

OpenLDAP in der Praxis

Das Handbuch für Administratoren

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

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
1.4 Downloads zum Buch	4
1.5 OpenLDAP-Version	4
1.6 Konfigurationsarten	4
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	10
2.1.7 Umwandeln eines Schemas in ein LDIF	14
2.1.8 Das LDIF-Format	16
2.1.9 Aufbau einer Struktur	18
2.1.10 Namensfindung	19
3 Installation des ersten OpenLDAP	20
3.0.1 Die statische Konfiguration	20
3.0.2 Die dynamische Konfiguration	24
3.1 Installation der Symas-Pakete	24
3.1.1 Die Datei ldap.conf	33
3.1.2 Erste Änderungen an der Konfiguration	33
3.2 Einspielen der ersten Objekte	35

4	Einrichten von TLS	43
4.1	Erstellen der Zertifikate am Beispiel von Debian.....	44
4.2	TLS vs. LDAPS	51
5	Client-Anbindung mit sssd	52
5.1	Was bietet der sssd?.....	53
5.2	Installation und Konfiguration.....	53
5.3	Abfrage der Benutzer und Gruppen.....	58
5.3.1	SRV-Records im DNS	59
6	Erste Schritte in der Objektverwaltung	62
6.1	Anlegen neuer Objekte.....	62
6.1.1	Anlegen von Organizational Units (OUs)	62
6.1.2	Anlegen von Benutzern und Gruppen	66
6.2	Ändern von Attributen	69
6.3	Der neue Administrator.....	71
6.4	Änderungen direkt in der Datenbank.....	72
7	Grafische Werkzeuge	74
7.1	Webbasierte Werkzeuge.....	74
7.1.1	Installation und Einrichtung des LAM	75
7.2	Lokale grafische Werkzeuge	80
7.2.1	Installation und Einrichtung des Apache Directory Studio	80
8	LDAP-Filter	84
8.1	Arten von Filtern	84
8.1.1	Beispiele zu einfachen Filtern	85
8.1.2	Beispiel zu erweiterten Filtern	88
8.2	Sonderzeichen in Attributen	89
9	Berechtigungen mit ACLs	90
9.1	Grundlegendes zu ACLs.....	90
9.1.1	Aufbau einer ACL.....	91
9.1.2	Die Berechtigungen	92
9.1.3	Die Privilegien	94
9.1.4	Erste Schritte mit ACLs	97
9.1.4.1	Neue Position für eine ACL	101
9.1.4.2	Löschen von ACLs	102
9.1.4.3	ACLs mit Filtern	103
9.1.5	ACL und grafische Werkzeuge	104
9.1.6	Rechte für den LDAP-Admin	105
9.2	ACLs in der Praxis	108

9.2.1	Rechte an der eigenen Abteilung.....	108
9.2.2	Rechte für Gruppen	111
9.2.3	Rechte für ein simpleSecurityObject	113
9.2.4	ACLs mit regulären Ausdrücken.....	114
9.2.5	ACLs mit Filtern in der Praxis.....	115
9.2.6	Filtern aufgrund von Hostinformationen.....	116
9.2.7	ACLs auf Grund von ssf.....	117
9.2.8	ACLs mit set	120
	9.2.8.1 Alle ACLs	125
9.2.9	Prüfen von ACLs	127
10	Erweiterte Funktionen durch Overlays	129
10.1	Datenaufbereitung	129
10.1.1	translucent	129
10.1.2	valsort	136
10.1.3	deref.....	139
	10.1.3.1 Einrichtung von deref	139
	10.1.3.2 Verwenden von dereferenzierten Suchen	139
10.2	Datenmanipulation	140
10.2.1	memberOf.....	141
10.2.2	dynlist	144
	10.2.2.1 Dynamische Gruppen.....	147
10.2.3	refint	148
10.2.4	unique	153
10.2.5	constraint	155
10.2.6	dds.....	157
10.3	Zusatzfunktionen	163
10.3.1	Vorabbermerkungen zur Protokollierung.....	163
10.3.2	accesslog	164
10.3.3	auditlog.....	168
10.3.4	ppolicy	170
	10.3.4.1 Komplexere Kennwortrichtlinien.....	174
10.3.5	autoca.....	178
	10.3.5.1 Einrichtung von autoca	179
	10.3.5.2 Automatische Erzeugung von Schlüsselmaterial	180
10.3.6	homedir	182
	10.3.6.1 Einrichten des Overlays homedir	182
10.3.7	otp	183
	10.3.7.1 Serverseitige Einrichtung von otp	183
	10.3.7.2 Definition der Vorgaben für die OTP-Authentifizierung	183
	10.3.7.3 Einrichten von OTP für die Benutzer per Skript	185

10.3.7.4	Einrichten von OTP für die Benutzer über LAM SelfService	187
10.3.8	remoteauth.....	190
10.3.8.1	Einrichtung von remoteauth	190
10.3.9	syncprov	192
10.3.10	variant	194
10.3.10.1	Einrichten mit einfachen Werten	195
10.3.10.2	Einrichtung mit regex	196
11	Dynamische Posix-Gruppen.....	198
11.1	Anpassungen am OpenLDAP-Verzeichnis	199
11.1.1	Einrichten der dynamischen Posix-Gruppen	201
11.2	Anpassung des Clients	202
12	Replikation des OpenLDAP-Baums.....	204
12.1	Grundlagen zur Replikation	205
12.1.1	Change Sequence Number	205
12.1.2	Zeitsynchronisation	206
12.1.3	Serverrollen	210
12.1.4	Replikationsumfang	211
12.2	Replikationsmethoden.....	212
12.2.1	LDAP Synchronization Replication – Die vollständige Replikation	213
12.2.2	refreshOnly.....	213
12.2.3	refreshAndPersist	221
12.2.3.1	Einrichtung	222
12.2.4	Zwischenstopp	224
12.2.5	DeltaSync.....	224
12.2.5.1	Einrichtung	226
12.2.6	Zusammenfassung und Ergänzung.....	230
12.3	Schreiben auf dem Consumer	231
12.4	Replikationstopologien	232
12.4.1	Standby-Provider oder Mirror-Mode	233
12.4.2	Vorbereitung der Replikation	235
12.4.3	Einrichtung der Replikation cn=config	235
12.4.4	Einrichtung der Replikation der Objektdatenbank.....	238
12.5	Consumer mit eingeschränkter Replikation	243
12.5.1	Einschränkungen über ACLs einrichten	244
12.5.2	Einschränkungen über Filter einrichten	248
12.5.3	Überprüfung der Replikation mit slapd-watcher	249
12.5.4	Troubleshooting mit CSN	251

13	Loadbalancer mit lload	254
13.1	Übersicht über lload.....	254
13.1.1	Funktionsweise von lload	254
13.1.2	Voraussetzungen	255
13.2	Vorbereitungen für lload	255
13.2.1	Proxy-Authentifizierung.....	256
13.2.2	Erstellen des Proxy-Benutzers	256
13.2.3	Rechte für den Proxy-Benutzer	257
13.3	Einrichten des Loadbalancers	258
13.3.1	Modul	258
13.3.2	Backend	258
13.3.3	Tier	259
13.3.4	Schreiboperationen.....	261
14	OpenLDAP als Proxy	263
14.1	Einrichtung eines einfachen LDAP-Proxy	264
14.1.1	Einrichtung des LDAP-Proxy	264
14.1.1.1	Das Rewriting bestimmter Attribute	268
14.1.1.2	Das Caching bestimmter Suchanfragen	269
14.1.1.3	Testen des Caches.....	272
14.2	Einrichtung eines meta-Proxyservers	273
15	OpenLDAP mit Kerberos	278
15.1	Funktionsweise von Kerberos	281
15.1.1	Einstufiges Kerberos-Verfahren	281
15.1.2	Zweistufiges Kerberos-Verfahren	281
15.2	Installation und Konfiguration des Kerberos-Servers	282
15.2.1	Konfiguration des ersten Kerberos-Servers.....	283
15.2.2	Initialisierung und Testen des Kerberos-Servers.....	288
15.2.3	Verwalten der Principals	290
15.3	Kerberos und PAM	294
15.3.0.1	PAM-Konfiguration unter Redhat	295
15.3.1	Testen der Anmeldung	296
15.4	Hosts und Dienste	297
15.4.1	Entfernen von Einträgen	302
15.5	Konfiguration des Kerberos-Clients.....	302
15.5.1	PAM und Kerberos auf dem Client.....	304
15.6	Replikation des Kerberos-Servers	304
15.6.1	Bekanntmachung aller KDCs im Netz.....	305
15.6.1.1	Bekanntmachung aller KDCs über die Datei krb5.conf	305
15.6.1.2	Bekanntmachung aller KDCs über SRV-Einträge im DNS	306

15.6.2	Konfiguration des KDC-Masters	308
15.6.3	Konfiguration des KDC-Slaves	309
15.6.4	Replikation des KDC-Masters auf den KDC-Slave	309
15.7	Kerberos Policies	312
15.8	Kerberos im LDAP einbinden	315
15.8.1	Vorbereitung des LDAP-Servers	316
15.8.2	Konfiguration des LDAP-Servers	317
15.8.3	Umstellung des Kerberos-Servers.....	320
15.8.4	Zurücksichern der alten Datenbank.....	327
15.8.5	Erstellung der Keys für den LDAP-Server	329
15.8.6	Bestehende LDAP-Benutzer um Kerberos-Principal erweitern	331
15.9	Neue Benutzer im LDAP	334
15.10	Authentifizierung am LDAP-Server über GSSAPI	336
15.10.1	Einrichtung der Authentifizierung.....	336
15.10.2	Der sssd mit GSSAPI	339
15.10.3	Anbinden des zweiten KDCs an den LDAP	342
15.10.4	Replikation mit Kerberos absichern	342
15.10.5	Vorbereitung des zweiten LDAP-Servers	343
15.10.6	Einrichtung von k5start	344
15.10.7	Umstellung der Replikation auf GSSAPI	347
15.11	Konfiguration des LAM-Pro	348
15.11.1	Vorbereitung des Webservers.....	349
15.11.2	Konfiguration des LAM.....	352
16	Einrichtung von Referrals	357
16.0.1	Namensauflösung.....	358
16.0.2	Einrichtung	358
16.1	Einrichtung ohne Chaining	358
16.1.1	Konfiguration des Hauptnamensraums	359
16.1.2	Einrichten der untergeordneten Datenbank	361
16.1.3	Testen der Referrals	363
16.1.3.1	Was macht der sssd?	364
16.2	Einrichtung mit Chaining	364
16.2.1	Einrichtung der untergeordneten Datenbank	365
16.2.2	Konfiguration der Server	366
16.2.3	Erste Tests	367
16.2.4	Das Overlay chain	369
16.2.4.1	Auf dem Hauptnamensraum.....	370
16.2.5	Der sssd Zugriff.....	371
16.2.5.1	Im Hauptnamensraum.....	371

17	Monitoring mit Munin	374
17.1	Warum Monitoring?	374
17.2	cn=monitor	374
17.3	Munin	379
17.3.1	Munin-Server	379
17.3.2	Knoten	383
17.3.3	OpenLDAP-Daten	389
17.3.4	Überwachung des Loadbalancers	394
17.4	Andere Monitoring-Systeme	396
18	OpenLDAP im Container	397
18.1	Docker	397
18.1.1	Einrichtung des Docker-Servers	398
18.1.2	Der erste Container	398
18.2	OpenLDAP	402
18.2.1	Netzwerken	405
18.2.2	Datenpersistenz	408
18.2.3	Compose	410
18.2.4	Ausblick	414
18.3	Image im Eigenbau	414
18.3.1	Der Build-Prozess	414
18.3.2	Das Dockerfile	417
18.3.3	Testen des Images	421
18.3.4	Ausblick	422
18.4	Kubernetes	422
18.4.1	minikube	423
18.4.1.1	Einrichtung unter Debian	423
18.4.1.2	Die Kommandozeile	423
18.4.1.3	Das Dashboard	424
18.4.2	Registry	424
18.4.3	Namespace	425
18.4.4	Volume	425
18.4.5	Deployment	426
18.4.6	Ausblick	427
19	OpenLDAP einrichten mit Ansible	428
19.1	Rolle zur Vorbereitung	429
19.2	Die Rolle zur Einrichtung von OpenLDAP	431
19.2.1	Vorbereitung für TLS	432
19.2.2	Die Templates	433
19.2.2.1	provider_main_config.j2	433
19.2.2.2	first-objects.j2	435
19.2.2.3	main_db_repl.j2	435
19.2.2.4	repl_config.j2	437
19.2.2.5	symas-openldap-default.j2	438
19.2.3	Die Tasks	438
19.2.4	Einspielen der Rolle	447

20	Beispiele aus der Praxis	449
20.1	Weitere Datenbanken einrichten	449
20.1.1	Zweite Datenbank einrichten	450
20.1.2	Anlegen der ersten Objekte	451
20.2	Ssh mit Kerberos und LDAP	452
20.3	Der sssd und Gruppen	453
20.4	Public Keys im LDAP	454
20.4.0.1	Anpassen des ssh-Servers	457
20.5	LDAP-Authentifizierung für den Apache-Webserver	459
	Stichwortverzeichnis	463