Seab@er Software AG

Oracle Dokumentation
04 - Benutzer / Rechte

1. Vorwort

Diese Dokumentation ist entstanden, da ich beruflich mich mit Oracle beschäftigen musste. Was ich sehr gerne übernommen habe und es macht richtig Spaß mit Oracle zu arbeiten. Alle Informationen, die ich zusammentragen konnte, habe ich nun in dieser Dokumentation geschrieben. Ebenso sind meine Erfahrungen in diese Dokumentation eingeflossen.

Oracle wird auf Linux und Windows Servern in unserer Firma betrieben. Die Installation von Oracle wird für die Linux Server beschrieben, da eine Windows Installation nicht so aufwendig ist.

Diese Dokumentation wurde für die Oracle Datenbank 10G R2 und 11G R1 geschrieben und auch getestet.

Die Datenbank in der Version 11G R1 wurde in einer VMWare Session installiert und als Betriebssystem wurde Novel SLES 10 SP2 installiert.

Bei dem Betriebssystem und auch Oracle handelt es sich um die 32 Bit Version. Für die 64 Bit Version werden noch zusätzliche Softwarepakete gebraucht.

Bei Fragen und Anregungen bin ich unter folgender Mail Adresse zu erreichen:

uwe@seabaer-ag.de

2. Benutzer- / Rechteverwaltung

2.1 Neue Benutzer einrichten

Um einen Benutzer einen Zugriff auf die DB zu ermöglichen, muss dieser Benutzer zunächst der DB bekannt gemacht werden.

```
sql>create user <username>
 2>identified by <passwd>
 3>default tablespace pds
 4>temporary tablespace temp_seg
 5>quota 100m on <tablespace_name>
 6>profile default
 7>password expire
 8>account unlock;
```

Domain User werden folgendermaßen angelegt. Da die `identification` mit `externally` angelegt worden ist, so braucht der User bei der Anmeldung an Oracle kein Passwort anzugeben.

```
sql>create user <domain>\<username> identified externally
 2>default tablespace pds temporary tablespace temp_seg;
```

Für die `identified` und `quota` gibt es folgende Möglichkeiten.

```
identified by <passwd>
identified externally
identified globally as 'CN=admin, OU=company, O=oracle, C=DE'

quota 50[k,m,g,t,e] on <tablespace_name>
quota unlimited on <tablespace_name>
```

Alle Zuordnungen, die mit *create user* getroffen wurden, können mit dem Befehl *alter user* geändert werden.

```
sql>alter user dbuschi temporary tablespace temp_segs;
```

2.2 Benutzer auflisten

Die Oracle User werden in der Tabelle `dba_users` verwaltet.

```
sql>select username, account_status, lock_date from dba_users
 2>order by username;

USERNAME    ACCOUNT_STATUS    LOCK_DATE
---------   ----------------  ---------
ANONYMOUS   EXPIRED & LOCKED  05.12.10
CTXSYS      EXPIRED & LOCKED  05.12.10
.
.
SYS         OPEN
SYSTEM      OPEN
.
.
```

2.3 Benutzer an DB anmelden

Der Benutzer muss sich an der Datenbank anmelden.

```
oracle@woby1002>sqlplus <dbuser>@<oracle_sid>

oracle@woby1002>sqlplus /nolog

sql>connect <dbuser>@<oracle_sid>
```

2.4 Löschen eines Benutzers

Alle Spuren des Benutzers werden aus der Datenbank entfernt, also der Benutzer selbst, seine Schema und damit auch alle seine Objekte. Hat der Benutzer noch Objekte in der Datenbank, so muss die Option *Cascade* benutz werden.

```
sql>drop user dbuschi cascade;
```

2.5 Kennwort ändern

```
sql>alter user <username> identified by <passwd>;
```

2.6 Benutzer sperren

```
sql>alter user <username> account lock;
```

2.7 Benutzer entsperren

```
sql>alter user <username> account unlock;
```

Sollte der Account des Benutzers abgelaufen (expired) sein, so kann man das mit einem neusetzen des Passwortes wieder aktivieren.

```
sql>select username, account_status, expiry_date from dba_users
 2>where username = 'SCOTT';

Username    Account_Status    Expiry_date
----------- ----------------- ------------
SCOTT       expired           10-May-2011

sql>alter user scott identified by <new_passwd>;
sql>select username, account_status, expiry_date from dba_users
 2>where username = 'SCOTT';

Username    Account_Status    Expiry_date
----------- ----------------- ------------
SCOTT       open
```

2.8 Account Expired(Grace)

```
sql>select spare4 from sys.user$ where name = '<username>';

sql>alter user <username> indetified by values 'Ergebnis von spare4 query';
```

2.9 Profile

2.9.1 Profile auflisten

Profile werden in der Tablle `dba_profiles` verwaltet.

```
sql>select resource_name, limit from dba_profiles
 2> where profile = 'DEFAULT';
RESOURCE_NAME                  LIMIT
------------------------------ ----------------
COMPOSITE_LIMIT                UNLIMITED
SESSIONS_PER_USER              UNLIMITED
CPU_PER_SESSION                UNLIMITED
CPU_PER_CALL                   UNLIMITED
LOGICAL_READS_PER_SESSION      UNLIMITED
LOGICAL_READS_PER_CALL         UNLIMITED
IDLE_TIME                      UNLIMITED
CONNECT_TIME                   UNLIMITED
PRIVATE_SGA                    UNLIMITED
FAILED_LOGIN_ATTEMPS           10
PASSWORD_LIFE_TIME             UNLIMITED
PASSWORD_REUSE_TIME            UNLIMITED
PASSWORD_REUSE_MAX             UNLIMITED
PASSWORD_VERIFY_FUNCTION       NULL
PASSWORD_LOCK_TIME             UNLIMITED
PASSWORD_GRACE_TIME            UNLIMITED
```

2.9.2 Profile erstellen

```
sql>create profile <profile_name>
 2>limit session_per_user 1
 3>idle_time 1
 4>failed_login_attempts 3;
```

2.9.3 Profile ändern

```
sql>alter profile <profile_name> limit connection_time 600;
```

2.9.4 Profile zuordnen

```
sql>alter user <username> profile <profile_name>;
```

2.10 Zugriffsrechte für die Datenbank

2.10.1 Erteilen / Löschen

Oracle kennt etwa 80 verschiedene Privilegien für den Datenbankzugriff. Diese Privelegien werden in *Roles* zusammengefasst. Nachfolgend eine kleine Auswahl der wichtigsten Oracle Rollen.

Roles	Privelegien
Connect	create session, alter session, create database link, create view, create table
resource	create table, create cluster, create sequence, create procedure, create trigger
Dba	all system privs mit admin option
exp_full_database	select any table, backup any table, insert/update/delete on sys.incvid / sys.incfil / sys.incexp
imp_full_database	become user

```
sql>grant connect, resource to dbuschi with admin option;
```

Wenn der Benutzer die Rechte mit der Option *with admin option* erhält, so kann er diese Rechte auch an andere Benutzer weitergeben.

```
sql>revoke privileg from dbuschi;
```

Mit dem `revoke` Befehl werden dem Benutzer die Privilegien/Rechte wieder entzogen.

Alle Rechte findet man in den DD-Views *DBA_ROLE_PRIVS* und *DBA_SYS_PRIVS*.

Wird einem Oracle User die DBA Rechte erteilt, so kann er sich normal und mit `as sysdba` anmelden. Erstellt der Oracle User nach der Anmeldung mit `as sysdba` z.B. Tabellen, so gehören diese dem Oracle User SYS.

```
sql>grant sysdba, dba to orauser;
sql>connect orauser/orauser;
sql>create table table1 (id number);
sql>connect orauser/orauser as sysdba;
sql>create table table2 (id number);
sql>select owner, object_name from dba_objects
 2>where object_name like 'TABLE_';
OWNER   OBJECT NAME
------- ---------------
SYS     Table2
Orauser Table1
```

2.10.2 Password Datei

Mit einer Password Datei wird Usern eine Anmeldung an der Datenbank ermöglicht, auch wenn die Datenbank nicht gestartet worden ist. Der User muss über `sysdba` Rechte verfügen. Ob eine Password Datei verwendet werden soll, wird mit dem Parameter `remote_login_passwordfile` geregelt. Für diesen Parameter gibt es die Werte None, Shared und Exclusive.

Exclusive	Die Password Datei ist nur für eine Instanz.
Shared	Wird von allen Instanzen verwendet, speichert nur `sys` und `system` User.
None	Es wird keine Password Datei verwendet.

Die Password Datei wird mit dem Befehl `orapwd` erstellt.

```
oracle@woby1002>orapwd file=$ORACLE_HOME/dbs/orapw$ORACLE_SID
```

Den Inhalt der Datei kann man mit dem folgenden Statement abgefragt werden.

```
sql>select * from v$pwfile_users;

USERNAME    SYSDB SYSOP SYSAS
----------- ----- ----- -----
SYS         TRUE  TRUE  FALSE
```

2.11 Zugriffsrechte für Datenbankobjekte

Nicht nur der Zugriff auf die DB selbst, sondern auch der Zugriff auf die Datenbankobjekte wird mit dem Befehl *Grant* und *Revoke* gesteuert. Diese Privilegien kann ein Benutzer für seine Objekte vergeben. Voraussetzung ist allerdings, dass er selbst das Systemprivileg *Grant any Privilege* besitzt.

Objektprivilegien	Beschreibung
Alter	Tabellen oder Sequenzen können geändert werden. Trigger für die Tabellen können erstellt werden.
Execute	Procedures können ausgeführt werden.
Delete	Datensätze in Tabellen oder Views können gelöscht werden.
Index	Indexe auf Tabellen können angelegt werden.
Insert	Einfügen neuer Datensätze ist erlaubt.
reference	Ein Foreign Key auf einen Tabelle kann erzeugt werden.
Select	Lesen einer Tabelle, eines Views oder einer Sequence.
Update	Verändern einzelner Datensätze.
All	alle oben genannten Rechte.

```
sql>grant select,update on pdtable_101 to dbsys;
sql>revoke select on pdtable_101 from dbsys;
```

Die Rechte können nicht nur einem Oracle User zugewiesen werden, sondern auch Rollen.

Für die Kontrolle der Privilegien stehen folgende Data Dictionary-Views zu Verfügung.

Oracle-Benutzeridentifizierung	dba_users
Systemprivilegien	user_sys_privs dba_sys_privs session_privs
Objectprivilegien	all_tab_privs user_tab_privs dba_tab_privs
Spaltenprivilegien	all_col_privs user_col_privs dba_col_privs
Objectprivilegien weitergegeben	all_tab_privs_made user_tab_privs_made
Objectprivilegien erhalten	all_tab_privs_recd user_tab_privs_recd
Spaltenprivilegien weitergegeben	all_col_privs_made user_col_privs_made
Spaltenprivilegien erhalten	all_col_privs_recd user_col_privs_recd
Quotas	user_ts_quotas all_ts_quotas dba_ts_quotas
Rechte Benutzer public	table_privileges
Spaltenbezogenen Rechte Benutzer public	column_privileges

2.12 Benutzerrechte auflisten

```
sql>select * from dba_role_privs order by grantee;

GRANTEE           GRANTED_ROLE            ADM   DEF
---------------  ---------------------   ---   ---
CTXSYS            CTXAPP                  YES   YES
CTXSYS            RESOURCE                NO    YES
DBA               XDBWEBSERVICES          NO    YES
.
.

sql>select * from dba_sys_privs order by grantee;

GRANTEE           PRIVILEGE               ADM
----------------- ----------------------  ---
DBA               GLOBAL QUERY REWRITE    YES
DBA               CREATE ANY CONTEXT      YES
DBA               DROP ANY ROLE           YES
.
.
```

2.13 Rollen

2.13.1 Rollen auflisten

Aktuelle Session Rollen auflisten.

```
sql>select * from session_roles;
```

Welche Rollen gibt es.

```
sql>select * from dba_roles;

ROLE                    PASSWORD
----------------------  --------
CONNECT                 NO
RESOURCE                NO
DBA                     NO
SELECT_CATALOG_ROLE     NO
EXECUTE_CATALOG_ROLE    NO
.
.
```

Die Zuordnung Rolle -> Privilegien befinden sich in der Tabelle / View `role_sys_privs`.

```
sql>select * from role_sys_privs order by role;

ROLE        PRIVILEGE               ADM
----------- ----------------------  ---
CONNECT     CREATE SESSION          NO
DBA         CREATE ANY TRIGGER      YES
DBA         ALTER ANY TRIGGER       YES
.
.
```

Eine Zuordnung Rolle -> Rolle findet man in der Tabelle / View `role_role_privs`.

```
sql>select * from role_role_privs order by role;

ROLE              GRANTED_ROLE                   ADM
----------------- ------------------------------ ---
DBA               JAVA_DEPLOY                    NO
DBA               GATHER_SYSTEM_STATISTCS        NO
DBA               EXECUTE_CATALOG_ROLE           YES
.
.
```

Die Rolle -> Tabellen Privelegie Zuordnung warden in der Tabelle / View `role_tab_privs` angezeigt.

```
sql>select * from role_tab_privs order by role;

ROLE        OWNER       TABLE_NAME      COLUMN_NAME   PRIVILEGE   GRA
----------- ----------- --------------- ------------  ----------  ---
DBA         SYS         DBA_TSM_STORAGE               SELECT      NO
DBA         SYS         DBMS_UADV_ADR                 EXECUTE     NO
.
.
```

Welche Rollen / Berechtigungen hat ein User erhalten. Bei der ersten Abfrage wird die Zuordnung `User -> Rolle` angezeigt und in der zweiten Abfrage die Zuordnung `User -> Privillegien`.

```
sql>select * from dba_role_privs where grantee = 'SCOTT';
GRANTEE     GRANTED_ROLE      ADM   DEF
----------- ---------------- ----- ----
SCOTT       Connect           No    Yes
SCOTT       Resource          No    Yes
SCOTT       Create Table      No    Yes

sql>select * from dba_sys_privs where grantee = 'SCOTT';
GRANTEE     PRIVILEGE               ADM
----------- ---------------------- ----
SCOTT       Create Session          No
SCOTT       Unlimited Tablespace    No
```

2.13.2 Rollen erstellen

```
sql>create role <role_name>;
```

```
sql>create role ris_pds;
```

2.13.3 Rollen löschen

```
sql>drop role <role_name>;
```

2.13.4 Systemprivilegien einer Rolle zuordnen

```
sql>grant <system_priv> to <role_name>;
```

```
sql>grant create database link, create sequence to ris_pds;
```

2.13.5 Rolle Kennwort zuordnen

```
sql>alter role <role_name> identified by <password>;
```

2.14 Quotas

2.14.1 Quotas setzen

Mit dieser Quota wird festgelegt, wie viel Platz der Benutzer für die Tabelle belegen darf.

```
sql>alter user dd_test quotas 15M on test;
```

2.14.2 Quotas anzeigen

Die vergebenen Quotas können für die User mit einer Abfrage auf die Tabelle `user_ts_quotas` abgefragt werden. Ausserdem gibt es noch die Tabelle `dba_ts_quotas`.

```
sql>select * from user_ts_quotas;

sql>select tablespace_name, username from dba_ts_quotas;
TABLESPACE_NAME   USERNAME
----------------- --------
USER              DD_TEST
USER              SCOTT
```

3. Copyright