

OpenLDAP - Praxiseinsatz im Netzwerk

Seminarunterlage

Version: 11.06



Dieses Dokument wird durch die ORDIX AG veröffentlicht.

Copyright ORDIX AG. Alle Rechte vorbehalten.

Alle Produkt- und Dienstleistungs-Bezeichnungen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen und beziehen sich auf Eintragungen in den USA oder USA-Warenzeichen.

Weitere Logos und Produkt- oder Handelsnamen sind eingetragene Warenzeichen oder Warenzeichen der jeweiligen Unternehmen.

Kein Teil dieser Dokumentation darf ohne vorherige schriftliche Genehmigung der ORDIX AG weitergegeben oder benutzt werden.

Adressen der ORDIX AG

Die ORDIX AG besitzt folgende Geschäftsstellen

ORDIX AG
Westernmauer 12-16
D-33098 Paderborn
Tel.: (+49) 0 52 51 / 10 63 - 0
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
An der alten Ziegelei 5
D-48157 Münster
Tel.: (+49) 02 51 / 9 24 35 – 00
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Marlene-Dietrich-Str. 5
D-89231 Neu-Ulm
Tel.: (+49) 07 31 / 9 85 88 – 550
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Kreuzberger Ring 13
D-65205 Wiesbaden
Tel.: (+49) 06 11 / 7 78 40 – 00
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Wikingerstraße 18-20
D-51107 Köln
Tel.: (+49) 02 21 / 8 70 61 – 0
Fax.: (+49) 01 80 / 1 67 34 90

Sie können die ORDIX AG von der ganzen Welt aus durch folgende Internet Adresse kontaktieren:
<http://www.ordix.de>

Sie können uns weiterhin über die Email-Adressen training@ordix.de oder info@ordix.de kontaktieren

Inhaltsverzeichnis

1	Grundbegriffe und Protokolle LDAP und X.500	6
1.1	Was ist ein Verzeichnisdienst?	7
1.1.1	Motivation Verzeichnisdienste	9
1.1.2	Was kann gespeichert werden?	10
1.2	Geschichte von LDAP	11
1.3	Warum LDAP einsetzen?	12
1.4	Directory Information Tree (DIT)	13
1.5	Aufbau von Verzeichnisdiensten	14
1.6	Wer spricht LDAP?	15
1.7	Verschiedene Verzeichnisdienste	16
1.8	Proprietäre Lösung Active Directory	18
1.9	Was ist LDAP?	19
1.10	Was ist OpenLDAP?	20
1.11	LDAP-Modelle	21
1.12	LDAP Server (technische Daten)	22
1.13	Protokolle	23
1.14	RFCs	24
1.15	Vorteile von LDAP	25
1.16	Nachteile von OpenLDAP	26
1.17	Single Sign-On	27
1.18	LDAP vs. Datenbanken	28
2	Aufbau und Komponenten eines Verzeichnisdienstes	29
2.1	Distinguished Name	30
2.2	Datentypen im LDAP	32
2.3	OpenLDAP Schema	33
2.4	LDAP Komponenten	34
2.4.1	Attribute	35
2.4.2	Objektklassen	36
2.4.3	Objekte	37
2.4.4	Objekte, Attribute und Regeln	38
2.4.5	Vererbung von Attributen	39
2.5	LDAP Directory Interchange Format	40
3	Installation und Konfiguration von LDAP	41
3.1	Installation aus dem Quellcode	42
3.2	Installation mit RPM Paketen	43
3.3	Konfiguration des LDAP-Servers	44
3.4	Die Konfigurationsdatei slapd.conf	45
3.5	Backend-Konfiguration	46
3.6	Authentifizierung	48
3.7	Start des LDAP-Server	49
3.8	Konfiguration der Protokollierung	50
3.9	http://www.openldap.org	51
4	LDIF Format und Befehle	52
4.1	LDAP Data Interchange Format (LDIF)	53
4.2	Häufig genutzte LDAP Objekte	57
4.2.1	Benutzerverwaltung mit LDAP	58
4.2.2	Anlegen der LDAP Struktur	59
4.2.3	Anlegen von LDAP Objekten	61
4.3	Kommandos zur LDIF Verwaltung	63
4.4	LDAP Funktionsmodell	64
4.5	Kommunikations- und Funktionsmodell	65
4.5.1	Angabe der Suchebene	66
4.5.2	Verknüpfen von Suchfiltern	68

4.5.3	Verwendung von Suchfiltern	69
4.5.4	LDAP Clientkonfiguration	70
4.5.5	LDIF Befehle: ldapadd	71
4.5.6	LDIF Befehle: ldapdelete	72
4.5.7	LDIF Befehle: ldapmodify	73
4.5.8	LDIF Befehle: ldap*	75
4.6	Grafische Verwaltungstools	76
4.6.1	LDAP Browser - Der Klassiker	77
4.6.2	JXplorer	78
4.6.3	phpldapadmin - Das Webbasierte	79
4.6.4	Ldapadmin - Das Windowsbasierte	80
4.6.5	Apache Directory Studio	81
4.6.6	ldapvi	82
5	LDAP erweitern mit Overlays	83
5.1	OpenLDAP Overlays	84
5.2	Overlays im Überblick	86
5.3	Overlays am Beispiel „accesslog“	87
5.4	Overlays am Beispiel „auditlog“	88
5.5	Overlays am Beispiel „valsort“	89
6	Authentifizierung und Clientanbindung	90
6.1	Authentifizierungsdienst	91
6.1.1	Authentifizierung am LDAP-Server	97
6.1.2	Architektur der Benutzerauthentifizierung	98
6.2	PAM konfigurieren	99
6.2.1	PAM Modul-Typen	100
6.2.2	PAM Kontroll-Flag	101
6.2.3	PAM Modul-Pfad	102
6.3	Authentifizierung über LDAP mit pam_ldap	103
6.3.1	Aufbau /etc/nsswitch.conf	104
6.4	Benutzerverwaltung mit nss_ldap	105
6.5	Automatisches Erstellen des Homeverzeichnisses	106
6.6	Autorisierung mit Hilfe von Netgroups	107
6.7	Autorisierung mit Hilfe von Netgroups – LDIF	108
6.8	Autorisierung mit Hilfe von Netgroups – Clientkonfiguration	109
6.9	Nameservice Cache Daemon	110
6.10	Pufferung von Informationen: nscd	111
6.11	Beispiele	112
7	Replikation	113
7.1	Gründe für die Replikation	114
7.2	Replikationsmöglichkeiten	115
7.3	syncrepl ab Version 2.3	116
7.4	Konfiguration des Provider	118
7.5	Konfiguration des Consumer	119
7.6	Der beschreibbare „Consumer“	120
7.7	N-Way Multi-Master	121
7.8	Multi-Master „master1“	123
7.9	Multi-Master „master2“	124
8	Schemaverwaltung	125
8.1	Das Schema von OpenLDAP	126
8.2	Was ist eine OID?	127
8.3	Wichtige Schemadateien	128
8.4	Typen von Objektklassen	129
8.5	Aufbau der Schemadefinitionen	130
8.6	Schemaerweiterung	131
8.7	Definition von Attributen	132

8.8	Definition von Objekten.....	133
8.9	Schema Attribut-Syntaxe	134
8.10	Schema Matching Rules	135
8.10.1	Beispiel für eigenes Schema	136
8.11	Schema Hardwareinventarisierung.....	137
8.11.1	Hardwareinventarisierung – LDIF	139
8.11.2	Hardwareinventarisierung – Skript.....	140
9	Verwaltung der LDAP Datenbank.....	141
9.1	Gründe für lange Antwortzeiten	142
9.2	BDB - Berkeley Datenbank.....	143
9.3	BDB Datenbankdateien	144
9.4	Datenbank Verwaltungstools	145
9.5	Datenbank Statistiken	146
9.6	BDB-Datenbanken	147
9.7	Dump und Restore (offline).....	148
9.8	Indizes.....	149
9.9	Die Indexdirektive	150
9.10	Limits.....	151
9.10.1	Benutzerspezifische Limits	152
10	Sicherheit und Verschlüsselung	153
10.1	Zugriffskontrolle beim LDAP-Server	154
10.2	Zugriffsschutz.....	155
10.3	Mögliche Zugriffsrechte.....	156
10.4	Beispiel einer ACL	157
10.5	Benutzer mit Replikationsrechten	158
10.6	SSL Verschlüsselung.....	159
10.7	SSL Verschlüsselung in slapd.conf	161
10.8	Nutzung der LDAP Befehle mit TLS	162
10.9	Authentifizierung mit TLS.....	163
10.10	Alleinige Nutzung von TLS	164
10.11	Replikation mit SSL Verschlüsselung	165
10.12	Authentifizierung mit SSL Verschlüsselung	166
11	Anbindung von Anwendungen	167
11.1	Übersicht.....	168
11.2	Anbindung von Samba.....	169
11.3	Anbindung von Apache.....	172
11.4	Anbindung des Automounter	174
11.5	Anbindung von sudo	176
12	Administration zur Laufzeit.....	179
12.1	Onlinekonfiguration	180
12.2	Konfigurationslayout	181
12.3	Konfiguration von cn=config	182
12.4	Onlineadministration von cn=config.....	183