

Tipps & Tricks: April 2005

Bereich:	SQL	Erstellung:	04/2005 MM
Versionsinfo:	9.2, 10.2, 11.1	Letzte Überarbeitung:	06/2009 EF

 [Als PDF Downloaden!](#)

Privilegien und Rollen

Für Zugriffe auf eine Oracle-Datenbank werden Zugriffsrechte benötigt. Jedes Zugriffsrecht (privilege) hat einen Namen. Mehrere Zugriffsrechte werden zu Gruppen zusammengefasst. Diese Gruppen werden Rollen (role) genannt. Rechte können den DB-Usern einzeln (direct grant) oder paketweise (als Rollen) zugeteilt werden.

Die View SESSION_ROLES zeigt die aktivierten Rollen an, über die direkt vergebenen Systemrechte kann man sich über die View SESSION_PRIVS informieren.

Rechte und Rollen werden den DB-Usern mit folgendem Befehl zugeteilt:

```
GRANT <rolename/privilege-name> TO <username>;
```

Zugeweilte Rechte und Rollen können auch wieder entzogen werden:

```
REVOKE <rolename/privilege-name> FROM <username>;
```

Rollen

Jedem User können beliebig viele Rollen zugeteilt werden. Innerhalb einer Session kann der User (oder eine Applikation) diese dann beliebig oft aktivieren/deaktivieren:

```
SET ROLE <role,role...>
```

Die Anzahl parallel aktivierbarer Rollen wird durch den Initialisierungs-Parameter MAX_ENABLED_ROLES begrenzt.

Default-Rollen

Die Aktivierung von Rollen kann auch automatisch beim Logon erfolgen. Alle Rollen, die bei jedem Logon des Users aktiviert werden sollen, nennt man Default-Rollen. Die Default-Rollen eines Users werden über

```
ALTER USER <username> DEFAULT ROLE <role, role, ...>
```

definiert. Voraussetzung ist natürlich, dass diese Rollen dem User vorher bereits zugeteilt wurden.

```
SQL> ALTER USER scott DEFAULT ROLE connect, resource, dba;  
-> ORA-01955: DEFAULT ROLE 'DBA' wurde Benutzer nicht erteilt
```

Alle einem User zugeteilten Rollen lassen sich mit folgender Kurzschreibweise als Default-Roles aktivieren:

```
ALTER USER <username> DEFAULT ROLE ALL;
```

Bei der ersten Zuteilung einer Rolle zu einem User wird sie automatisch in die Liste der DEFAULT-Roles aufgenommen:

```
SQL> GRANT DBA TO scott;
Benutzerzugriff (Grant) wurde erteilt.

SQL> SELECT * FROM dba_role_privs WHERE GRANTEE = 'SCOTT';

GRANTEE      GRANTED_ROLE  DEFAULT_ROLE
-----
SCOTT        DBA           YES
```

Die Default Rollen-Liste kann jederzeit neu definiert werden:

```
SQL> ALTER USER scott DEFAULT ROLE connect , resource;
Benutzer wurde geändert.
```

Es sind jedoch immer nur die im letzten ausgeführten Befehl angegebenen Rollen als DEFAULT-Rollen definiert.

```
SQL> SELECT * FROM dba_role_privs WHERE GRANTEE = 'SCOTT';

GRANTEE      GRANTED_ROLE  DEFAULT_ROLE
-----
SCOTT        DBA           NO
SCOTT        CONNECT       YES
SCOTT        RESOURCE      YES
```

User-Logon

Beim Logon werden nun zunächst automatisch alle Privilegien aktiviert, die dem User explizit zugeteilt (grant) worden sind. Zusätzlich werden dann alle Privilegien der Default-Roles des Users aktiviert.

Falls einem User eine der ihm zugeteilten Rollen wieder entzogen wird, verschwindet natürlich auch der zugehörige Eintrag in der dba_role_privs:

```
SQL> REVOKE dba FROM scott;
Benutzerzugriff wurde aufgehoben (Revoke).

SQL> SELECT * FROM dba_role_privs WHERE GRANTEE = 'SCOTT';

GRANTEE      GRANTED_ROLE  DEFAULT_ROLE
-----
SCOTT        CONNECT       YES
SCOTT        RESOURCE      YES
```

Erneute Zuteilung von Rollen

Nach erneuter Zuteilung einer Rolle muss diese auch wieder explizit in die DEFAULT-Liste des Users aufgenommen werden, damit sie dann beim Logon automatisch aktiviert wird. Weil die Aufnahme einer Rolle in die Default-Liste eines Users davon abhängt, ob es sich um die erste oder eine spätere Zuteilung dieser Rolle handelt, sollte die korrekte Einstellung des DEFAULT-ROLE-Flags nach jeder Veränderung der Zugriffsrechte

eines Users durch Selektion der View dba_role_privs überprüft werden.