Geleitwort ..... **XI**

Vorwort ..... **XIII**

1 Einleitung **1**

1.1 Formales 1

1.2 Schriftarten 1

1.2.1 Eingabe langer Befehle 2

1.2.2 Screenshots 2

1.2.3 Internetverweise 2

1.2.4 Icons 2

1.3 Linux-Distributionen 3

2 LDAP-Grundlagen **5**

2.1 Grundlagen zum Protokoll 5

2.1.1 Der Einsatz von LDAP im Netzwerk 7

2.1.2 Das LDAP-Datenmodell 7

2.1.3 Attribute 8

2.1.4 Objektklassen 9

2.1.5 Objekte 10

2.1.6 Schema 11

2.1.7 Das LDIF-Format 14

2.1.8 Aufbau einer Struktur 15

2.1.9 Namensfindung 17

3 Installation des ersten OpenLDAP **19**

3.1 Grundlegende Überlegungen 19

3.1.1 Die statische Konfiguration 19

3.1.2 Die dynamische Konfiguration 23

Bibliografische Informationen
http://d-nb.info/1207944386

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3.2 Installation unter Debian 24
3.3 Installation unter CentOS 30
3.3.1 Die dynamische Konfiguration 31
3.4 Einspielen der ersten Objekte 35
3.5 Erste Objekte 38

4 Einrichten von TLS 41
4.1 Einrichten von TLS unter Debian 42
4.2 Einrichtung von TLS unter CentOS 49
4.3 Überprüfung von TLS 55
4.4 TLS vs. LDAPS 57

5 Client-Anbindung mit sssd 59
5.1 Was bietet der sssd? 60
5.2 Installation und Konfiguration 60
5.3 Abfrage der Benutzer und Gruppen 65
5.4 Anmeldung am System 66

6 Grafische Werkzeuge 69
6.1 Webbasierte Werkzeuge 69
6.1.1 Installation und Einrichtung des LAM 70
6.2 Lokale Werkzeuge 74
6.2.1 Installation und Einrichtung des JXplorer 75
6.2.2 Installation und Einrichtung des Apache Directory Studio 78

7 Erste Schritte in der Objektverwaltung 81
7.1 Anlegen neuer Objekte 81
7.1.1 Anlegen von Organizational Units (OUs) 81
7.1.2 Anlegen von Benutzern und Gruppen 84
7.1.3 Ändern von Attributen 87

8 LDAP-Filter 91
8.1 Arten von Filtern 91
8.1.1 Beispiele zu einfachen Filtern 92
8.1.2 Beispiel zu erweiterten Filtern 95
8.2 Sonderzeichen in Attributen 96

9 Berechtigungen mit ACLs ... 99
9.1 Grundlegendes zu ACLs ... 99
9.1.1 Aufbau einer ACL ... 100
9.1.2 Die Berechtigungen ... 101
9.1.3 Die Privilegien ... 102
9.1.4 Arten der ACL-Verwaltung ... 106
9.1.4.1 Statische Konfiguration ... 106
9.1.4.2 Dynamische Konfiguration ... 107
9.1.5 ACL und grafische Werkzeuge ... 111
9.1.6 Rechte für den LDAP-Admin ... 116
9.2 ACLs in der Praxis ... 120
9.2.1 Rechte an der eigenen Abteilung ... 120
9.2.2 Rechte für Gruppen ... 123
9.2.3 Rechte für ein simpleSecurityObject ... 126
9.2.4 ACLs mit regulären Ausdrücken ... 127
9.2.5 Prüfen von ACLs ... 129

10 Erweiterte Funktionen durch Overlays ... 133
10.1 Datenaufbereitung ... 133
10.1.1 translucent ... 133
10.1.2 valsort ... 141
10.2 Datenmanipulation ... 144
10.2.1 dynlist ... 144
10.2.2 refint ... 148
10.2.3 memberOf ... 153
10.2.4 unique ... 157
10.2.5 constraint ... 159
10.2.6 dds ... 161
10.3 Zusatzfunktionen ... 167
10.3.1 Vorabbemerkungen zur Protokollierung ... 168
10.3.2 accesslog ... 169
10.3.3 auditlog ... 173
10.3.4 ppolicy ... 175
10.3.5 syncprov ... 179

11 Dynamische Posix-Gruppen ... 183
11.1 Anpassungen am OpenLDAP-Verzeichnis ... 184
11.1.1 Einrichten der dynamischen Posix-Gruppen ... 186
11.2 Anpassung des Clients ... 187
11.3 Fertig, aber (noch) nicht betriebsbereit ... 188

12 Replikation des OpenLDAP-Baums 189
12.1 Grundlagen zur Replikation 189
12.1.1 Change Sequence Number 189
12.1.2 Zeitsynchronisation 190
12.1.3 Serverrollen 194
12.1.4 Replikationsumfang 195
12.2 Replikationsmethoden 196
12.2.1 LDAP Synchronization Replication – Die vollständige Replikation 196
12.2.2 refreshOnly 197
12.2.3 refreshAndPersist 204
12.2.3.1 Einrichtung 205
12.2.4 Zwischenstopp 207
12.2.5 DeltaSync 208
12.2.5.1 Einrichtung 209
12.2.6 Zusammenfassung und Ergänzung 212
12.3 Schreiben auf dem Consumer 213
12.4 Replikationstopologien 215
12.4.1 Standby-Provider oder Mirror-Mode 215
12.4.2 Multi-Provider 220
12.4.3 Zusammenfassung und Ausblick 223
12.4.4 Troubleshooting mit CSN 224

13 OpenLDAP mit Kerberos 227
13.1 Funktionsweise von Kerberos 230
13.1.0.1 Einstufiges Kerberos-Verfahren 230
13.1.0.2 Zweistufiges Kerberos-Verfahren 230
13.2 Installation und Konfiguration des Kerberos-Servers 231
13.2.1 Konfiguration des ersten Kerberos-Servers 232
13.2.2 Initialisierung und Testen des Kerberos-Servers 237
13.2.3 Verwalten der Principals 239
13.3 Kerberos und PAM 243
13.3.0.1 PAM-Konfiguration unter CentOS 245
13.3.1 Testen der Anmeldung 245
13.4 Hosts und Dienste 246
13.4.1 Entfernen von Einträgen 251
13.5 Konfiguration des Kerberos-Clients 253
13.5.1 PAM und Kerberos auf dem Client 254
13.6 Replikation des Kerberos-Servers 255

13.6.1 Bekanntmachung aller KDCs im Netz ... 255
13.6.1.1 Bekanntmachung aller KDCs über die Datei krb5.conf ... 255
13.6.1.2 Bekanntmachung aller KDCs über SRV-Einträge im DNS ... 256
13.6.2 Konfiguration des KDC-Masters ... 258
13.6.3 Konfiguration des KDC-Slaves ... 259
13.6.4 Replikation des KDC-Masters auf den KDC-Slave ... 260
13.7 Kerberos Policies ... 262
13.8 Kerberos im LDAP einbinden ... 266
13.8.1 Vorbereitung des LDAP-Servers ... 267
13.8.2 Konfiguration des LDAP-Servers ... 269
13.8.3 Umstellung des Kerberos-Servers ... 273
13.8.4 Zurücksichern der alten Datenbank ... 278
13.8.5 Erstellung der Keys für den LDAP-Server ... 281
13.8.6 Bestehende LDAP-Benutzer um Kerberos-Principal erweitern ... 283
13.9 Neue Benutzer im LDAP ... 286
13.10 Authentifizierung am LDAP-Server über GSSAPI ... 288
13.10.1 Einrichtung der Authentifizierung unter Debian ... 288
13.10.2 Einrichten der Authentifizierung unter CentOS ... 293
13.10.3 Der sssd mit GSSAPI ... 293
13.10.4 Anbinden des zweiten KDCs an den LDAP ... 296
13.10.5 Replikation mit Kerberos absichern ... 296
13.10.6 Vorbereitung des zweiten LDAP-Servers ... 296
13.10.7 Einrichtung von k5start ... 298
13.10.8 Umstellung der Replikation auf GSSAPI ... 300
13.11 Übersicht über alle ACLs ... 301
13.12 Konfiguration des LAM-Pro ... 303
13.12.1 Vorbereitung des Webservers ... 304
13.12.2 Konfiguration des LAM ... 307

14 Monitoring mit Munin ... 311
14.1 Warum Monitoring? ... 311
14.2 cn=monitor ... 311
14.3 Munin ... 316
14.3.1 Munin-Server ... 317
14.3.2 Knoten ... 321
14.3.3 OpenLDAP-Daten ... 327
14.4 Andere Monitoring-Systeme ... 331

15 OpenLDAP im Container ... 333
15.1 Docker ... 333
15.1.1 Einrichtung des Docker-Servers ... 334
15.1.2 Der erste Container ... 334
15.2 OpenLDAP ... 338
15.2.1 Netzwerken ... 341
15.2.2 Datenpersistenz ... 345
15.2.3 Compose ... 347
15.2.4 Ausblick ... 350
15.3 Image im Eigenbau ... 351
15.3.1 Der Build-Prozess ... 351
15.3.2 Das Dockerfile ... 353
15.3.3 Testen des Images ... 355
15.3.4 Beispiel CentOS ... 355
15.3.5 Ausblick ... 358

16 Beispiele aus der Praxis ... 359
16.1 Weitere Datenbanken einrichten ... 359
16.1.1 Zweite Datenbank mit der statischen Konfiguration ... 360
16.1.2 Zweite Datenbank mit der dynamischen Konfiguration ... 361
16.1.3 Anlegen der ersten Objekte ... 362
16.2 Ssh mit Kerberos und LDAP ... 363
16.3 Der sssd und Gruppen ... 365
16.4 Public Keys im LDAP ... 366
16.4.0.1 Anpassen des ssh-Servers ... 370
16.5 LDAP-Authentifizierung für den Apache-Webserver ... 371
16.6 Attribute von Gruppenmitgliedern schneller finden ... 374
Stichwortverzeichnis ... 377

Stichwortverzeichnis ... 377