RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 8
Issue 3
July
2014

Default UACC & Connect UACC

If you do not specify a UACC when creating a profile, RACF automatically assigns it a UACC based on the Default UACC value for the class as specified in the Class Descriptor Table (CDT). For most IBM classes the default is NONE, but for a few, DATASET class included, it is ACEE. See the DSMON CDT report to identify such classes.

ACEE is the acronym for Accessor Environment Element, a control block which is built in memory by RACF during VERIFY (i.e., logon) and contains the user's identity and attributes. UACC is one such attribute, and its value is assigned as a new profile's UACC when the Default UACC is ACEE.

The UACC in the ACEE is obtained from the UACC specified in the user's current connect group, typically the user's default group. Every group connection has a UACC, and it can be seen in the output of a LISTUSER command.

You can specify a value for UACC when you first connect a user to a group with the CONNECT command. If you do not specify a value, it defaults to NONE. You can use the CONNECT command to change the setting on an existing connection.

To avoid accidentally allowing too high a level of default access, best practice is to set all connect UACCs to NONE.

Operator Command Entry

Physical consoles are but one method of entering MVS operator commands. Here are four other methods and the controls that govern their use.

TSO CONSOLE command: A user with a TSO segment requires READ access to TSOAUTH resource CONSOLE; otherwise, the user requires an entry in SYS1.UADS that grants this authority.

SDSF / command: If a profile protects SDSF resource ISFOPER.SYSTEM, the user requires READ access; otherwise, the user's ISFPARMS group must be defined with CMDAUTH(ALL).

JES2 /*$VS control statement: The JES2 internal reader (INTRDR) must be configured with AUTH SYSTEM(YES). If a profile protects OPERCMDS resource *jesx*.VS ('*jesx*' is the JES Subsystem name), the user requires CONTROL access.

JCL COMMAND statement: In JES2, the ability to use the COMMAND JCL statement requires that the JOBCLASS be configured with COMMAND set to a value other than IGNORE. As of z/OS 2.1 with either JES, if JES.JOBCLASS.SUBMITTER or JES.JOBCLASS.OWNER is defined as a discrete FACILITY class profile, JES will check the JOBCLASS.*localnodeid.jobclass.jobname* resource in the JESJOBS class. The job submitter, job execution user (i.e., owner), or both may require READ access to use the job class.

Even if authorized to submit commands, the user must still be authorized to execute the commands by either OPERCMDS profiles or MVS controls.

Auditors: Ensure OPERATIONS is Controlled, Part 4

The preceding three newsletters introduced you to the powerful OPERATIONS authority attribute and described how to identify OPERATIONS users and restrict their access. In this article we will address monitoring and alternatives to its use.

Activate the SETROPTS option OPERAUDIT to monitor use of OPERATIONS. This will generate an SMF record each time OPERATIONS is used. A batch job will be needed to produce a report from these records. To verify this option is active, check the first line of a SETROPTS LIST.

OPERATIONS was intended to enable Storage Administrators to manage datasets (e.g., move, defrag, backup, and restore). Its major drawback is that it also allows the user to access the data.

Over the years, IBM has introduced other authorities for allowing Storage Administrators to manage datasets without accessing the data. Their use is governed by DASDVOL class profiles and FACILITY class profiles prefixed STGADMIN.

Best practice is to implement these profiles to their fullest extent to replace OPERATIONS use.

There is a significant system performance benefit from the use of these alternative authorities. A single RACF access authorization check to an STGADMIN profile can allow processing of thousands of datasets, whereas use of OPERATIONS authority requires an access authorization check and the creation of an SMF record for each individual dataset.

It may not be possible to entirely eliminate the use of OPERATIONS authority. The alternative authorities cannot handle certain conditions and the ALTER access provided by OPERATIONS is needed. These conditions are rare and infrequent. Best practice is to provide senior Storage Administrators an alternate ID with OPERATIONS to be used only in these situations and to require each use to be justified and documented.

For more on Storage Administration authorities, visit our website for a copy of the presentation RACF & Storage Administration.

Comparing z/OS Unix and RACF

z/OS Unix permissions are READ, WRITE, and EXECUTE; although for a directory, EXECUTE means SEARCH. Here is how they roughly correlate to RACF DATASET permissions.

Directory	WRITE	ALTER
Directory	READ	READ to a catalog
Directory	SEARCH	READ to a catalog
File	WRITE	UPDATE
File	READ	READ
File	EXECUTE	EXECUTE

Unlike RACF, Unix permissions are independent of one another and are not hierarchical. WRITE, for instance, does not include READ.

Unix Superuser authority (UID 0) is comparable to the combination of TRUSTED and SPECIAL.

For the full details on Unix security, attend RSH's RACF - Securing z/OS Unix course.

Special Grouping Classes

Several RACF classes are technically grouping classes even though we do not recognize them as such. As with other grouping classes, they have companion member classes and you manage the contents of their profiles using ADDMEM and DELMEM. Each of these classes is shown below with its associated member class.

PROGRAM	PMBR
GLOBAL	GMBR
NODES	NODMBR
RACFHC	RACHCMBR
RACFVARS	RVARSMBR

The member classes exist solely because RACF architecture requires every grouping class to have an associated member class. RACF does not allow profiles to be created in these classes.

z/OS 2.1 REXX EXECIO Control

In z/OS 2.1, users who execute REXX EXECs that allocate the internal reader and use the EXECIO instruction to submit JCL will need READ permission to TSOAUTH resource JCL.

RSH News

One of the most challenging RACF tasks is **merging databases**. You must carefully analyze and synchronize every exit, table, option, and profile. Our tools and techniques enable us to excel at this task. Call RSH today for help.

Upcoming ***RSH RACF Training*:**

- RACF - Audit & Compliance Roadmap
  October 27-30, 2014 - Boston, MA
- RACF - Intro and Basic Administration
  December 8-12, 2014 - WebEx
- RACF - Securing z/OS Unix
  September 30 - October 3, 2014 - WebEx