ORACLE ENTERPRISE MANAGER 12c

ORACLE

Mandantentrennung von der Anwendung bis zum Storage

Weblogic Server und OLS

Ulf Lämmerhirt

Oracle Deutschland B.V. & Co. KG

Warum ?

- Datenbankverbindungen werden aus dem Connectionpool bedient und laufen standardmäßig aller unter dem gleichen Datenbankuser
- In der Datenbanksession ist der einzelne Applikationsuser nicht mehr bekannt.
- Sessioneinstellungen u.U. bleiben erhalten wenn die DB-Verbindung an den Connectionpool zurückgegeben und für eine andere Verbindung verwendet wird => Potientelle Sicherheitslücke

Kernproblem:

- Eindeutige Clientinformationen müssen von der Middleware in die DB-Verbindung durchgereicht werden.

Bedingung

- **Der Benutzer muss im Weblogic bekannt sein**
  - Nur Applikationen, die über die Authentisierung des Weblogic laufen werden unterstützt.

Konfiguration

- **Parameter: “Set client ID On Connection”**
  - CLIENT_IDENTIFIER wird mit Wert aus Mappingtabelle gefüllt.
    Wenn kein Mapping für den WL-Benutzer vorhanden ist, bleibt Feld leer.
  - Datenbankverbindungen laufen alle unter der Identität des Standardusers

- **Vorteil:**
  - Keine Änderungen/Beeinflussungen an bestehenden Applikationen und Connectionpool
- **Nachteil:**
  - Sessioneinstellungen bleiben erhalten wenn die DB-Verbindung an den Connectionpool zurückgegeben und für eine andere Verbindung verwendet wird => Potientelle Sicherheitslücke

Konfiguration

- **Parameter: “Enable Identity Based Connection Pooling”**
  - Es wird im Pool eine Datenbankverbindung mit der angefragten Identität im Connectionpool gesucht und wieder benutzt oder, wenn nicht vorhanden, eine Neue eröffnet.
  - Wenn kein Mapping vorhanden ist, wird der Standarduser benutzt.

- **Vorteile:**
  - Eindeutige Trennung, da Eindeutige WLS<->DB Benutzerzuordnung
  - Weitreichende Möglichkeiten da „vollwertiger“ DB Benutzer
- **Nachteile:**
  - Muss in Applikationsarchitektur berücksichtigt sein.
  - Zusätzliche Pflege von DB Benutzern
  - Connectionpool muss ggf. angepasst werden

Nutzung der Benutzeridentität in der DB

Virtual Private Database (VPD)
Jedes Statement wird vor der Ausführung um eine WHERE Klausel erweitert. Das Argument der WHERE Klausel ist der Rückgabewert einer Funktion

Oracle Lable Security (OLS)
Anwendung der VPD bei dem ein Label-, Gruppen-, und Hierarchiebasiertes System zur Rechteverwaltung auf Datensatzebene bereitgestellt wird

OLS

Level (Hierarchisch):
zB. Öffentlich -> Vertraulich -> Streng Vertraulich

Abteilungen:
z.B. Abteilung A | Abteilung B | Abteilung C

Gruppen:
Gruppenhierarchie, z.B Leiter -> Mitarbeiter

Demo

Aufzeigen des gewählten Wegs

Middleware:
“Enable Identity Based Connection Pooling”
Feststellen der Identität

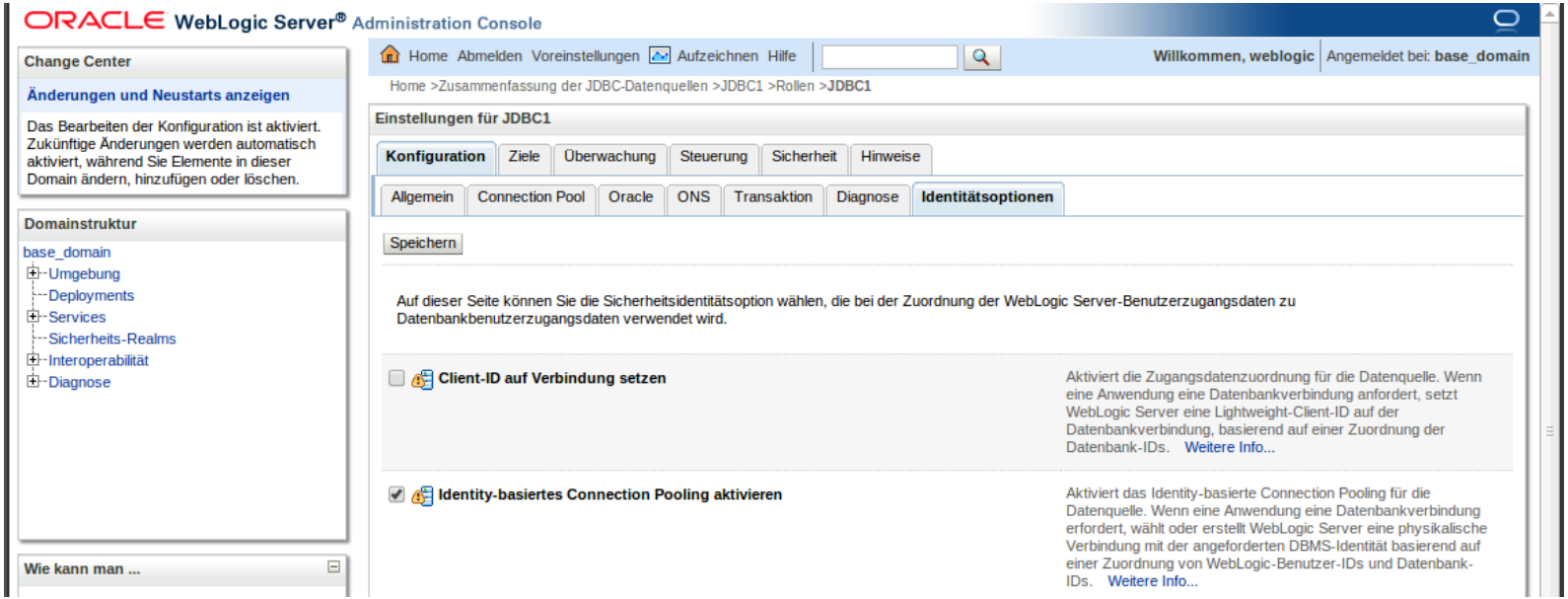
Datenbank:
Oracle Lable Security
Umsetzung der Berechtigungsstufen

Storage:
Partitioning
Unterteilung nach Bundesländern

Berechtigungen in der Demo

- Bürger – alles was öffentliche ist
- Bearbeiter – vertrauliches ggf. beschränkt auf Land
- Leiter – streng vertrauliches gg. beschränkt auf Land

Data Source konfigurieren 1



Data Source konfigurieren 2

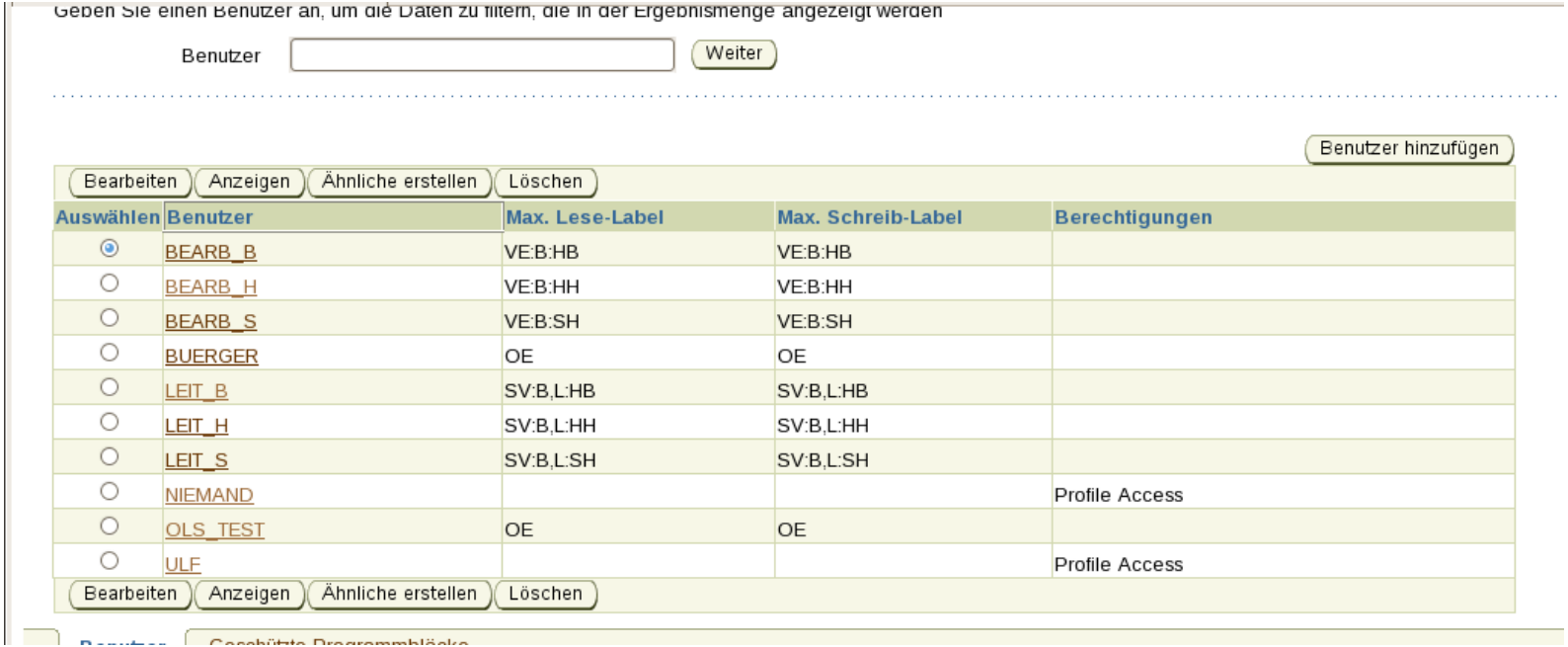
Mappingtabelle anlegen

Data Source konfigurieren 1

Mappingtabelle anlegen

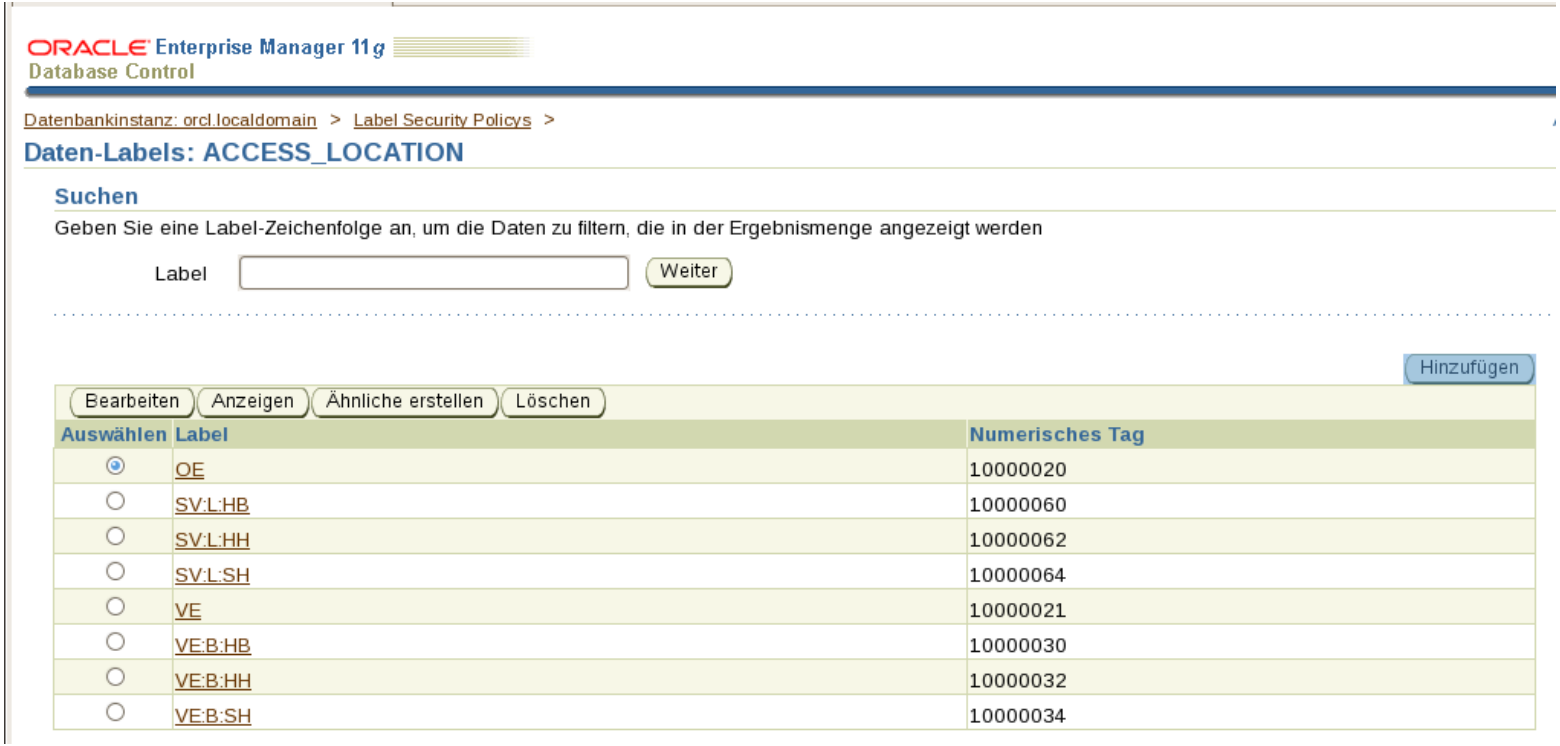
OLS Konfiguration

Autorisierungen festlegen



OLS Konfiguration

Label anlegen



OLS Daten

Alle Daten, alle DB Sessions

```
SQL> r
  1* select sid,username from v$session where length(username)>0

       SID USERNAME
---------- ------------------------------
        15 LBACSYS
        17 SYSTEM
        18 OTEST
        19 ULF
        21 ULF
        22 SYSMAN
        29 SYSMAN
       140 SYSMAN
       141 OLS_TEST
       147 SYSTEM
       150 DBSNMP

       SID USERNAME
---------- ------------------------------
       152 SYSMAN
       153 SYSMAN
       156 SYSMAN
       158 DBSNMP

15 Zeilen ausgewahlt.
```

```
SQL> r
  1* select * from ols_test.appdata order by id

        ID ZU DATEN                          LAN SI OLS_SPALTE
---------- -- ------------------------------ --- -- ----------
         1 L  Leiter Hamburg Oeffentlich     HH  Oe   10000020
         2 B  Bearbeiter Hamburg Oeffentlich HH  Oe   10000020
         3 B  Bearbeiter Bremen Vertraulich  HB  VE   10000030
         4 B  Bearbeiter Bremen Vertraulich  HB  VE   10000030
         5 L  Leiter Bremen Streng Vert.     HB  SV   10000060
         6 B  Bearbeiter Bremen Oeffentlich  HB  Oe   10000020
         7 L  Leiter SH Streng Vertraulich   SH  SV   10000064
         8 L  Leiter HH Streng Vertraulich   HH  SV   10000062
         9 L  Allgemein Vertraulich          HH  VE   10000021
        10 B  Bearbeiter HH Vertraulich      HH  VE   10000032
        11 B  Bearbeiter HH Vertraulich      HH  VE   10000032

        ID ZU DATEN                          LAN SI OLS_SPALTE
---------- -- ------------------------------ --- -- ----------
        12 L  Leiter HB Streng Vertraulich   HB  SE   10000060
        13 L  Leiter HB Streng Vertraulich   HB  SE   10000060
        14 L  Leiter SH Streng Vertraulich   SH  SV   10000064
        15 B  Bearbeiter SH  Vertraulich     SH  VE   10000034
        16 L  Leiter SH Streng Vertraulich   SH  SV   10000064
        17 B  Bearbeiter SH  Vertraulich     SH  VE   10000034
        18 B  Bearbeiter HB Vertraulich      HB  VE   10000030
        19 B  Bearbeiter HB Vertraulich      HB  VE   10000030

19 Zeilen ausgewahlt.

SQL> show user
USER ist "LBACSYS"
SQL>
```

OLS

Beschränkte Sichtbarkeit 1

```
SQL> r
  1* select sid,username from v$session where length(username)>0

       SID USERNAME
---------- ------------------------------
        15 LBACSYS
        17 SYSTEM
        18 OTEST
        19 ULF
        21 ULF
        22 SYSMAN
        29 SYSMAN
       140 SYSMAN
       141 OLS_TEST
       147 SYSTEM
       149 LEIT_B

       SID USERNAME
---------- ------------------------------
       150 DBSNMP
       152 SYSMAN
       153 SYSMAN
       156 SYSMAN
       158 DBSNMP

16 Zeilen ausgewahlt.

SQL>
```

OLS Demo Seite

Tue Nov 13 15:17:31 CET 2012

DB-Session User: LEIT_B

SID: 149

Weblogic User: leiterhb

Benutzerdaten:

ID	ZUGRIFF	DATEN	LAND	SICHERHEIT	OLS_SPALTE
1	L	Leiter Hamburg Oeffentlich	HH	Oe	10000020
2	B	Bearbeiter Hamburg Oeffentlich	HH	Oe	10000020
3	B	Bearbeiter Bremen Vertraulich	HB	VE	10000030
4	B	Bearbeiter Bremen Vertraulich	HB	VE	10000030
5	L	Leiter Bremen Streng Vert.	HB	SV	10000060
6	B	Bearbeiter Bremen Oeffentlich	HB	Oe	10000020
12	L	Leiter HB Streng Vertraulich	HB	SE	10000060
13	L	Leiter HB Streng Vertraulich	HB	SE	10000060
18	B	Bearbeiter HB Vertraulich	HB	VE	10000030
19	B	Bearbeiter HB Vertraulich	HB	VE	10000030
9	L	Allgemein Vertraulich	HH	VE	10000021

OLS

Beschränkte Sichtbarkeit 2

```
SQL> r
  1* select sid,username from v$session where length(username)>0

       SID USERNAME
---------- ------------------------------
        15 LBACSYS
        17 SYSTEM
        18 OTEST
        21 ULF
        22 SYSMAN
        27 BEARB_H
        29 SYSMAN
       140 SYSMAN
       141 OLS_TEST
       147 SYSTEM
       149 LEIT_B

       SID USERNAME
---------- ------------------------------
       150 DBSNMP
       152 SYSMAN
       153 SYSMAN
       156 SYSMAN
       158 DBSNMP

16 Zeilen ausgewahlt.

SQL>
```

OLS Demo Seite

Tue Nov 13 15:21:53 CET 2012

DB-Session User: BEARB_H

SID: 27

Weblogic User: bearbeiter_hh

Benutzerdaten:

ID	ZUGRIFF	DATEN	LAND	SICHERHEIT	OLS_SPALTE
1	L	Leiter Hamburg Oeffentlich	HH	Oe	10000020
2	B	Bearbeiter Hamburg Oeffentlich	HH	Oe	10000020
6	B	Bearbeiter Bremen Oeffentlich	HB	Oe	10000020
10	B	Bearbeiter HH Vertraulich	HH	VE	10000032
11	B	Bearbeiter HH Vertraulich	HH	VE	10000032
9	L	Allgemein Vertraulich	HH	VE	10000021

Q&A

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®