RACF AND RBAC

September 2015

ROLE BASED ACCESS CONTROL (RBAC): Prior to RBAC, strict adherence to the principle of "least necessary privilege" was regarded as the "best-practice" for the administration of computer security. Each user was only to be given as much access authority as he or she individually required. However, custom tailoring access permissions for each individual user proved to be time consuming and error prone. It was especially cumbersome and complex in large organizations with many thousands of users.

The concept of RBAC emerged in 1992 as a way to improve the efficiency and accuracy of security administration. As stated by the National Institute of Standards and Technology: "With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles." (See http://csrc.nist.gov/rbac/ for more on RBAC.) RBAC is the dominant model for administering access controls today.

RESOURCE ACCESS CONTROL FACILITY (RACF): RACF is ideally suited to RBAC because its design organizes users into groups. A group is simply a collection of users with similar access needs, which in essence constitutes a role. RACF allows a user to be connected (i.e., joined) to multiple groups. RACF groups offer considerable flexibility in designing an RBAC structure and can be created to correspond to organizational business units, staff positions, job functions, and even specific tasks.

Resources such as transactions can also be organized into groups through the use of resource grouping profiles. Access permitted to such profiles applies to all the resources in the group. Grouping profiles are most commonly used with CICS and IMS where sets of transactions are associated with specific roles. RBAC group design and resource grouping profile design go hand in hand.

The design of RBAC in RACF requires considerable thought to avoid creating a complex, confusing group architecture that is difficult to administer. Here are characteristics of a well-designed implementation.

- A group naming convention and hierarchical structure are defined that ensure groups used for RBAC are recognizable and the responsible business unit is identifiable.
- Groups used for RBAC are not used for other purposes (e.g., resource owning).
- Each ID is connected to a relatively small number of RBAC groups.
- Most business units have relatively few RBAC groups.
- IDs assigned to processes such as system started tasks, application batch jobs, and data transfer are not connected to RBAC groups containing IDs assigned to people. People and processes ordinarily have distinctly different access requirements.
- People are permitted access via RBAC groups rather than having access permitted directly to their IDs. (Generally, the opposite is true for process IDs.)
- IDs assigned to vendors, consultants, external auditors, and other non-employees are connected to groups whose names denote both their status and the business unit they serve.
- The administration of RACF users and groups is automated via software which cross-references and processes RACF and Human Resources (HR) data. This greatly improves administration efficiency and accuracy. A good RBAC design facilitates automation.

Aside from improving administrative effectiveness, a well-designed and implemented RBAC structure often boosts RACF processing performance by reducing both the number of groups to which a user is connected and the number of permissions in resource profile access lists.

Contact RSH Consulting for assistance with designing, implementing, and automating RBAC in RACF.

RSH CONSULTING, INC.
29 Caroline Park, Newton, Massachusetts 02468
www.rshconsulting.com ■ 617-969-9050

RACF PROFESSIONAL SERVICES