RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 12
Issue 2
April
2018

IRRRID00 EXIT Statement

The Remove ID utility IRRRID00 creates a CLIST with commands such as PERMIT DELETE to remove references to obsolete IDs from the RACF database. If a dataset or general resource profile happens to have a qualifier matching an obsolete ID, IRRRID00 also generates an RDELETE or a DELDSD command to delete the profile. Such a profile may still be valid, so further evaluation is required before deleting it. To prevent the delete commands from being executed accidentally, IRRRID00 places them after a CLIST EXIT statement. EXIT halts further execution of the commands, ***but only if the commands are executed as a CLIST***. If, instead, the commands are executed via TSO batch DD SYSTSIN, EXIT is ignored and all the commands will be executed.

ISPF Unix Violations Not logged

ISPF and Unix-related REXX EXECs such as OEDIT which invoke ISPF use the callable service 'access' to check a user's authority before opening the requested file or directory. If the user does not have sufficient authority, a message is displayed at the terminal indicating access is not authorized, and no open is performed. Consequently, no SMF record is written to log the attempted unauthorized access. This "feature" could enable someone to surreptitiously probe the Unix file system looking for unprotected sensitive data or configuration information that might reveal a security weakness.

Special thanks to Bruce Wells of IBM for his assistance relative to analyzing this issue.

EXECUTE Access Permission

EXECUTE permission can be used to allow a user to execute a program containing confidential data (e.g., password) or proprietary code without being able to read, copy, or dump the program contents.

To implement execute-only program control effectively, identify all datasets where copies of the program or its source code reside and ensure their corresponding DATASET profiles strictly limit READ access. Then permit users EXECUTE access only to the profile for the dataset containing the copy of the program you want them to execute. We recommend using a fully-qualified generic profile for this purpose.

If the program's dataset is in the LINKLIST concatenation, define a PROGRAM profile for the program and permit users EXECUTE access to this profile. For added safety, always define a PROGRAM profile for the program just in case the dataset is later added to the LINKLIST.

Be advised that users who execute a program from a dataset to which they only have EXECUTE access may generate a dataset access violation with INTENT(READ) ALLOWED(EXECUTE) if the protecting DATASET profile has AUDIT(ALL) or if the user has UAUDIT. The program will still execute. Such violations can be ignored.

Attempts to read, copy, or dump a program when only EXECUTE access is permitted will fail. Symptoms include SA00, S306, S806, and S913 ABENDs, system message CSV025I, or a RACF message in the range of ICH419I to ICH429I.

Started Task Logon Logging

Started Task logons result in the generation of an SMF Type 30 - Subtype 1 "Common Address Space Work - Initiation" record unless the task is started before SMF is initialized, in which case no record is generated. Setting TRACE(YES) on STARTED profiles can help identify such logons.

CFIELD and CFDEF Deletion Affects CSDATA Field Admin

RACF will allow you to delete either a custom field CFIELD profile or its associated CFDEF segment even though the corresponding field is defined in user or group CSDATA segments. Once the RACF Dynamic Parsing Table has been updated

RACF is a Trademark of the International Business Machines Corporation

following such an action, RACF will not allow you to change or delete the custom field value in any CSDATA segments. The field still appears when you list a CSDATA segment, but the field's former LISTHEAD title will be missing. To administer a CSDATA field whose CFIELD profile or CFDEF segment were deleted, recreate the profile and/or segment and update the table with IRRDPI00.

Long Commands Trip Up IRRADU00

SMF unload IRRADU00 abends if it encounters a RACF command that, along with all its operands, is longer than 1,024 characters. (APAR OA52357)

EOS and PPRC

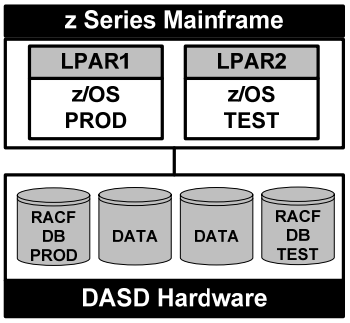
The performance of Erase-On-Scratch (EOS) was greatly improved in z/OS 2.1 and even more so in z/OS 2.2. If you use Peer-to-Peer Remote Copy (PPRC) to mirror disks, to further improve performance apply APAR OA46511 and then set new PARMLIB DEVSUPxx option EOSV2 to YES.

Auditors: DASD Sharing Affects Audit Scope

Most z/OS data resides on Direct Access Storage Devices (DASD or disk). DASD is organized into volumes (analogous to PC disk partitions), each with a unique volume-serial identifier (VOLSER). Data is stored in datasets (i.e., files) on these volumes. A typical mainframe environment has hundreds of volumes. Hardware devices connect banks of DASD volumes to one or more zSeries mainframe computers.

A zSeries mainframe has virtualization software in its microcode that enables it to run multiple instances of z/OS, each in its own Logical Partition (LPAR). Each of these z/OS systems is capable of accessing datasets on any volume connected to the computer. It is merely a matter of configuring a z/OS system to recognize the volume is connected and make it accessible with a VARY ONLINE command. Individual volumes are often shared by multiple z/OS systems, even by those on separate zSeries computers.

Each z/OS system is configured to use a specific RACF database. A system can have its own database or share one with other z/OS systems. Each RACF database has options and profiles specifying how every dataset is protected. When a DASD volume is shared by z/OS systems that use different RACF databases, there may be inconsistencies in how the volume's datasets are protected by each of the RACF databases.



When auditing RACF protection for production datasets, first determine which z/OS systems are configured to share the DASD volumes where these datasets reside. Next, identify the RACF database(s) used by these various systems. Then compare and evaluate the protections for the datasets in each of these RACF databases. This may require a review of RACF protections in non-production z/OS systems such as Test or QA.

Note that a similar analysis may be required for data stored on tape if the tapes can be accessed from multiple z/OS systems.

For more on auditing RACF, attend our "RACF Audit & Compliance Roadmap" course.

RSH News

Training admission fees now earn credits that can be applied to professional services - yet another way our RACF training provides exceptional ROI.