from being 28
Execution: 28
i. Add initial entries to your directory. 29
i. create an LDIF file 29
ii. run ldapadd 29
Execution: 30
k. See if it works 31
l. You are now ready to add more entries using ldapadd(1) or another LDAP client, experiment with various configuration options, backend arrangements, etc. 32
Execution: 32
####### Add a use to LDAP 33
########## Adding a user to a group 37
2. Confirm running 'slapd' 39
3. Install Jxplored for graphical use 39
4. Explore configuration 40
Execution: 40
Execution: 40
Execution: 41

Execution:.... 42
Execution:.... 47
Execution:.... 49
Execution:.... 50
Execution for server utilities:.... 51
Execution for client utilities:.... 58

Chaptert 3: 'slapd-config' - Configuration.... **59**
Features:.... 59
1. LDAP-stored and driven configuration.... 59
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'.... 59
3. 'cn=config' - root of configuration of LDAP instance - server-wide configuration attributes.... 59
4. 'slapd.conf' - still supported, but deprecated - Debian-systems (Ubuntu | Debian) auto-migrate entries from: 'slapd.conf'.... 59
Configuration - 'slapd-config'.... 59
Tasks:.... 59
1. Explore 'slapd-config' hierarchy.... 59
Execution:.... 59
Execution:.... 61
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'.... 61
Execution:.... 62
2. Dump Default Configuration - Fully-amalgamated.... 62
Solve the problem:.... 63
Execution:.... 63
3. Enable logging with: 'cn=config'.... 64
Execution:.... 64
Note: This is a realtime, configuration change sans need to restart 'slapd'.... 64
Note: Base of interest in new configuration is: 'cn=config' - change keys/values that drive server behavior here.... 64
Execution:.... 64

Chaptert 4: LDAP Entries and Commands.... **67**
dc=raja,dc=internal, o, ou, users, machines, groups, etc.... 67
Tasks:.... 67
1. Create basic top-level entries in:dc=raja,dc=internal.... 67
Execution:.... 67
Execution:.... 68

Note: 'ldapadd' permits multiple records sans delimiting '-' unlike 'ldapmodify' 69
Note: '-c' option will skip errors pertaining to existing records 69
Current Structure: 69
2. Search for objects 70
Execution: 70
Note: Default search from: 'dc=raja,dc=internal' reveals ALL objects in DIT (dc=raja, dc=internal) 72
3. Filter Results 72
Execution: 72
4. Add Users 73
Execution: 74
Execution: 75
Execution: 75
5. Change Users' Passwords 80
Execution: 80
4. Modify Users' details 85
Note: When modifying records with: 'ldapmodify', separate actions (add,replace,delete) with '-', but separate records (LDAP DNs) with whitespace 85
Execution: 85
5. Delete User 86
Execution: 86

Chaptert 5: LDAP Authentication 87
LDAP AUTH - Centralized Accounts 87
Definition: 87
1. Centralized accounts 87
2. Centralized configuration data for applications: i.e. MySQL, Postfix, Apache, etc. 87
3. Reduced administrative overhead 87
Typical Stack: 87
1. AUTH Client (LDAP Client) 87
2. PAM Hook 87
3. NSS Hook 87
#RedHat | CentOS Clients - LDAP AUTH # 87
Features: 87
1. Uses: sssd to cache and interact with directory services: i.e. LDAP, NIS, ADS, etc. ... 87
2. Stack: 88
Tasks: *88*
1. Review | Build stack *88*
Execution: *88*
Note: 'authconfig' is $SHELL alternative to updating CLIENT AUTH mechanism of CentOS | RedHat instances *92*

Execution:..... 92
2. Test access to LDAP Directory Users..... 92
Execution:..... 92
Note: If this fails, re-run: 'system-config-authentication' and check settings..... 100
3. Update PAM config to auto-create $HOME..... 100
Execution:..... 100
4. Update using 'ldapmodify' cn=raja3 to have 'loginShell' attribute..... 101
Execution:..... 101
Note: new login session may be required..... 103
Tasks:..... 103
1. Configure Ubuntu to use LDAP AUTH..... 103
Note: 'nscd' - will cache lookups of: passwd, group, hosts..... 104
Note: UDS 'ldapi://' - requires no AUTH to view entries in LDAP..... 104
Note: If problems accessing LDAP, re-configure with: 'sudo dpkg-reconfigure ldap-auth-config'..... 104
2. Configure dependent LDAP client components..... 104
Note: prepend: 'passwd', 'group', and 'shadow' with: 'ldap ' - to allow NSSWITCH to search LDAP for results..... 104
3. Prepare for new AUTH environment..... 104
Note: Add user as objectclass=POSIX_USER to realize via LDAP AUTH client: i.e. 'getent passwd'..... 104
4. SSH to local LDAP clients as LDAP users..... 104
5. Ensure that: raja@ubdesk2 also uses common LDAP..... 104
6. Confirm current LDAP client access..... 105
Note: On CentOS / RedHat systems - check: /etc/openldap/ldap.conf to ensure appropriate LDAP URIs..... 105
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..... 105
Note: LDAP permits each user object to have multiple 'uid' values, which may conflict with: /etc/passwd users..... 105
#Debian Clients - LDAP AUTH #..... 105
Tasks:..... 105
1. Configure Debian clients to use LDAP servers as AUTH sources..... 105
Note: Password AUTH issues often relate to mismatch in LDAP client algorithm default: i.e. Server uses: SHA256, client supports MD5..... 106
Note: Ensure that ALL LDAP clients use matching algors with LDAP server..... 106

Chaptert 6: LDAP Account Manager - Enterprise LDAP Administration..... 107
Features:..... 107
1. Web GUI to assist with LDAP DIT Management..... 107
2. Schema Browser..... 107

Note : I use jxplorer for LDAP DIT Management. 107
Tasks: 107
1. Install & Explore 107
2. Use Interface - Update defaults 107
3. Clean-up existing users 107
4. Create new users 108
5. Test connectivity 108
Note: Now that MD5 algo is part-and-parcel of ALL users, AUTH issues should be fixed .. 10
6. Further exploration 108
Note: Use: 'slappasswd' to generate password strings for user accounts when using LDAP client utilities 108
Note: By default, pam_mkhomedir.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_mkhomedir.so accordingly to flag permissions as: i.e. 'root/root' 108
Note: Default LDAP implementation permits ALL users, including anonymous, access to 'read' contents of Default DIT - dc=raja,dc=internal 108

Chaptert 7: Replication **109**
Features: 109
1. New model: Provider | Consumer - instead of Master | Slave 109
2. Providers (Masters) and Consumers (Slaves) can interchange roles 109
3. Syncrepl 109
Note: If connections are unstable, then use 'refreshOnly'(pull) synchronization 109
4. Synchs are provided via special searches by consumer to provider: i.e. 'ldapsearch...' 109
5. Each synched object(record) has unique: entryUUID attribute - more unique than DN because DN is subject to change 109
6. Single-Master && Multi-Master Replication Supported 109
7. Replicas can be built from backups or using syncrepl (auto-converges) 109
8. Replication configuration is made directly to DIT DBs 110
Tasks: 110
Execution: 110
1. Server Configuration 110
Execution: 110
Note: We will assume for now that 'cn=repl' has access to read DIT 111
2. Client Configuration 112
3. Create Dummy POSIX accounts and ensure replication 113
4. Add: 'rajabuild2' as Consumer of: 'rajaopenldap1' 113
Note: 'usermod', 'userdel', and 'useradd' do NOT update LDAP by default 114
Note: 'passwd' command has special hook for LDAP and local users 114
Execution: 115

1) Configure LDAP Provider. Add syncprov module. 115
2) Configure LDAP Consumer. 115
Note: spaces are important 115
3) Configure LDAP Client to bind LDAP Consumer, too. 116
Very Important Note: after ldapsearch the consumer or slave(rajaopenldap2.raja.internal) you not recive updates and it seem replication not work. 116
The Provider or Master result: 118

Chaptert 8: LDAP over TLS - Secure Communications 133
Features: 133
1. Secure communications over standard LDAP port of TCP:389 (Default) 133
Note: Traditionally, LDAP functioned over 2-ports: TCP:389(Clear-text) && TCP:636(Secure)(-H ldaps:///) 133
Note: (ldaps:///) - considered deprecated - use: LDAP over TLS via TCP:389 133
Note: With this model, clients will attempt to use TLS if available, with clear-text if unavailable 133
Tasks: 133
1. Examine default connection 133
2. Install TLS support on server: rajaopenldap[12] 133
Note: '/etc/ssl/private/cakey.pem' && '/etc/ssl/certs/cacert.pem' - form the keypair for the self-signed CA server 134
TLS Client Configuration 135
Features: 135
1. Secure client communications with LDAP Servers - Not Default 135
2. Clear-text as a fallback for default connections using TLS: i.e. '-Z' 135
Tasks: 135
1. Update 'ldap.conf' client configuration file 135
Note: Default Linux bundle containing numerous certs except internal, self-signed certs 135
Note: One tactic is to append OpenLDAP TLS cert to generic: '/etc/ssl/certs/ca-certificates.crt' 135
Note: Another tactic, is to create a new, OpenLDAP-specific bundle file: i.e. '/etc/ssl/certs/cacert.pem' 135
Note: TLS | SSL clients auto-cycle through available certs in bundle files 135
2. Test Default Connection to Server 135
Note: Ensure that '/etc/hsots' && || DNS are updated accordingly to fulfill extra check of: '-ZZ' 136
Note: At this point, both LDAP servers still support clear-text communications 136
3. Force TLS | SSL Connection 136
Note: Applied per-database || globally (systemwide) 136
Note: Replication MUST be updated to support TLS if DB requires confidentiality 136
URL: https://help.ubuntu.com/12.04/serverguide/openldap-server.html 136