RACF - An Overview

Version 2

April 2019

Introduction to z/OS & RACF

z/OS is an IBM general-purpose, 64-bit operating system for IBM's zSeries mainframe computers. The “z” denotes “zero downtime” to emphasize the resilience and dependability of both the hardware and software.

z/OS services provide interactive on-line user interfaces and batch processing in support of business-critical applications. They include Time Sharing Option (TSO), Customer Information Control System (CICS), TCP/IP, Database 2 (DB2), Job Entry Subsystem (JES) , FTP, Information Management System (IMS), and z/OS Unix.

RACF (Resource Access Control Facility) is IBM's software product that provides security services for z/OS. It performs the following functions:

- Verifies a user's identity at logon using a password, a phrase of up to 100 characters, a digital certificate, or Multi-Factor Authentication (MFA) token+PIN,
- Determines whether a user is permitted to access a dataset (i.e., file) or resource,
- Logs a user's activities, and
- Decides if a user can administer security controls.

Background

z/OS is the latest iteration in a series of operating systems dating back to 1964. With IBM's emphasis on "backward compatibility," z/OS supports business applications written decades ago under prior versions of the operating system to maximize customer software ROI. To maintain compatibility, certain limitations in the system architecture have had to be retained, such as 8-character USERIDs and 44-character dataset names.

Early versions of the operating system were designed during information technology’s infancy and well before security was a major consideration. Initial security features were rudimentary (e.g., dataset passwords). To meet the evolving security needs of more modern systems, IBM developed RACF, first released in 1976.

To compensate for the lack of security functionality in early versions of both the operating system and RACF, developers incorporated security controls of their own design into their software products. Such controls became known as “internal” security. Over time RACF improved its functionality and performance, and most products added options to transfer their internal controls to “external” security, i.e., RACF. Nonetheless, many products continue to rely on internal security by default. One of the many challenges faced in properly securing a z/OS system is ensuring all software products are configured to use RACF to govern security.

RACF Components

RACF consists of a database and an extensive set of programs that manage and query it.

The RACF database includes a Primary dataset(s) and optional on-line Backup dataset(s). The Primary is used for security decisions. The Backup is for rapid recovery.

The database contains records called "Profiles" that are used to govern security. There are four kinds of profiles.

- GROUP - A Group profile exists for every group and contains a group's attributes and user members, a.k.a. "Connects" in RACF terms. Groups are used to implement Role-Based Access Controls (RBAC).
- USER - A User profile exists for every logon USERID and contains a user's description, attributes, one-way encrypted password/phrase, and group connects.
- DATASET - A Dataset profile defines protection for datasets and can either be Discrete, which protects a single, specific dataset, or Generic, which uses masking characters to protect a set of like-named datasets (e.g., SYS1.RACF*.**). A Dataset profile contains control options, logging specifications, and a list of the users and groups permitted access.
- GENERAL RESOURCE - A General Resource profile defines protection for entities such as programs, commands, functions, and transactions. A General Resource profile can be Discrete, Generic, or Grouping, the latter of which protects a set of resources with dissimilar names. A General Resource profile always specifies a "Class'" which identifies the type of resource (e.g., OPERCMDS for operator commands). A General Resource profile contains control options, logging specifications, and a list of the users and groups permitted access.

RACF programs perform a variety of functions. Some do the security decision-making. These programs are loaded as an integral component of z/OS during system start-up, a.k.a. Initial Program Load (IPL).

RACF commands are programs that create, change, and delete profiles. Commands for User profiles are ADDUSER, ALTUSER, DELUSER and LISTUSER. Similar commands exist for the other profiles.

SETROPTS is a command used to list and set global RACF options such as the minimum password length. RACF stores options in the first record of the database.

Programs known as utilities perform maintenance tasks such as backing up the database. Utility DSMON (Data Security Monitor) generates RACF and z/OS security control reports. The database unload utility creates a text copy of the database, excluding passwords, for use with custom report-generating software tools.

RACF's behavior can be customized to meet unique requirements by coding and installing programs known as Exits. Exits can, for example, enforce local password rules or allow internal auditors to read any dataset. Improperly coded exits can create vulnerabilities.

RACF in Action

RACF does not control access. It merely responds to security questions asked by "resource managers" (i.e., system services and authorized software products). When a user enters a USERID and password to log into TSO, TSO asks RACF "Is this a valid user?" RACF searches for a matching user profile, validates the password, and answers YES or NO. Likewise, when a user enters CICS transaction PAY1, CICS asks RACF "Is the user allowed to execute this transaction?" RACF searches for the profile that protects PAY1, checks the permissions, and replies YES, NO, or UNPROTECTED. In formulating a reply, RACF first checks the profile's access list to see if the user, any of the user's groups, or ID * (all RACF users) are allowed access. RACF then checks the profile's default Universal Access (UACC) permission and whether it is in WARNING (test mode). Upon receiving RACF's reply, the resource manager, not RACF, decides whether to grant or deny access.

UNPROTECTED means either the resource class was not active or no profile was found. Access is often granted. To fully secure z/OS, resource classes for all software products must be activated and carefully crafted, comprehensive sets of profiles must be defined.

High-Level Access Authorities

The attribute OPERATIONS grants a user full access to resources within certain classes, including DATASET, mostly to facilitate data management. Few users should be given OPERATIONS, and its use should be logged.

PRIVILEGED and TRUSTED authorities both grant a system service unlimited access to all resources, but only TRUSTED can be logged. No service should be given PRIVILEGED. TRUSTED should only be given to critical system services specifically designated by IBM.

Logging & Monitoring

The RACF term for logging is "Auditing." SETROPTS and profile auditing options together determine whether an event is logged. In general, most access violations are logged; whereas, most authorized access events are not. Many SETROPTS options designed to ensure comprehensive monitoring are disabled by default.

RACF uses the z/OS logging service SMF (System Management Facilities) to record events. RACF's SMF unload utility creates a text copy of SMF records for use with custom report-generating software tools.

Security Administration

RACF provides a number of options to govern who can view and change RACF controls. SPECIAL authority enables RACF Administrators to create or change any profile and modify most SETROPTS options. AUDITOR allows auditors and administrators to view any profile and change SETROPTS audit options. ROAUDIT, new in z/OS 2.2, allows users to view everything but not make changes. These authorities can optionally be limited in scope to specific groups. Special-purpose profiles can be defined to delegate password reset authority to help desk staff. Other options can further delegate and decentralize security administration.

RACF + Skill + Effort = Secure z/OS

RACF can provide a z/OS system with near ironclad security provided it is fully and properly implemented and maintained. This requires activating RACF options, activating resource classes, defining profiles, and turning on external security options in other software products. It also requires a well-designed group structure and profile naming convention to facilitate the orderly and efficient administration of RACF. This is no small undertaking and is usually very complex. Considerable effort and advanced technical skills are required to attain and sustain a high level of protection.

RSH Consulting, Inc.

RSH Consulting is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and technical training. RSH is world renowned for its generous contributions to the RACF community in supporting RACF User Groups, publishing tips, and posting valuable reference materials on its website.

Special thanks to Ed Norris, Russ Hardgrove, Dave Bell, Joel Tilton, and others for reviewing drafts of this document.

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

RACF
PROFESSIONAL SERVICES