



Database Security

Semester 2 / 1400-1401 (Spring 1401)

Instructor: Dr. Fakhrahmad

TA: Rahmani

Homework #3: Access Control in Databases

The learning objective of this homework is for you to gain hands-on experience with row level security (or somehow VPD) in Microsoft SQL Server.

VPD technology can restrict access to selected rows of tables. Oracle Virtual Private Databases (fine-grained access control) allows for the creation of policies that restrict table and row access at runtime. Oracle Virtual Private Database (VPD) enables you to create security policies to control database access at the row and column level. Essentially, Oracle Virtual Private Database adds a dynamic WHERE clause to a SQL statement that is issued against the table, view, or synonym to which an Oracle Virtual Private Database security policy was applied.

No matter how users connect to the protected table (via an application, a Web interface or SQL*Plus), the result is the same. There is no "application security problem" anymore, since the access policy is attached to the table, and cannot be bypassed.

CUST_FIRST_NAME	CUST_LAST_NAME	CUSTOMER_ID
Matthias	Hannah	106

ORDER_DATE	CUSTOMER_ID	ORDER_TOTAL
31-AUG-99 09.19.37.811132 AM	105	22150.1
20-MAR-96 05.18.21.862632 PM	106	5546.6
01-AUG-00 10.22.48.734526 AM	106	2075.2
31-AUG-99 08.53.06.008765 PM	107	70576.9

Example: A customer can only see his orders in the 'orders' table (below), when he is listed in the 'customers' table (above).

VPD in SQL Server. SQL Server lets you configure permissions at server level, database level, object level and even at column level. But what about row level security? Is there an equivalent feature (VPD) in SQL Server? I host a database application for different clients. Instead of creating a separate database for every client, can I have a single database, with only one set of tables to store all clients' information and let each client access only his/her data?

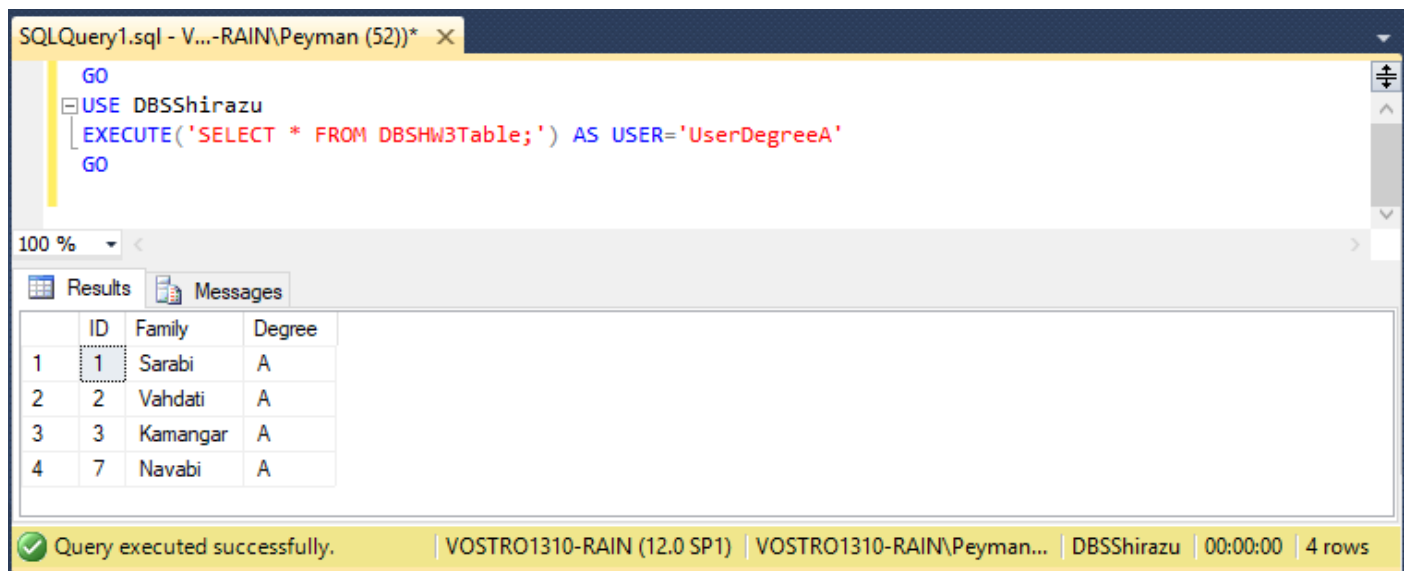
The answer is Row Level Security (RLS). RLS simplifies the design and coding of security in your application. RLS enables you to implement restrictions on data row access. For example ensuring that workers can access only those data rows that are pertinent to their department, or restricting a customer's data access to only the data relevant to their company.

The access restriction logic is located in the database tier rather than away from the data in another application tier. The database system applies the access restrictions every time that data access is attempted from any tier. This makes your security system more reliable and robust by reducing the surface area of your security system.

Assignment

We will create two groups (Degree A and B) data in the DBSHW3Table and then will restrict group manager to be able to see only their own group data (Degree A can see only Degree A students and vice versa)(In the attached database- create query).

Like the Following Figure:



The screenshot shows a SQL query window titled 'SQLQuery1.sql - V...-RAIN\Peyman (52)*'. The query is as follows:

```
GO
USE DBSShirazu
EXECUTE('SELECT * FROM DBSHW3Table;') AS USER='UserDegreeA'
GO
```

Below the query window, the 'Results' tab is active, displaying a table with 4 rows and 4 columns: ID, Family, Degree, and an unnamed column. The data is as follows:

	ID	Family	Degree
1	1	Sarabi	A
2	2	Vahdati	A
3	3	Kamangar	A
4	7	Navabi	A

At the bottom of the window, a status bar indicates: 'Query executed successfully. | VOSTRO1310-RAIN (12.0 SP1) | VOSTRO1310-RAIN\Peyman... | DBSShirazu | 00:00:00 | 4 rows'.

```
USE DBSecShiraz
GO
EXECUTE('Select * from HW3DBSecTable;') AS USER ='UserDegreeA'
GO
```

Please note that in the mentioned scenario, although we want to return all of the DBSHW3Table's records via the query (select * ...), but only the records which their Degree is 'A' are returned and this is achieved by row level security and restricting the user 'UserDegreeA' to appropriate role. (In this example 'UserDegreeA' has access to return only Degree 'A' record. We have another user which can return only Degree 'B' records while we select whole table to be returned). You should do like that. You should restrict group managers (based on degree –A and B) to view their own group data and only the DBA can view the whole table data. This means, one manager can see only three records and the other one can see 4 records in our table.

Hint: You can get help from this [link](#) to solve this homework.

Submission

You should submit the queries which you have used to achieve the mentioned goal with a self-descriptive report. We will run your queries to observe that two user which you have created can view only their assigned records (exactly like figure).

Please email your solutions till **June 3th, 2022** (1401/03/13) to peyman.rahmani@gmail.com with a subject and file name of the following format: DBS.HW#3.[Your Student ID].[Your full name].

If you have any questions, please feel free to contact me by email at peyman.rahmani@gmail.com.

Kind regards,

DB Sec. Team