December 2011 / January 2012

zData Perspectives

Security Improvements in DB2 10 for z/OS

by Craig S. Mullins

In this day and age of database breaches, regulatory compliance and hacking, improved security is a must. Thankfully, DB2 10 adds multiple improvements for securing the data in your databases.

Perhaps the most important improvement is the introduction of the SECADM authorization, which can be assigned to an authid or role. By using SECADM, you can separately ascribe the privileges needed to manage and access DB2 security privileges and authorization without requiring any data or other system privileges to be granted. Separation of duties, and the flexibility to assign the least possible level of privileges necessary to accomplish tasks, such as delivered by SECADM, are key requirements of many regulations and security

There are two granular options that can be set when granting system DBADM authority: ACCESSCTRL and DATAACCESS. You can specify whether the system DBADM designation is to be granted with or without either. Specifying WITH ACCESSCTRL allows system DBADM to grant all authorities and privileges except system DBADM, DATAACCESS, ACCESSCTRL authorities, and privileges on security-related objects. Specifying WITH DATAACCESS allows the system DBADM to access data in all user tables, views, and materialized query tables in a DB2 subsystem and allows the user to execute plans, packages, functions, and procedures.

Many security regulations and compliance initiatives favor prohibiting high-level authorities such as SYSADM and/or DBADM being conferred in conjunction with data access

are key requirements of many regulations and security compliance objectives. Prior to DB2 10, auditors have had issues with DB2's authorization scheme because it lacked such separation.

Traditionally, SYSADM authority was required for granting and revoking DB2 authorization and privileges. But with the advent of SECADM, you have the option to minimize usage of SYSADM. Given the high level of privileges, the stronger approach from a security perspective is to make full use of the SECADM functionality to provide the greatest level of security control.

A security administrator (that is, a role or authid assigned as SECADM) can perform security- and authorization-related tasks, including issuing GRANT and REVOKE statements, and managing ROLEs, TRUSTED CONTEXTs, row permissions, column mask, and audit policies. Security administrators also will have access to the DB2 Catalog and can issue START, STOP, and DISPLAY TRACE commands.

A DSNZPARM named SEPARATE_SECURITY has been provided to define the role of SECADM. When SEPARATE_SECURITY is set to YES, only a security administrator can perform the security tasks associated with SECADM. That means SYSADM and any other users granted security privileges will lose authorization-related abilities. Use of SECADM is optional. Assigning SEPARATE_SECURITY to NO causes DB2 to behave as in previous releases with no security administrator capability.

Additionally, DB2 10 delivers two new group-level privileges to enable more granular and functional security support for DB2 administrators. The system DBADM authority is for DBAs at shops that are looking to minimize SYSADM usage, and SQLADM authority is for users who focus predominantly on performance-related issues.

System DBADM authority can be assigned to enable a user to DBADM being conferred in conjunction with data access privileges. Keeping administrative and data access separate is another control designed to protect user data.

DB2 10 also introduces the ability to grant the SQLADM privilege for DBAs who work as SQL performance specialists. The SQLADM privilege can be granted to authids and roles, indicating that the user can perform SQL and SQL performance management-related actions without requiring any additional privileges. These abilities include EXPLAIN, RUNSTATS, PREPARE, DESCRIBE TABLE, and BIND-related activities.

Also new as of DB2 10 is the EXPLAIN privilege, which allows a user to perform explain-related activities without having access to data. EXPLAIN authority is particularly useful for performance analysts responsible for tuning and optimizing SQL, especially in a production environment where operational data should be accessed only by authorized business users. It's also quite useful for managing the performance of dynamic SQL, where SYSADM authority was previously the only way to EXPLAIN the SQL in the dynamic statement cache.

Indeed, there are many new security-related features added to DB2 10. I've summarized most of the major ones here, but there are others, such as the ability to configure how, or if cascading revokes should be permitted, row and column access controls, data masking, and improved data auditing capabilities. Take the time to review these new security features as you migrate your DB2 subsystems to 10.

manage all objects within a DB2 subsystem, but without necessarily being able to access data. This authority can be granted to an authid or role. By using system DBA authority judiciously, the need for SYSADM authority can be minimized. So, as of DB2 10, DBADM security can be granted at the system level or at a database-by-database level as in all past versions of DB2.

From zJournal, December 2011 / January 2012.