

Inhaltsverzeichnis

I	LDAP verstehen	1
1	Einführung in LDAP	3
2	Verzeichnisdienste	5
2.1	Von X.500 zu LDAP	8
2.2	LDAP v3	13
2.3	LDAP in der Netzwerkadministration	14
3	Das X.500-Datenmodell	17
3.1	Objekte	18
3.2	Attribute	19
3.3	Verzeichniseinträge	20
3.4	Vererbung	20
3.5	Klassenzugehörigkeit und Polymorphie	21
3.6	Standardisierung von Attributen und Objektklassen	21
3.7	Typen von Objektklassen: structural, auxiliary und abstract..	23
3.8	Der Verzeichnisbaum	24
3.9	Aliase	25
3.10	Distinguished Name und Relative Distinguished Name	25
3.11	»Relative« Namen	26
3.11.1	Zusammengesetzter RDN	27
3.11.2	Vom RDN zum DN	28
3.11.3	Kodierung von RDN	29
4	Das funktionale Modell	31
4.1	Die LDAP-Session	31
4.2	Messages und Operationen	31
4.3	Controls und Extended Operations	33
5	Partitionierung	35
5.1	Naming Context	35
5.2	Referrals und Continuations	37
5.3	LDAP-Proxying: Serverseitige Auflösung von Referrals	38

6	LDAP-URL und Search Filters	41
6.1	Beispiele für LDAP-URLs	43
6.2	Sonderzeichen in URLs	43
6.3	Suche im Verzeichnis	44
7	Sicherheit	51
7.1	Autorisierung und Authentifizierung	52
7.2	Zugriffskontrolle im LDAP	53
7.3	Authentifizierung	54
7.3.1	SASL	55
7.3.2	Der Strong Bind	56
7.4	Transport Layer Security	56
8	Schema	59
8.1	Schema Discovery	61
8.2	Allgemeiner Aufbau eines Schemas	61
8.3	Eigene Schemas entwerfen	62
8.3.1	Referenzierung von Objekten durch Name oder OID .	62
8.3.2	Der Object Identifier (OID)	63
8.3.3	Der eigene OID	66
8.3.4	AttributeTypes definieren	66
8.3.5	Object Classes definieren	70
8.3.6	Spezielle Attribute für den Serverbetrieb	71
9	Das LDIF-Format	73
II OpenLDAP einsetzen		77
10	Was ist OpenLDAP?	79
11	OpenLDAP installieren und konfigurieren	81
11.1	OpenLDAP installieren	81
11.1.1	Die Kompilation	83
11.1.2	Die Overlays	87
11.1.3	Die unterschiedlichen Backends	89
11.1.4	Die Konfiguration	91
11.2	Überlegungen zur Struktur des Verzeichnisbaumes	93
11.3	Eine Basiskonfiguration	94
11.3.1	Was bewirkt die Indexkonfiguration?	96
11.3.2	Das Backend cn=config	97
11.3.3	Einrichten der Database	99
11.4	Die Serverfunktionen und -operationen	102
11.4.1	Die Client-Tools	102

11.4.2	Simple Paged Results Control	103
11.4.3	Dynamic Directory Services extended Operation	104
11.4.4	Proxy-Autorisierung-Control	105
11.4.5	All Operational Attributes extended Operation	106
12	Methoden der Authentifizierung und Autorisierung	109
12.1	Cyrus-SASL	109
12.1.1	Cyrus-SASL kompilieren	111
12.1.2	Verwendung der SASL-Mechanismen	111
12.2	Verwendung von EXTERNAL-Mechanismen	113
13	Die Log-Backends	115
13.1	Accesslog	115
13.2	Auditlog	117
14	Aspekte der Zugriffs- und Transportsicherheit	119
14.1	Schutz vor unberechtigten Zugriffen	119
14.2	Berechtigungskontrolle durch ACL	120
14.2.1	Regeln für die <i>Was</i> -Funktion	121
14.2.2	Regeln für die <i>Wer</i> -Funktion	124
14.2.3	Regeln für den Security Strength Factor	126
14.2.4	Die zu vergebenden Rechte	126
14.2.5	Anwendungsbeispiele für diverse Regelsätze	127
14.3	Regelsätze mittels <i>Sets</i> definieren	130
14.4	Berechtigungskontrolle durch ACL	132
14.5	Zugangskontrolle durch TCP-Wrapper	135
14.6	Berechtigungskontrolle durch Overlays	135
14.7	Transportsicherheit	136
14.7.1	X.509-Zertifikate erstellen	137
14.7.2	OpenLDAP mit TLS-Optionen konfigurieren	142
15	Verteilte Systeme	147
15.1	Verweise auf andere Einträge	147
15.2	Verweise auf andere Server	149
15.3	Einbinden mehrerer Datenbasen	150
15.4	Replikation von gesamten Verzeichnissen und Teilbäumen ..	152
15.4.1	Replikation durch slurpd	153
15.5	Replikation durch Synchronisation	155
15.5.1	Synchronisierte Replikation einrichten	156
15.6	Proxy, Meta- und Virtual Server	161
15.6.1	LDAP Backend	162
15.6.2	Meta Backend	166
15.6.3	SQL Backend	167
15.6.4	Directory mit subordinate SQL Backend	168

16	Authentifizierung mittels PAM	171
16.1	PAM testen	173
17	Lösungsansätze mit Overlays	175
17.1	Dynamische Einträge erstellen, darstellen und verwalten	175
17.2	Konsolidierte Attributdarstellung	178
17.3	Passwort-Regeln und Kontrolle	180
18	Die Administration	183
18.1	Die SLAPD-Tools	183
18.1.1	Die regelmäßige Datensicherung	183
18.1.2	Die Indexdatenbanken pflegen	184
18.2	Die BerkeleyDB-Werkzeuge	185
18.2.1	Alte Logdateien entfernen	185
18.2.2	Database reparieren	185
18.2.3	Ist die Cachegröße ausreichend?	186
18.2.4	Die Datei DB_CONFIG	186
18.3	Tools zur Administration eines Directory	187
18.3.1	web2ldap	187
18.3.2	JXplorer	188
19	Ausgewählte Anwendungen	189
19.1	Die zentrale Mailadministration	189
19.1.1	Sendmail	190
19.1.2	Postfix-Mailrouting mit LDAP	192
19.1.3	Mailrelaying mit SASL-Authentifizierung	195
19.2	Cyrus-Imap	198
19.3	OpenLDAP als Backend für BIND	199
III	Entwickeln mit LDAP	203
20	LDAP-APIs und SDKs	207
20.1	APIs und SDKs im Überblick	208
21	libldap	211
21.1	libldap-Clients konfigurieren	212
21.2	libldap-Code mit dem GCC kompilieren	213
21.3	Eine LDAP-Sitzung mit der libldap	214
21.4	Eine einfache libldap-Anwendung	215
21.5	Speicherbefreiung	224
21.6	Asynchrone Operationen und Timeouts	224
21.7	Listings	227

22	Perl und Net::LDAP	233
22.1	Net::LDAP	233
22.2	Installation von Net::LDAP	235
22.3	Eine LDAP-Sitzung mit Net::LDAP	236
22.4	Asynchrone Operationen und Callbacks	241
22.5	Timeout	243
23	Java und das JNDI	247
23.1	Das JNDI	248
	23.1.1 Namens- und Verzeichnisdienste	249
	23.1.2 JNDI-Dokumentation	249
23.2	Eine JNDI-Anwendung	250
	23.2.1 Contexts	250
	23.2.2 Der Initial Context	252
	23.2.3 Erzeugung des Context	253
	23.2.4 Bind	254
	23.2.5 LDAP-Suche	255
	23.2.6 Das Suchergebnis	256
	23.2.7 unbind	259
23.3	Listing	259
24	Die Directory Service Markup Language	263
24.1	LDIF oder DSML?	263
24.2	Darstellung von Verzeichnisdaten	265
24.3	DSMLv1: Statische Verzeichnisdaten in XML-Verpackung	269
	24.3.1 Verzeichnisdaten in DSMLv1	269
	24.3.2 Schemadaten in DSMLv1	271
24.4	DSML mit Net::LDAP erzeugen	273
	24.4.1 Ein Schema-Dokument in DSML	274
	24.4.2 Ein Suchergebnis nach DSML wandeln	275
24.5	DSMLv2: Requests und Responses in XML-Verpackung	276
Anhang		279
A	Beispiel eines Schemas für Postfix	281
B	OIDs für extended Controls und extended Operations	282
C	UTF-8 und Base64	284
D	X.500-Standards erwerben	286
E	Häufig benutzte Matching-Rules	287
F	Syntaxen nach RFC 4517	289
G	TLS/SSL-Konfigurationen	291
H	Schema des Konfigurations-Backends	294

I	Auflistung der relevanten RFC und Drafts.....	303
J	Schema für ein kombiniertes Adressbuch.....	306
	Glossar	315
	Tabellenverzeichnis	322
	Abbildungsverzeichnis	323
	Literaturverzeichnis	325