DB2 Security
A Common Language for a Common Goal

One of the best aspects of the IDUG user community is our willingness to share knowledge. From a technical perspective, our common commitment to contributing valuable tips has served us well. But, until recently, the implementation effort to securely protect our z/OS databases and our LUW databases typically traveled on different paths. Other than sharing the concepts of the basic security principles, database professionals had little in the way of common functionality or a common language when it came to creating a robust security approach. Despite our willingness to share, there was no Rosetta Stone for the translation of DB2 z/OS to DB2 LUW security concepts or vice versa. Fortunately with DB2 10 z/OS and DB2 9.7 LUW, we have made a significant leap toward that goal of a common security language.

Common Ground

Two of the basic foundational tenants of security are enforcing 'least privilege' and ensuring 'separation of duties.' Using authorities that are designed only for the specific task at hand helps enforce least privilege. Separating the administration and security responsibilities between different individuals and/or groups helps enforce separation of duties. Fortunately, there are new DB2 authorities that allow us to easily meet both these security goals.

DB2 Security Boss -- SECADM

Both DB2 LUW and DB2 z/OS now provide the SECADM authority. In previous versions of DB2, security related tasks such as assigning permissions often required the use of one of the high level DB2 administration authorities. With security breaches becoming seemingly a daily occurrence, organizations need the ability to provide a hands-off approach between the high level administration authorities, such as those held by the SYSADM, and those tasks that are specific to security protections. With the introduction of the SECADM authority, security responsibility can now be separated from administration responsibility. Another security benefit is that the SECADM authority does not inherently provide the holder with the ability to read data.

More Alike, Less Different

We are all too familiar with that constant trade-off between wanting to keep our security set-up strong while allowing enough access to keep the business running. Because the need to run the business typically is the number one priority, over-granting privileges was the end result when conflicts between the two goals arose. To prevent the need to escalate permissions, granular authorities have been introduced to easily solve the most common of these dilemmas. For example, the long acknowledged approach of entrusting SYSADM authority to multiple individuals just to make sure they could accomplish all tasks is no longer necessary.

Some Birds of a Feather

DATAACCESS is one of the new granular authorities and, just as the name implies, allows holders to access the data without also holding a higher level authority. For DB2 z/OS, DATAACCESS authority allows the holder to access and update data in user tables, views, and materialized query tables. It also allows the holder to execute plans, packages, functions, and procedures. For DB2 LUW, DATAACCESS provides LOAD authority, SELECT, INSERT, UPDATE and DELETE, as well as EXECUTE on packages and routines (except audit routines). DATAACCESS authority allows the SECADM to delegate appropriately without having to over-grant in order to provide appropriate access to the data.

SQLADM authority is now available for both DB2 z/OS and DB2 LUW. SQLADM includes the ability to run EXPLAINs and RUNSTATS. It provides the ability to EXECUTE system defined routines (except audit routines for DB2 LUW). This authority is designed to allow the holder to monitor and tune SQL statements without also allowing access to the data.

ACCESSCTRL is another new authority. ACCESSCTRL allows the holder to grant and revoke privileges. This level of authority is particularly useful for certain software product's user ids that manage permissions via the application.

DB2 ROLEs are now available for ease of security administration. Since Db2 9.5, DB2 LUW SECADMs have used roles quite effectively to easily manage users and their associated authorities. Db2 for z/OS DBA also have this capability as of Version 9.

DB2 Security, Let's Discuss!

There is much more to learn about DB2 Security and the full range of authorities that are now available, but with this new ability to communicate security knowledge based on common terms and shared approaches, we can now leverage our IDUG user community to help each other succeed in protecting ***all*** our DB2 databases.

BY: CRAIG S. MULLINS & REBECCA BOND, CISSP

Craig S. Mullins is president and principal consultant of Mullins Consulting, Inc., an IBM Champion, and author of two books: "DB2 Developer's Guide" and "Database Administration: The Complete Guide to Practices and Procedures." More information available at www.craigsmullins.com.

Rebecca Bond, CISSP (aka the DB2Locksmith) is an IBM Champion and author of the book "Understanding DB2 9 Security".