

RACF AUDIT GUIDANCE

INTRODUCTION: Since RACF was first introduced in 1976, its security capabilities along with those of the IBM mainframe operating system (currently known as z/OS) have been progressively enhanced. New control features and functionality have been added while earlier control options have faded in importance or become obsolete altogether. The purpose of this document is to inform RACF auditors of some control options and issues that may no longer be of significant concern or merit an audit finding.

SETROPTS JES(XBMALLRACF) & EXECUTION BATCH MONITORS (XBM): A desirable RACF control objective is ensuring all batch work entering the system has proper RACF identification. Therefore, the RACF SETROPTS option JES(BATCHALLRACF) should be active in all installations as it requires user identification for all normal batch work. The same is not necessarily true for JES(XBMALLRACF). This option only addresses Execution Batch Monitors (XBM), and XBMs are very rarely used. The existence of an XBM is determined by examining the initialization parameters associated with JES2 (a.k.a. JESPARMS). The keyword XBM=*procedure-name* on a JOBCLASS statement indicates an XBM is in use. If this keyword is not coded on any JOBCLASS statements, no XBMs are being used and SETROPTS JES(XBMALLRACF) need not be active. It is acceptable to encourage the auditee to activate it simply for completeness and consistency; however, if XBMs are not being used, no audit finding should be issued. (Reference: z/OS JES2 Initialization and Tuning Reference)

SETROPTS JES(EARLYVERIFY): In releases of JES prior to 3.1.3 (before 1990), the USERID and password on a batch job would not be verified until job execution. This could occur quite some time after the job was initially submitted. Someone with the ability and authority to inspect JES memory could discover the password during that period of time. To address this concern, RACF introduced JES(EARLYVERIFY) to force the password check at job submission time so that the password would not need to be retained. Beginning with JES release 3.1.3, this early verification process became automatic. The JES(EARLYVERIFY) option is now meaningless, and its status should not trigger an audit finding. (Reference: z/OS Security Server RACF Security Administrator's Guide)

PROGRAM AMASPZAP (A.K.A. SUPERZAP OR SPZAP): SUPERZAP is a service aid utility that can be used to fix a program load module or correct a Direct Access Storage Device (DASD) Volume Table of Contents (VTOC) entry. Originally, it would modify programs and VTOCs without checking for RACF authorization. Back then, a dataset's protection was enforced by the VTOC RACF-Indicated bit which prompted the checking of a Discrete profile. The ability to turn this bit off with SUPERZAP was a significant security concern, and consequently, the protection and control of SUPERZAP was once a major issue. This is no longer the case. SUPERZAP now runs in "Problem" state (as opposed to "Supervisor" state), and its use is subject to normal RACF controls. To change a program, the user must have at least UPDATE access to the library where the target program resides. To update a VTOC, the user must have at least UPDATE access to the DASDVOL or GDASDVOL profile guarding the DASD volume (but only if such a profile exists) and the console operator must respond to a message permitting the action. Furthermore, in today's RACF environments, datasets are almost always protected by Generic profiles rather than Discrete ones, and the RACF-Indicated bit is superfluous. Hence, restricting the use of SUPERZAP is no longer a necessity. (Reference: z/OS MVS Diagnosis: Tools and Service Aids)

SETROPTS ADSP (AUTOMATIC DATASET PROTECTION): Prior to the introduction of Generic profiles in the mid-1980s, it was necessary to define a Discrete profile for each dataset in order to protect it. The ADSP option was introduced back then to ensure a Discrete profile was automatically defined each time a dataset was created. When SETROPTS ADSP was active and a user also had the ADSP attribute, every time the user created a dataset, RACF created a companion Discrete profile. Nowadays datasets are almost always protected by Generic profiles, and there is no need, nor is it generally desirable, to define a Discrete profile for datasets. Hence, it is perfectly acceptable for this option to be turned off. In fact, IBM recommends it be deactivated. (Reference: z/OS Security Server RACF Security Administrator's Guide)

IBMUSER: IBMUSER is the default USERID that comes with RACF. It is intended to be used to create the first few IDs with SPECIAL authority (i.e., Security Administrator IDs) when RACF is first implemented and then be REVOKED (i.e., deactivated) immediately thereafter. Installations wishing to fully emasculate this ID can optionally remove its SPECIAL and OPERATIONS authority and also make

RACF Audit Guidance

it RESTRICTED and PROTECTED. This ID, however, should not be deleted. If deleted, RACF will recreate it during an upgrade. The recreated ID will have the default password assigned and will not be REVOKED, making it exposed for misuse by anyone who knows the default password. (Reference: z/OS Security Server RACF Security Administrator's Guide)

PROGRAM PROPERTIES TABLE (PPT): The PPT is used to assign special authorities to specific programs executed from Authorized Program Facility (APF) libraries. These authorities include the ability to execute with a System Key (allowing access to operating system software in memory) and Bypass Password Protection (circumventing RACF dataset access authorization checking). IBM includes a substantial set of PPT entries with the operating system. Installations can add their own entries by defining them in a system parameter library (a.k.a. PARMLIB) in a member named SCHEDxx, where 'xx' is determined by other operating system parameters. The RACF DSMON utility provides an optional report listing the contents of the current PPT. The IBM-provided entries include programs that may not be applicable to every system (e.g., IATINTK (JES3)). There is no harm in having these dormant entries in the PPT, and removing them does nothing to improve system security. Any user with UPDATE or greater access to an APF-authorized library could misuse any PPT entry, dormant or not, simply by creating and executing an identically named program. Restricting UPDATE access to APF-authorized libraries is the only meaningful form of protection. (Reference: z/OS MVS Initialization and Tuning Reference)

ADDITIONAL RACF AUDIT INFORMATION: If you have questions concerning this document or require training or assistance with conducting an audit of RACF, contact RSH Consulting, Inc. at 617-969-9050 or info@rshconsulting.com. Additional information is available at www.rshconsulting.com.