DAL: Updating DB2 Database and Limiting User Access

Article Created: 20 April 1992
Article Last Reviewed: 18 June 1992

TOPIC ---

I'm using DAL and QMF (Query Management Facility, a mainframe application) to access DB2 on an IBM Mainframe. I allow the users read access only to the databases using QMF. We use DAL for client/server applications for Macintosh computers and PCs. The client/server applications require reading and updating the DB2 databases. To ensure that the information is entered through CICS, it creates a transaction. Then a program updates the DB2 databases with this transaction file. We use RACF security on the DB2 database.

The problem is that if we give users read and update access for client/server applications, they have read and update capabilities when they use QMF. With a client/server application, we can limit user access to specific tables, but with QMF a user with update capabilities can cause problems.

Here are some of the things we've tried:

1) We set a different SQL ID for a query to a group with fewer rights than the individual. This didn't work because the DB2 remembers the individual rights as well as inheriting the group rights.

2) We tried to hide tables from QMF users, but the users soon found them.

3) We created a view for the table with read-only access and hid the name, but users soon found this too. IBM said we couldn't easily hide files from QMF.

4) We created a view for each individual. But it would be difficult to manage now, and impossible if we transition to a client/server environment.

5) We set different security with DAL and QMF to DB2. This didn't work.

6) We wrote a flat file with DAL (or something like Mitem), and had an IBM

program apply the changes to the DB2 databases. But others could still trash the flat file.

DISCUSSION ----------

DB2 looks at the USERID to determine access to its databases. The USERID is maintained in RACF; the corresponding access to DB2 is granted within DB2 itself. Thus, when DB2 gets some kind of request (read, update, and so on), it verifies the capabilities that were granted against the USERID that submitted the request.

As you discovered, it doesn't matter whether the request comes from DAL, QMF, SPUFI, and so on. Unfortunately, since the security system (RACF) is the same, and you're using the same database, there is no way for DB2 to differentiate between the various methods of gaining access to its databases.

The problem here is that you gave users update access to the database indirectly via the transaction file. Users can update the transaction file with the same ID, and access the database in read-only mode.

With DAL, you let the users bypass the transaction file and go directly to the database. We don't see how you can use the same ID now to update with DAL, and give read-only privileges with QMF.

The equivalent of the previous model would be number 6 in your list. The users are given update access to a "transaction file," and a program will read that transaction file to update the DB2 database. That same ID still only has read-only access to DB2. We understand the fear of users trashing the transaction file, but you can build the same validation criteria from the CICS program into the DAL applications.

Just as a point of clarification, this isn't a DAL bug, nor would there be any way to rectify this situation in a future release. It's a host limitation.

Keywords: <None>

==========

19960215 11:05:19.00
Tech Info Library Article Number: 10136