ABS Tech Note: DAL25 DB2 and Secondary AUTHIDs (12/92)

Revised: 9/2/93
Security: Everyone

ABS Tech Note: DAL25 DB2 and Secondary AUTHIDs (12/92)

==========

Article Created: 23 December 1992

TOPIC

This Tech Note explains what actions are necessary to implement DAL using secondary AUTHIDs, a facility of DB2. Secondary AUTHIDs are utilized in conjunction with a system resource security package (for example, RACF) to simplify access to tables under DB2.

DISCUSSION

Information on DB2 modifications necessary to support secondary AUTHIDs should be obtained from the relevant IBM publications. Similarly, more information on security procedures and strategies (such as GROUP definitions with RACF) can be found in the related IBM or third-party publications.

Why secondary AUTHIDs might be used

Secondary AUTHIDs are generally implemented in large IS environments where there are many users that require access to multiple tables in DB2. Although a GRANT could be done for each user/table combination, it is easier to assign users to different groups within the security software and then GRANT table access to the groups, as opposed to the users. For example, there might be fifteen users who all work in the accounting department that require identical access to a DB2 table. All fifteen users can be 'connected' to a group named 'ACTG' within RACF and then the necessary access can be GRANTed (using SPUFI or other DB2 utilities) to 'ACTG'. This way, if more people are added to the accounting department, they only have to be 'connected' to the group within RACF; no other GRANT would be necessary.

How DAL implements secondary AUTHIDs

Since DAL is not used for GRANTing access to tables or performing any system security functions, it can only take advantage of those accesses that are already in place. To do so, the database open must be performed with the 'as user <username>' option. This should be done right after opening the DBMS. An example is shown on the next page.

The DBMS and database are opened without usage of secondary AUTHIDs. The USERID that was utilized to logon to the DAL MVS/VTAM Server is 'RJOHNSO'.

```
DAL> open DB2 DBMS;
DAL> open database 'DB2T' ;
```

A selection is performed against a nonexistent table. The error generated indicates that the USERID was prepended to the query.

```
DAL> select * from foo;
••••Remote DAL Error••••
•Error:
undefined table name in database (-10204) table not found in database
"network", line 1 :
DSNT408I SQLCODE = -204, ERROR:  RJOHNSO.FOO IS AN UNDEFINED NAME
DSNT415I SQLERRP = DSNXOCA SQL PROCEDURE DETECTING ERROR
DSNT416I SQLERRD = 500  0  0  1  0  0 SQL DIAGNOSTIC INFORMATION
```

The database is closed and reopened using a secondary AUTHID that either does not exist or of which 'RJOHNSO' is not a member.

```
DAL> close database;
DAL> open database 'DB2T' as user 'DALPROD' ;
••••Remote DAL Error••••
•Error:
database not opened (-923) DB2T
"network", line 1 :
DSNT408I SQLCODE = -553, ERROR:  DALPROD SPECIFIED IS NOT ONE OF THE
VALID AUTHORIZATION IDS
DSNT415I SQLERRP = DSNXRST SQL PROCEDURE DETECTING ERROR
```

The database is now opened using a valid secondary AUTHID, and a selection is again performed against a nonexistent table. This time, however, the error message indicates that the secondary AUTHID is now prepended to all queries.

```
DAL> open database 'DB2T' as user 'DALTEST' ;
DAL> select * from foo;
••••Remote DAL Error••••
•Error: undefined table name in database (-10204) table not found in
database
"network", line 1 :
DSNT408I SQLCODE = -204, ERROR:  DALTEST.FOO IS AN UNDEFINED NAME
DSNT415I SQLERRP = DSNXOCA SQL PROCEDURE DETECTING ERROR
DSNT416I SQLERRD = 500  0  0  1  0  0 SQL DIAGNOSTIC INFORMATION
```

If the table 'DALTEST.FOO' actually existed, a query would have been

performed against it even though the USERID that logged on to the server is 'RJOHNSO'.

Verifying DB2 service levels

If V2.2.0 of DB2 is being used, it is important to verify the application of a PTF from IBM. This PTF, number UN23430, is specifically related to the use of secondary AUTHIDs with DB2. Contact your authorized IBM service representative for more information.

Tech Info Library Article Number:11651