

سازمان نشر علوم
۱۴۴۸۶۴۸



کانون نشر علوم

راهنمای کاربردی مدرک بین‌المللی

لینوکس

LPIC-3 301(OpenLDAP 2.3)

(جلد دوم: مثال‌ها و سناریوهای عملی اجرا شده)



مؤلف:

مهندس سید حسین رجاء

ناشر:

کانون نشر علوم



ناشر علوم

www.nashreloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سرشناسه: رجاء، سید حسین، ۱۳۶۲ -

عنوان و نام پدیدآور: راهنمای کاربردی مدرک بین‌المللی لینوکس (LPIC-3 301 (openLDAP2.3/ مولف سید حسین رجاء، مشخصات نشر: تهران: کانون نشر علوم: انتشارات آترا، ۱۳۹۵.

مشخصات ظاهری: ۲ ج.

شابک: ۹۷۸۹۶۴۳۲۷۱۵۶۵ : دوره ۱ : ۹۷۸۹۶۴۳۲۷۱۵۴۱ ج ۱ : ۹۷۸۹۶۴۳۲۷۱۵۵۸ ج ۲

وضعیت فهرست‌بسی: فیا

مندرجات: ج ۱: سیستم، نحوه و راه‌اندازی، پیکربندی و مدیریت-ج ۲: خلاصه، مثال‌ها و سناریوهای عملی اجرا شده.

موضوع: سیستم عامل لینوکس

موضوع: Linux

موضوع: سیستم‌های عامل (کامپیوتر)

موضوع: Operating Systems (Computers)

رده‌بندی کنگره: ۱۳۹۵ ۹۴۳۶۰۵ QA ۷۶۱

رده‌بندی دیویی: ۰۵/۴۳۲

شماره کتابشناسی ملی: ۴۱۵۴۹۲۰

نام کتاب: راهنمای کاربردی مدرک بین‌المللی لینوکس (LPIC-3 301 (OpenLDAP 2.3

(جلد دوم: خلاصه مثال‌ها و سناریوهای عملی اجرا شده.)

ناشر: کانون نشر علوم

ناشر همکار: آترا

مولف: سید حسین رجاء،

صفحه‌آرا: فاطمه آدیگوزل‌پور اردبیلی

طرح جلد: زهرا سلطان آبادی

چاپ اول: پاییز ۱۳۹۵

تیراژ: ۱۰۰۰

چاپ و صحافی: کانون نشر علوم

قیمت دوره دو جلدی: ۳۸۰۰۰ تومان

شابک جلد دوم: ۹۷۸۹۶۴۳۲۷۱۵۵۸

شابک دوره: ۹۷۸۹۶۴۳۲۷۱۵۶۵

مراکز پخش:

پخش علوم، خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد ۱

تلفن: ۶۶۹۶۱۵۶۸-۶۶۴۹۴۹۱۱

پخش آترا، میدان انقلاب، خیابان جمالزاده جنوبی، کوچه شهید آقا صبوری، پلاک ۱۳

تلفن: ۶۶۹۴۲۰۸۲



سخن ناشر

به نام خداوند بخشنده و مهربان

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

تلاش کانون نشر علوم، هواره موقوف به تولید آثار شایسته و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه مشکلات دشواری‌های فراوانی حادث شده و خواهد شد. این امر تا حدی بسیار، تابعی از ماهیت رشته‌های فنی و مهندسی و معارف مربوط به آنهاست؛ چرا که این رشته‌ها به سرعت و بی‌وقفه در حال نو شدن و نو شدن می‌باشند. این امر رسالت کانون نشر علوم را در نشر آثار مربوطه، اعم از تألیف یا ترجمه، خطری تر کرده و می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که آثار فاخره علوم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن رعایت علمی، در خور شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند متّان در این راه هم مساعدت فرماید.

پایان سخن اینکه، کانون نشر علوم دست یاری و همت تمامی مؤلفین و مترجمین علاقه‌مند در زمینه علوم فنی و مهندسی را به گرمی می‌فشارد و تمامی ایشان را مساعدت 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 منوری

کانون نشر علوم



فهرست مطالب

Course Objectives	11
Introduction - Features.....	11
LDAP Concepts	11
Master Server Configuration	11
Define Directory Information Tree (DIT)	11
Configure Replication.....	12
LDAP Add.....	12
LDAP Delete	12
LDAP Modify	12
LDAP Search	13
Logging	13
LDIF	13
LDAP Schemas.....	14
Migrate to LDAP Authentication	14
Syncrpl Replication.....	14
LDAP Security	14
Chapter 1: OpenLDAP Features.....	15
1. Centralized directory of useful information (user accounts, contacts, mail info, address, etc.)	15
2. Optimized for Reads.....	15
3. Redundant Configuration	15
4. Namespace is similar to DNS: i.e. dc=raja,dc=internal DNS(raja.internal)	15
5. Supports AUTH encryption of clear-text AUTHS - LDAPS - TCP:636	15
6. Supports StartTLS over regular TCP:389 LDAP port - secures entire connection.....	15
7. Extensible - supports many attributes via schemas - /etc/openldap/schema: allows us to stretch schema	15
8. Data storage is independent of LDAP: default is DBM	15
9. Provides various tools: slap*(offline backend) - use when LDAP is NOT running	15
10. Provides various tools: ldap*(online daily admin).....	16
11. Separates binaries for: LDAP daemon (slapd) and replication (slurpd)	16
Chapter 2: LDAP Concepts	17
1. Distinguished Name (DN)	17
2. Object Class	19
3. Schemas - /etc/openldap/schema	19
4. Attributes - Fields.....	19
5. PAM - authenticates users on behalf of calling application - supports LDAP	19
6. Name Service Switch (NSS) - used by applications to find common Unix databases:	19
7. Both PAM & NSS work in conjunction to authenticate using LDAP (/etc/ldap.conf)	19
Chapter 3: Config of LDAP.....	21
1. Explore current auth environment	21
2. Setup LDAP Environment	21
###Key Online Management Utilities###	21
###Super-User Info###	22
###Search the DIT###	24
###LDAPSEARCH###	24
###LDAP BROWSER###	25
Chapter 4: DIT Creation	27
Task: Create a DIT	27
1. Create Root OU (Container) (DC) - using a pre-defined LDIF file - build_root_ou.ldif.....	27



2. Create organizational units: people, engineering, sales	27
Execution:.....	27
3. Create some users	28
Export Full Table Tree LDIF with jxplorer	30
Chapter 5: Replication	33
Requires:.....	33
Requirements:	33
1. OpenLDAP RPMs are installed - openldap*, nss_ldap*(includes PAM support)	33
Steps to replication (regardless of distribution):.....	33
1. Stop master LDAP server /etc/init.d/ldap stop - takes offline	33
2. Export the contents of the primary(master server) (DIT) to an LDIF file	33
Execution:.....	33
Execution:.....	36
3. Update /etc/hosts on both machines.....	36
a. Master	36
Execution:.....	36
b. Slave	36
Execution:.....	36
4. Update slapd.conf on the master(primary) server support replication.....	36
#Replication	36
-- this is for redhat ,centos	37
-- this is for suse	37
Execution:.....	37
5. Install LDAP on Slave.....	37
Execution:.....	37
6. Copy and import DIT on slave server.....	38
Execution:.....	38
Execution:.....	39
Execution:.....	40
7. Update slapd.conf on the slave(secondary) server.....	41
8. start slapd(LDAP process) on the slave(secondary/replica) server.....	41
9. start slapd(LDAP process) on the master(primary) server	41
Execution:.....	41
10. Ensure that services are set to start when the system reboots.....	42
Chapter 6: Confirm LDAP records on Primary(Master)and Secondary (Slave) systems..	43
Task:.....	43
1. Use 'ldapsearch' to confirm the existence of records on both systems.....	43
Execution:.....	43
Execution:.....	44
Chapter 7: LDAP Add.....	47
LDAP Add Features:.....	47
1. Facilitates the addition of objects to the DIT	47
2. 'ldapadd' is a symlink to 'ldapmodify -a'.....	47
Execution:	47
3. Default invocation reads attributes from STDIN	47
Tasks:	47
1. Add user 'raja1' to remaining OUs	47
Execution:.....	47
#Add First User.....	47
#Add 2nd User	48



#Add 3rd User.....	48
#Add fourth User	49
Execution:.....	49
Execution:.....	52
2. Add users 'raja3,raja4,raja5' to the DIT, wholesale, via STDIN from slave server	58
Execution:.....	59
Execution:.....	62
3. Use LDAP Browser to view DIT and to make changes	66
Execution:.....	66
4. Add 5 users to 2 OUs (Engineering & Sales) via text file	67
5. Confirm results using:	67
Execution:.....	67
Chapter 8: LDAP Delete	83
LDAP Delete Features:.....	83
1. A means to remove DIT objects	83
Tasks:	83
1. Delete an object from the command line	83
Execution:.....	83
2. Delete objects wholesale from: ou=sales.dc=raja.dc=internal - via STDIN	84
Execution:.....	84
4. Delete remaining OUs and objects via file	84
Execution:.....	84
Chapter 9: LDAP Modify	85
LDAP Modify Features:.....	85
1. Functionality found in:	85
2. Manipulates objects in DIT	85
Tasks:	85
1. Rebuild the DIT - create top-level OUs and users/OUs	85
2. Modify Attributes.....	85
Execution:.....	85
3. Delete Items	86
Chapter 10: LDAP Search	87
LDAP Search Features:	87
1. Ability to search the DIT	87
2. Supports Boolean Operators: &(AND), (OR), !(NOT) - Using prefix notation	87
3. Supports Wildcards: *, +(internal operations).....	87
Usage:.....	87
1. ldapsearch [options] "(attribute filteroperator value)"	87
Filter Operators:	87
Value(s):.....	87
Tasks:.....	87
1. Search specifict OUs for information	87
Execution:.....	88
2. Search the DIT for Organizational Units (OUs)	90
Execution:.....	90
Execution:.....	91
Execution:.....	98
3. Use Boolean Operators.....	101
Execution:.....	104
Execution:.....	106



Execution:	107
Execution:	110
Chapter 11: Logging/Debugging	113
Features:	113
1. Logs using SysLog (defaults to: LOCAL4)	113
2. Includes ldap searches as well as starts/stops/etc.	113
Configuration:	113
Debugging in Red Hat openldap v2.3:	113
Table 5.1: Debugging Levels Level Description	113
Example:	114
loglevel -l	114
Default:	114
loglevel 256	114
Debugging in Suse openldap v2.3:	114
Task:	115
1. Setup Syslog logging	115
Execution:	115
Task:	126
1. Purposely misname a slapd.conf directive	126
Chapter 12: LDIF Format	127
Features:	127
1. Standard import/export format returned by LDAP tools (offline/online)	127
2. RFC-2849	127
3. Very similar to name/value pairs from programming/scripting environments	127
Tasks:	127
1. ldapsearch -dumps DIT to STDOUT	127
2. Add 'TestUser1' to the DIT	127
Chapter 13: Schema	129
Features:	129
1. The definition of fields that constitute an object	129
Execution:	129
Execution:	129
Execution:	130
2. 'UP name' means, the higher-level (parent) attribute 'name' governs 'st' attribute	131
3. LDAP objects support single-inheritances	131
Task:	131
1. Created LDAP user based on additional: core.schema attributes	131
Execution:	131
Chapter 14: Setup to use LDAP and Migrate to LDAP from /etc/*Files	133
Features:	133
1. Ability to take advantage of LDAP authentication	133
2. Ability to support both local (/etc/passwd) and distributed (LDAP) users	133
3. Facilitates the sharing of most /etc/* tabular databases (/etc/hosts/etc/group/etc/services/etc.)	133
4. Setup LDAP auth of users/groups	133
5. Ability to migrate users/records from flat files to LDAP	133
6. http://www.padl.com/OSS/MigrationTools.html (makers of: pam_ldap.so & nss_ldap.so)	133
Task:	134
0. Setup LDAP	134
Execution:	134



2. /etc/ldap.conf (LDAP client configuration).....	134
Execution:.....	134
3. /etc/pam.d/system-auth-ac.....	135
Execution:.....	135
2. Test LDAP connectivity using SSH from slave LDAP host.....	136
Execution:.....	136
Execution:.....	137
Create organizational units: Group.....	141
Results:.....	145
3. Create new LDAP user and authenticate to both hosts: linuxcent & linuxcent-slave.....	156
Execution:.....	156
Test from slave:.....	157
Execution:.....	157
Execution:.....	157
Further work:.....	160
1. Create local users on linuxcent and linuxcent-slave boxes.....	160
2. Migrate those users to LDAP.....	160
Chapter 15: Migrate Other Tables.....	161
Task:.....	161
1. Shared records via LDAP DIT.....	161
2. Migrate: /etc/hosts to LDAP DIT.....	161
3. Migrate: /etc/services.....	161
4. Migrate: /etc/protocols.....	161
Chapter 16: Rebuild of DIT.....	163
Tasks:.....	163
1. Purge existing DIT using 'ldapdelete'.....	163
Execution:.....	163
2. Rebuild OUs (people & group).....	163
Execution:.....	163
Chapter 17: Account Maintenance.....	173
Task:.....	173
1. Create a user named 'bagher' derived from LDIF output.....	173
Execution:.....	173
2. Create a group named 'bagher' derived from LDIF output.....	174
Execution:.....	174
3. Create a directory: /home/bagher - for members of the LDAP group: 'bagher'.....	175
Execution:.....	175
4. Confirm user: bagher is unable to write to: /home/bagher.....	175
5. Use: 'ldpasswd' to assign a password to the user: 'bagher'.....	175
Execution:.....	175
6. Add user: 'bagher' to group: 'bagher'.....	176
Execution:.....	176
7. Change users' passwords:.....	176
8. Change Relative Distinguished Name (RDN) of an object.....	176
Chapter 18: Replication with SyncRepl.....	177
Features:.....	177
1. More efficient and reliable than SLUPD-based replication.....	177
2. Implemented as a slapd thread.....	177
3. Push/Pulls are supported:.....	177
4. Provider (Master) & Consumers(clients) relationship.....	177



5. Also supports cascading configurations: Provider -> Secondary Provider(s) -> Consumer(s) ...	177
6. Configuration is defined primarily on 'consumer' servers, NOT the provider	177
7. Specific queries (searches) can be replicated, including specific attributes	177
8. SyncRepl is search-based - searches define what gets replicated - search criteria is identical to that of: 'ldapsearch'	177
9. Uses built-in LDAP Content Sync protocol	177
10. Replication is incremental	177
Tasks:	178
1. Configure SyncRepl	178
Execution:	178
Execution:	178
Execution:	179
Execution:	182
2. Create new object on provider	184
3. Replicate SyncRepl configuration on Another client	184
4. Provider Configuration - update provider (master) in the DB section of: slapd.conf ..	184
Chapter 19: ACLs with OpenLDAP	185
Features:	185
1. General and granular restrictions	185
2. First match wins (top-down)	185
3. Implicit: 'by * none' at the end of ACLs which denies access	185
4. ACLs are stored in: slapd.conf	185
Template:	185
Task:	185
1. Examine the Default ACL	185
Execution:	185
I) non authenticated user or anonymous	186
II) Authenticated user: rootDN:	187
III) Authenticated user bagher:	187
3. Allow 'anonymous' access to 'hosts' OU and nothing else	189
4. Restrict access on an attribute level	189
Execution:	189
Chapter 20: OpenLDAP with SSL/TLS Encryption	193
Features:	193
1. Encrypted communications (default LDAP communications is sent via clear-text) ..	193
2. SSL binds, by default, to TCP:636 - i.e. URI: ldaps://hostname	193
3. TLS uses the default TCP:389 (StartTLS) - i.e. URI: ldap://hostname	193
Tasks:	193
1. Launch an 'wireshark' session in conjunction with 'tcpdump'	193
Execution:	193
2. Enable SSL/TLS Encryption on the primary server	195
Execution:	195
Execution:	196
Execution:	197
Execution:	197
Execution:	197
Execution:	199
Execution on not configured server for tls:	200