

Datenbank Architektur für Fortgeschrittene

Ausarbeitung 2: Zugriffssteuerung und Views

Daniel Gürber
Stefan Eggenschwiler

21.06.2013

Inhaltsverzeichnis

1	Oracle 11g	1
1.1	Vorbereitung	1
1.1.1	Einrichten User	1
1.2	Zugriffssteuerung mit User und Rollen	1
1.2.1	Tabellen erzeugen	1
1.2.2	View erstellen	1
1.2.3	Rollen definieren	2
1.2.4	Den Rollen Rechte zuweisen	2
1.2.5	Den User Rollen zuweisen	2
1.2.6	Überprüfung der Rechte der beiden Rollen	2
1.3	Zugriffsrechte: Objekt- und Systemrechte	3
1.3.1	Objektrechte	3
1.3.2	Systemrechte	3
1.4	Views	4
1.4.1	Rechte von Views	4
1.4.2	DDL-Änderungen an den Basistabellen	4
1.4.3	Updatable Views	5
1.4.4	WITH CHECK OPTION	6

1 Oracle 11g

1.1 Vorbereitung

1.1.1 Einrichten User

```
1 CREATE USER nutzer01 IDENTIFIED BY nutzer01;
2 CREATE USER nutzer02 IDENTIFIED BY nutzer02;
3
4 GRANT CREATE SESSION TO nutzer01;
5 GRANT CREATE SESSION TO nutzer02;
6
7 GRANT CREATE ROLE TO scott;
8 GRANT CREATE VIEW TO scott;
```

1.2 Zugriffssteuerung mit User und Rollen

1.2.1 Tabellen erzeugen

```
1 DROP TABLE klassen;
2 DROP TABLE studenten;
3
4 CREATE TABLE klassen(
5 k_id number(9),
6 k_bezeichnung VARCHAR2(20),
7 k_zimmer VARCHAR2(10),
8 k_server VARCHAR2(10));
9
10 CREATE TABLE studenten(
11 s_id number(9),
12 s_name VARCHAR2(10),
13 s_vname VARCHAR2(10),
14 s_tel VARCHAR2(20),
15 s_konto_stand NUMBER(9),
16 s_klasse NUMBER(9));
17
18
19 INSERT INTO klassen values ( 10, 'ia00', '3333', 'pluto');
20 INSERT INTO klassen values ( 20, 'ia01', '2222', 'saturn');
21
22 INSERT INTO studenten values( 101, 'meier', 'hans', '11111', 5000, 10);
23 INSERT INTO studenten values( 102, 'hirt', 'otto', '22222', -100, 10);
24 INSERT INTO studenten values( 103, 'kok', 'thomas', '33333', 1000, 20);
25 INSERT INTO studenten values( 104, 'guzman', 'anna', '44444', 3000, 20);
26 INSERT INTO studenten values( 105, 'lorch', 'felix', '45678', 7000, 20);
```

1.2.2 View erstellen

```
1 CREATE VIEW view1 AS
2 select s_name, s_vname, k_zimmer, k_server
3 FROM studenten, klassen
```

```
4 WHERE s_klasse = k_id
```

1.2.3 Rollen definieren

```
1 CREATE ROLE view1_verwalter;  
2 CREATE ROLE view1_nutzer;
```

1.2.4 Den Rollen Rechte zuweisen

```
1 GRANT INSERT,SELECT,UPDATE,DELETE ON studenten TO view1_verwalter;  
2 GRANT INSERT,SELECT,UPDATE,DELETE ON klassen TO view1_verwalter;
```

```
1 GRANT SELECT ON view1 TO view1_nutzer;
```

1.2.5 Den User Rollen zuweisen

```
1 GRANT view1_verwalter TO nutzer01;  
2 GRANT view1_nutzer TO nutzer02;
```

1.2.6 Überprüfung der Rechte der beiden Rollen

Was kann der Verwalter lesen und bearbeiten?

```
1 SELECT * FROM scott.studenten;  
2 INSERT INTO scott.studenten VALUES (106, 'peter', 'muster', 12345,2000,20);  
3 UPDATE scott.studenten SET s_tel = 54321 WHERE s_id = 106;  
4 DELETE FROM scott.studenten WHERE s_id = 106;  
5  
6 SELECT * FROM scott.klassen;  
7 INSERT INTO scott.klassen VALUES (30, 'ia02', 1111, 'uranus');  
8 UPDATE scott.klassen SET k_zimmer = 4444 WHERE k_id = 30;  
9 DELETE FROM scott.klassen WHERE k_id = 30;  
10  
11 SELECT * FROM scott.view1;  
12 INSERT INTO scott.view1 VALUES ('peter','muster',2222,'saturn');  
13 UPDATE scott.view1 SET s_name = 'kook' WHERE s_vname = 'thomas';  
14 DELETE FROM scott.view1 WHERE s_vname = 'thomas';
```

ORA-00942: Tabelle oder View nicht vorhanden

Was kann der Nutzer lesen und bearbeiten?

ORA-00942: Tabelle oder View nicht vorhanden ORA-01031: Nicht ausreichende Berechtigungen

1.3 Zugriffsrechte: Objekt- und Systemrechte

1.3.1 Objektrechte

Als scott:

```
1 CREATE VIEW view2 AS
2 select s_name, s_vname, k_zimmer, k_server
3 FROM studenten, klassen
4 WHERE s_klasse = k_id;
5
6 GRANT SELECT ON view2 TO nutzer01 WITH GRANT OPTION;
```

Als nutzer01:

```
1 GRANT SELECT ON scott view2 TO nutzer02;
```

Erfolgreich.

Als nutzer02:

```
1 SELECT * FROM scott view2;
```

Erfolgreich.

Als scott:

```
1 REVOKE SELECT ON view2 FROM nutzer01;
```

Als nutzer02:

```
1 SELECT * FROM scott view2;
```

ORA-00942: Tabelle oder View nicht vorhanden

1.3.2 Systemrechte

Als system:

```
1 REVOKE create session FROM nutzer01;
2 REVOKE create session FROM nutzer02;
```

ORA-01045: user STUDENT02 lacks CREATE SESSION privilege; logon denied.

Als system:

```
1 GRANT create session TO nutzer01 WITH ADMIN OPTION;
```

als nutzer01:

```
1 GRANT create session TO nutzer02;
```

Beide können Sessions erstellen.

Als system:

```
1 REVOKE create session FROM nutzer01;
```

nutzer02 kann IMMERNOCH Sessions erstellen. (Keine Kaskade)

1.4 Views

1.4.1 Rechte von Views

als system:

```
1 GRANT CREATE VIEW TO nutzer01;
```

als nutzer01:

```
1 CREATE VIEW cheat_view AS
2 SELECT * FROM scott.studenten
```

ORA-01031: Nicht ausreichende Berechtigungen

als system:

```
1 GRANT CREATE ANY VIEW TO nutzer01;
```

als nutzer01: ORA-01031: Nicht ausreichende Berechtigungen

als system:

```
1 GRANT INSERT,SELECT,UPDATE,DELETE ON scott.studenten TO nutzer01;
```

als nutzer01: erfolgreich

als nutzer01:

```
1 GRANT SELECT ON cheat_view TO nutzer02;
```

als nutzer02:

```
1 CREATE VIEW cheat_view AS
2 SELECT * FROM scott.studenten
```

ORA-01720: Berechtigungsoptionen für 'SCOTT.STUDENTEN' nicht vorhanden

1.4.2 DDL-Änderungen an den Basistabellen

als scott:

```
1 ALTER TABLE studenten ADD birthday TIMESTAMP;
```

```
1 SELECT * FROM view1;
```

Kein Problem, da view1 nicht beeinträchtigt wird.

```
1 ALTER TABLE studenten DROP COLUMN birthday;
```

```
1 ALTER TABLE studenten DROP COLUMN s_name;
```

```
1 SELECT * FROM view1;
```

ORA-04063: view "view1" enthält Fehler

```
1 ALTER TABLE studenten ADD s_name VARCHAR2(10);
```

Fixed.

1.4.3 Updatable Views

als scott:

```
1 CREATE VIEW view_distinct AS
2 SELECT DISTINCT s_vname
3 FROM studenten;
4
5 UPDATE view_distinct SET s_vname='ana' WHERE s_vname='anna';
```

ORA-01732: Datenmanipulationsoperation auf dieser View nicht zulässig

```
1 CREATE VIEW view_all AS
2 SELECT *
3 FROM studenten
4 INNER JOIN klassen ON s_klassen=k_id;
```

```
1 SELECT * FROM view_all;
2
3 UPDATE view_all SET s_name='muster' WHERE s_id=101;
```

ORA-01779: Kann keine Spalte, die einer Basistabelle zugewiesen wird, verändern

```
1 ALTER TABLE studenten
2 ADD CONSTRAINT STUDENT_PK PRIMARY KEY ( S_ID ) ENABLE;
3
4 ALTER TABLE klassen
5 ADD CONSTRAINT KLASSE_PK PRIMARY KEY ( K_ID ) ENABLE;
```

```
1 UPDATE view_all SET s_name='muster' WHERE s_id=101;
```

erfolgreich aktualisiert.

```
1 UPDATE view_all SET k_bezeichnung='test' WHERE k_id=10;
```

ORA-01779: Kann keine Spalte, die einer Basistabelle zugewiesen wird, verändern

1.4.4 WITH CHECK OPTION

```
1 CREATE VIEW v1 AS
2 SELECT *
3 FROM studenten
4 WHERE s_klasse = 20 WITH CHECK OPTION;
```

```
1 CREATE VIEW v2 AS
2 SELECT *
3 FROM v1
4 WHERE s_tel < 40000
```

```
1 INSERT INTO v2 VALUES (200, 'muster', 'peter', 40001, 2000, 20);
2 INSERT INTO v2 VALUES (201, 'muster', 'peter', 40001, 2000, 10);
```

ORA-01402: Verletzung der WHERE-Klausel einer View WITH CHECK OPTION

```
1 CREATE VIEW v3 AS
2 SELECT *
3 FROM v2
4 WHERE s_vname='peter' WITH CHECK OPTION;
```

```
1 INSERT INTO v3 VALUES (202, 'muster', 'thomas', 30000, 2000, 20);
```

ORA-01402: Verletzung der WHERE-Klausel einer View WITH CHECK OPTION

```
1 INSERT INTO v3 VALUES (202, 'muster', 'peter', 30000, 2000, 20);
```

Funktioniert.

```
1 INSERT INTO v3 VALUES (203, 'muster', 'thomas', 30000, 2000, 10);
```

ORA-01402: Verletzung der WHERE-Klausel einer View WITH CHECK OPTION

```
1 INSERT INTO v3 VALUES (204, 'muster', 'thomas', 40000, 2000, 20);
```

ORA-01402: Verletzung der WHERE-Klausel einer View WITH CHECK OPTION