

Single Sign on mit Oracle

Seminarunterlagen

Version: 1.05



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
Karl-Schurz-Straße 19a
D-33100 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
Welser Straße 9
D-86368 Gersthofen
Tel.: (+49) 08 21 / 507 492 – 0
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

Internet: <http://www.ordix.de>

Email: seminare@ordix.de

Inhaltsverzeichnis

1	Konzepte und Architektur	8
1.1	Motivation Enterprise User Security.....	9
1.2	Oracle Fusion Middleware	12
1.3	Oracle Identity Management.....	14
1.4	Vergleich OID, OVD und OUD.....	17
1.5	Gesamtkonzept.....	20
1.6	Ziele.....	22
2	Authentifizierung.....	23
2.1	Authentisierung	24
2.2	Authentifizierung	25
2.3	Single Sign-On.....	26
2.4	Zentralisierung der Benutzerdaten.....	27
2.5	Herausforderungen	28
2.6	Accounttypen	29
2.7	Administrative Accounts.....	30
2.8	Nicht Administrative Accounts.....	32
2.9	Authentifizierungsmöglichkeiten	34
2.9.1	Schwache Authentifizierung.....	35
2.9.1.1	Vor-/Nachteile.....	36
2.9.2	Externe Authentifizierung.....	37
2.9.2.1	Vor-/Nachteile.....	38
2.9.3	Authentifizierung via Proxy User.....	39
2.9.3.1	Vor-/Nachteile.....	40
2.9.4	External Password Store.....	41
2.9.4.1	Anpassungen.....	42
2.9.4.2	Vor-/Nachteile.....	43
2.9.5	Authentifizierung über SSL	44
2.9.5.1	Konfiguration	46
2.9.5.2	Vor-/Nachteile.....	48
2.9.6	Kerberos.....	49
2.9.7	Globale Authentifizierung (LDAP)	50
2.10	Kombinationen	51
3	Directory Server	52
3.1	Verzeichnisdienste	53
3.2	Anwendungsbeispiele	54
3.3	Kommunikation Client Server.....	55
3.4	Baumstruktur in LDAP.....	56
3.5	Identifikation von Einträgen.....	57
3.5.1	Informationsmodell.....	58
3.6	Objekte, Attribute und Regeln.....	59
3.7	LDAP Data Interchange Format.....	60
3.7.1	LDIF Syntax.....	61
3.8	Authentifizierungsmechanismen	62
3.8.1	LDAP Funktionsmodell.....	63
3.8.2	LDAP Verbindung.....	64
3.8.3	Partitionierung	65
3.9	LDAP Kommandos.....	66
3.9.1	Suche im LDAP Baum.....	67
3.10	Replikation	68
3.11	Abkürzungen	69
4	Oracle Unified Directory (OUD).....	70
4.1	Einführung.....	71
4.2	Vergleich OUD und OID.....	72
4.3	Architektur	73
4.4	Betriebsarten.....	74

4.4.1	Directory Storage und Replication Server.....	74
4.4.2	Proxy	75
4.4.3	Replication Gateway und Verwaltung	76
4.5	Warum Oracle Unified Directory	77
4.6	Voraussetzungen	78
4.6.1	Hardware.....	78
4.6.2	Repository Datenbank.....	79
4.6.3	Betriebssystem.....	80
4.6.4	Kompatibilität.....	81
4.7	Installation	82
4.7.1	Installationsdateien.....	82
4.7.2	Umgebungsvariablen	83
4.8	Fusion Middleware Infrastructure.....	84
4.8.1	Installation	84
4.8.2	Fusion Middleware Control (Enterprise Manager)	85
4.8.3	Weblogic Server Administrations Console	86
4.8.4	OID Installationsoptionen	87
4.8.5	Installation mit GUI.....	88
4.8.6	Installation mit Kommandozeile/Skript	90
4.8.7	Installation mit Weblogic Skripting Tool	94
4.9	OID Instanz.....	96
4.9.1	Verzeichnisstruktur.....	96
4.9.2	Stoppen und Starten	97
4.9.3	Konfiguration mit dsconfig.....	102
4.9.4	Anmeldeinformationen in einem Properties File definieren	105
4.9.5	dsconfig – Remote Anmeldung.....	106
4.9.6	Konfiguration Oracle Directory Service Manager (ODSM)	111
4.10	Oracle Net Konfiguration.....	112
sqlnet.ora.....		112
4.11	Monitoring.....	114
4.11.1	Ziel.....	114
4.11.2	Komponenten	115
4.11.3	Provider	116
4.11.4	Log Publisher	117
4.11.5	Log Dateien	119
4.11.6	Log Formate	120
4.11.7	Log Retention Policy	121
4.12	Backup und Recovery	122
4.12.1	Übersicht	122
4.12.2	Backup Tool	123
4.12.3	Backup Aufruf.....	124
4.12.4	Backup Directory	125
4.12.5	Backup Information	126
4.12.6	Sicherung der Datei config.ldif	127
4.12.7	Disaster Recovery Backup.....	128
4.12.8	Restore Tool.....	129
4.12.9	Restore Aufruf	130
5	Enterprise User Security (EUS).....	131
5.1	Agenda EUS	132
5.2	Definition Enterprise User Security	133
5.3	Grundlagen – Oracle User Authentifizierung	134
5.4	Grundlagen – Enterprise User Security (EUS)	135
5.5	Struktur planen.....	137
5.6	Vorbereitung des Oracle Unified Directory	140
5.6.1	Container für Gruppen und Benutzer hinzufügen	141
5.6.2	Admin Benutzer zur Datenbank-Registrierung anlegen.....	142
5.6.3	Rechtevergabe an Admin User	143
5.6.4	Default Suche auf cn=Users, cn=Groups.....	144
5.7	Oracle Datenbanken registrieren	145

5.7.1	Kommunikationsweg einrichten	146
5.7.2	Datenbank registrieren - GUI	148
5.7.3	Datenbank registrieren – CLI	149
5.7.4	Datenbank-Eintrag im Verzeichnisbaum.....	150
5.7.5	Datenbank – Domain Zuordnung.....	151
5.7.6	Information anzeigen.....	153
5.8	Anpassungen in der Oracle Datenbank.....	154
5.8.1	Anlegen von Globalen Rollen.....	155
5.8.2	Globale Rollen einer Datenbank anzeigen	156
5.8.3	Global User als Exclusive Schema User.....	157
5.8.4	Beispiel Exclusive Schema	158
5.8.5	Globaler Benutzer als Shared Schema.....	159
5.8.6	Globaler Benutzer als Enterprise Proxy User	160
5.9	Anpassung im Oracle Unified Directory	161
5.9.1	Enterprise User einem Global User zuordnen	161
5.9.2	Anmeldung als Enterprise User testen.....	162
5.9.3	Enterprise Domain.....	163
5.9.4	Enterprise Domain anlegen.....	164
5.9.5	Enterprise Domain auflisten	165
5.9.6	Informationen zu einer Enterprise Domain anzeigen.....	166
5.9.7	Enterprise Rollen.....	167
5.9.8	Enterprise Rollen auflisten	168
5.9.9	Enterprise Rolle im Verzeichnisbaum	169
5.9.10	Enterprise Rollen – globale Rolle.....	170
5.9.11	Enterprise Rolle – Benutzer	171
5.9.12	Zuweisung einer Enterprise Rolle kontrollieren	172
5.9.13	Information zur Enterprise Rolle anzeigen.....	173
5.9.14	Verbindung testen	174
5.10	Sicherheit	175
6	Directory Integration Platform (DIP).....	177
6.1	DIP Übersicht	178
6.1.1	Integration	179
6.2	Architektur	180
6.3	DIP in der EUS Gesamt Konfiguration	182
6.4	Überblick der Komponenten.....	183
6.4.1	Konnektoren	184
6.4.2	Synchronisierung Profile	185
6.4.3	Security	186
6.5	Konfiguration OUD mit DIP	187
6.5.1	dipConfigurator.....	188
6.5.2	manageDIPServerConfig	189
6.5.3	manageSyncProfiles	190
6.6	DIP Web Konsole.....	192
6.6.1	DIP Konsole Übersicht	193
6.6.2	DIP Backend Konfiguration	194
6.6.3	Synchronisierungsprofile.....	196
6.6.3.1	Synchronisierungsprofile Konfiguration.....	197
6.6.3.2	Zuordnungsliste.....	198
6.6.3.3	Domain Zuordnung.....	199
6.6.3.4	Domain Exklusion Liste	200
6.6.3.5	Attribut Mapping	201
6.6.3.6	Erweitertes Mapping und Plugins.....	204
6.6.3.7	Objekt Filter	206
6.6.3.8	Parameter Konfiguration	207
6.6.3.9	Parameter Übersicht	208
6.6.3.10	Profile in Textform	209
6.6.4	DIP Initiales Laden der Daten	210
6.6.5	DIP Tester	211
6.6.5.1	Testausgabe.....	212

6.6.6	Log Konfiguration	213
6.6.7	Performance.....	215
6.7	Synchronisierungsprofil in Textform.....	216
7	DIP Praxisbeispiele	218
7.1	DIP Active Directory Synchronisierung	219
7.1.1	Übersicht AD LDS	219
7.1.2	Domänen Übersicht.....	220
7.1.3	Objekte Filtern	221
7.1.4	AD Papierkorb	223
7.1.5	Mengengerüst der Synchronisierung	224
7.1.6	Objekte und Attribute im AD.....	225
7.1.7	Testzugriff.....	226
7.1.8	Authentifizierung Methoden	228
7.1.9	Password on Demand.....	229
7.1.10	Password Mapping.....	230
7.1.11	Nickname Mapping.....	231
7.1.12	EUS User und Gruppen im AD	233
7.1.13	EUS User und Gruppen im OUD	234
7.2	DIP OpenLdap -Synchronisierung	235
7.2.1	OpenLdap Verbindung	235
7.2.2	OpenLdap Übersicht	236
7.2.3	DIP Profile erstellen.....	237
7.2.3.1	Attribute Anpassen	238
7.2.3.2	DIP Übersicht	239
7.2.4	syncProfileBootstrap	240
7.2.4.1	Ergebnis der Synchronisierung	241
8	Kerberos.....	242
8.1	Allgemeines.....	243
8.1.1	Die Anwendersicht	244
8.1.2	Die Lösung: SSO.....	245
8.1.3	Die Administratorensicht	246
8.1.4	Was ist Kerberos?	247
8.1.4.1	Wer nutzt Kerberos?	248
8.1.4.2	Kerberos Komponenten	249
8.1.4.3	Definitionen – Ticket.....	250
8.1.4.4	Definitionen – Session Key	251
8.1.5	Der Ablauf	252
8.1.6	Der schematische Ablauf	253
8.1.7	Vorbereitungen auf dem Kerberos-Server	259
8.1.8	Vorbereitung der Datenbank	261
8.1.9	Mit der Datenbank verbinden	262
8.1.10	Fazit.....	263
9	Hochverfügbarkeit.....	264
9.1	Hochverfügbarkeit	265
9.2	EUS Konfiguration als Hochverfügbarkeitslösung	266
9.3	Replikation	267
9.4	Load Balancing	269
10	Lizenzen / Fazit	270
10.1	Allgemeine Kostenstrukturen	271
10.2	Vorteile und Ersparnisse	272
10.3	Oracle Komponenten	273
10.4	Lizenzierung.....	274
10.4.1	Produktlizenzierung.....	274
10.4.2	Ergänzungen	275
10.4.3	Lizenzkosten	276
10.5	Support.....	277

10.6	My Oracle Support	278
10.7	Vergleich Authentifizierungsmöglichkeiten	279
10.8	Fazit.....	280
11	Centrally Managed User	281
11.1	Allgemeines zu Centrally Managed User.....	282
11.2	Übersichtsbild.....	283
11.3	Vorbereitung des Active Directory	284
11.4	Erweiterungen im Active Directory	285
11.5	Passwort Verifier	286
11.6	Arbeiten auf dem Datenbankserver	287
11.7	Konfigurationsdateien ldap.ora und dsi.ora	288
11.8	Suchreihenfolge der Konfigurationsdateien	289
11.9	Wallet File.....	290
11.10	Verwendung der Datei ldap.ora	291
11.11	Verwendung der Datei dsi.ora	292
11.12	Globale User	294
11.13	SQL Syntax für globale Benutzer und Rollen	295
11.14	Anmelde Syntax	296
11.15	Identitätsprüfung in der Datenbank.....	297
11.16	Kerberos und PKI.....	298
11.17	Fehlersuche	299
11.18	Dokumentation	300
11.19	Fazit.....	301