



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 => Potentielle 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 => Potentielle 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 Label Security (OLS)

Anwendung der VPD bei dem ein Label-, Gruppen-, und Hierarchiebasiertes System zur Rechteverwaltung auf Datensatzebene bereitgestellt wird

OLS

Level (Hierarchisch):

z.B. 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 Label 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

The screenshot displays the Oracle WebLogic Server Administration Console interface. The top navigation bar includes the Oracle logo, the text 'WebLogic Server® Administration Console', and a search bar. The breadcrumb trail reads 'Home > Zusammenfassung der JDBC-Datenquellen > JDBC1 > Rollen > JDBC1'. The main content area is titled 'Einstellungen für JDBC1' and features several tabs: 'Konfiguration', 'Ziele', 'Überwachung', 'Steuerung', 'Sicherheit', and 'Hinweise'. The 'Konfiguration' tab is active, and within it, the 'Identitätsoptionen' sub-tab is selected. A 'Speichern' button is located at the top of the configuration area. Below this, a text block states: 'Auf dieser Seite können Sie die Sicherheitsidentitätsoption wählen, die bei der Zuordnung der WebLogic Server-Benutzerzugangsdaten zu Datenbankbenutzerzugangsdaten verwendet wird.' Two configuration options are listed: 'Client-ID auf Verbindung setzen' (unchecked) and 'Identity-basiertes Connection Pooling aktivieren' (checked). Each option includes a brief description and a 'Weitere Info...' link. On the left side, a 'Change Center' panel shows 'Änderungen und Neustarts anzeigen' and a 'Domainstruktur' tree with nodes for 'base_domain', 'Umgebung', 'Deployments', 'Services', 'Sicherheits-Realms', 'Interoperabilität', and 'Diagnose'. A 'Wie kann man ...' panel is partially visible at the bottom left.

ORACLE WebLogic Server® Administration Console

Home > Zusammenfassung der JDBC-Datenquellen > JDBC1 > Rollen > JDBC1

Einstellungen für JDBC1

Konfiguration | Ziele | Überwachung | Steuerung | Sicherheit | Hinweise

Allgemein | Connection Pool | Oracle | ONS | Transaktion | Diagnose | **Identitätsoptionen**

Speichern

Auf dieser Seite können Sie die Sicherheitsidentitätsoption wählen, die bei der Zuordnung der WebLogic Server-Benutzerzugangsdaten zu Datenbankbenutzerzugangsdaten verwendet wird.

- Client-ID auf Verbindung setzen**
Aktiviert die Zugangsdatenzuordnung für die Datenquelle. Wenn eine Anwendung eine Datenbankverbindung anfordert, setzt WebLogic Server eine Lightweight-Client-ID auf der Datenbankverbindung, basierend auf einer Zuordnung der Datenbank-IDs. [Weitere Info...](#)
- Identity-basiertes Connection Pooling aktivieren**
Aktiviert das Identity-basierte Connection Pooling für die Datenquelle. Wenn eine Anwendung eine Datenbankverbindung erfordert, wählt oder erstellt WebLogic Server eine physikalische Verbindung mit der angeforderten DBMS-Identität basierend auf einer Zuordnung von WebLogic-Benutzer-IDs und Datenbank-IDs. [Weitere Info...](#)

Wie kann man ...

Data Source konfigurieren 2

Mappingtabelle anlegen

Das Bearbeiten der Konfiguration ist aktiviert. Zukünftige Änderungen werden automatisch aktiviert, während Sie Elemente in dieser Domain ändern, hinzufügen oder löschen.

Domainstruktur

- base_domain
 - Umgebung
 - Deployments
 - Services
 - Sicherheits-Realms
 - Interoperabilität
 - Diagnose

Wie kann man ...

- Zugangsdatenzuordnung für eine JDBC-Datenquelle konfigurieren

Systemstatus

Integrität der gestarteten Server

Failed (0)

Einstellungen für JDBC1

Konfiguration | Ziele | Überwachung | Steuerung | **Sicherheit** | Hinweise

Rollen | Polycys | **Zugangsdatenzuordnungen**

Bei der Zugangsdatenzuordnung für eine JDBC-Datenquelle wird ein WebLogic Server-Benutzer einem Remote-Benutzer zugeordnet.

Auf dieser Seite können Sie Zugangsdatenzuordnungs-Services für eine JDBC-Datenquelle konfigurieren.

[Diese Tabelle anpassen](#)

Zugangsdatenzuordnungen

Neu | Löschen Anzeigen 1 für 8 von 8 | Vorherige | Weiter

<input type="checkbox"/>	WLS-Benutzer ↕	Remote-Benutzer
<input type="checkbox"/>	Bearbeiter_HB	BEARB_B
<input type="checkbox"/>	Bearbeiter_HH	BEARB_H
<input type="checkbox"/>	Bearbeiter_SH	BEARB_S
<input type="checkbox"/>	Buerger	Buerger
<input type="checkbox"/>	dbuf	logontest
<input type="checkbox"/>	LeiterHB	LEIT_B
<input type="checkbox"/>	LeiterHH	LEIT_H
<input type="checkbox"/>	LeiterSH	LEIT_S

Data Source konfigurieren 1

Mappingtabelle anlegen

The screenshot displays the Oracle WebLogic Administration Console interface. The left sidebar shows the 'Change Center' with a notification about configuration changes and a 'Domainstruktur' tree. The main content area is titled 'JDBC-DataSource-Zugangsdatenzuordnung bearbeiten'. It includes a 'Speichern' button at the top, a breadcrumb trail, and a 'WebLogic Server-Benutzer' dropdown set to 'Bearbeiter_HB'. Below this, there are input fields for 'Remote-Benutzer' (containing 'BEARB_B'), 'Remote-Kennwort', and 'Kennwort bestätigen', all masked with dots. A 'Speichern' button is located at the bottom of the form.

Change Center

Änderungen und Neustarts anzeigen

Das Bearbeiten der Konfiguration ist aktiviert. Zukünftige Änderungen werden automatisch aktiviert, während Sie Elemente in dieser Domain ändern, hinzufügen oder löschen.

Domainstruktur

- base_domain
 - Umgebung
 - Deployments
 - Services
 - Sicherheits-Realms
 - Interoperabilität
 - Diagnose

Wie kann man ...

- Zugangsdatenzuordnung für eine JDBC-

Home Abmelden Voreinstellungen Aufzeichnen Hilfe Willkommen, weblogic Angemeldet bei: base_domain

Home > Zusammenfassung der JDBC-Datenquellen > JDBC1 > Rollen > JDBC1 > Rollen

JDBC-DataSource-Zugangsdatenzuordnung bearbeiten

Speichern

Bei der Zugangsdatenzuordnung für eine JDBC-Datenquelle werden WebLogic Server-Benutzer-IDs Remote-Benutzern zugeordnet.

Auf dieser Seite können Sie Zugangsdatenzuordnungs-Services für eine Datenquelle konfigurieren.

WebLogic Server-Benutzer:	Bearbeiter_HB	Die WebLogic Server-Benutzer-ID, die der Remote-Benutzer-ID zugeordnet wird. Weitere Info...
Remote-Benutzer:	<input type="text" value="BEARB_B"/>	Die Datenbankbenutzer-ID, die dem gewählten WebLogic Server-Benutzer zugeordnet werden soll. Weitere Info...
Remote-Kennwort:	<input type="password" value="....."/>	Das Datenbankkennwort für die Datenbankbenutzer-ID. Weitere Info...
Kennwort bestätigen:	<input type="password" value="....."/>	

Speichern

OLS Konfiguration

Autorisierungen festlegen

Geben Sie einen Benutzer an, um die Daten zu filtern, die in der Ergebnismenge angezeigt werden

Benutzer

Weiter

Benutzer hinzufügen

Benutzer				
Bearbeiten Anzeigen Ähnliche erstellen Löschen				
Auswählen	Benutzer	Max. Lese-Label	Max. Schreib-Label	Berechtigungen
<input checked="" type="radio"/>	BEARB_B	VE:B:HB	VE:B:HB	
<input type="radio"/>	BEARB_H	VE:B:HH	VE:B:HH	
<input type="radio"/>	BEARB_S	VE:B:SH	VE:B:SH	
<input type="radio"/>	BUERGER	OE	OE	
<input type="radio"/>	LEIT_B	SV:B:L:HB	SV:B:L:HB	
<input type="radio"/>	LEIT_H	SV:B:L:HH	SV:B:L:HH	
<input type="radio"/>	LEIT_S	SV:B:L:SH	SV:B:L:SH	
<input type="radio"/>	NIEMAND			Profile Access
<input type="radio"/>	OLS_TEST	OE	OE	
<input type="radio"/>	ULF			Profile Access

Bearbeiten

Anzeigen

Ähnliche erstellen

Löschen

OLS Konfiguration

Label anlegen

ORACLE Enterprise Manager 11g Database Control

Datenbankinstanz: orcl.localdomain > Label Security Policies >

Daten-Labels: ACCESS_LOCATION

Suchen

Geben Sie eine Label-Zeichenfolge an, um die Daten zu filtern, die in der Ergebnismenge angezeigt werden

Label

Weiter

Hinzufügen

Auswählen	Label	Numerisches Tag
<input checked="" type="radio"/>	<u>OE</u>	10000020
<input type="radio"/>	<u>SV:L:HB</u>	10000060
<input type="radio"/>	<u>SV:L:HH</u>	10000062
<input type="radio"/>	<u>SV:L:SH</u>	10000064
<input type="radio"/>	<u>VE</u>	10000021
<input type="radio"/>	<u>VE:B:HB</u>	10000030
<input type="radio"/>	<u>VE:B:HH</u>	10000032
<input type="radio"/>	<u>VE:B:SH</u>	10000034

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 ausgewählt.

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

```
ID ZU DATEN LAN SI OLS_SPALTE
-----
1 L Leiter Hamburg Oeffentlich HH 0e 10000020
2 B Bearbeiter Hamburg Oeffentlich HH 0e 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 0e 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 ausgewählt.

```
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 ausgewählt.

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 ausgewählt.
```

```
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®