RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 2
Issue 3

July
2008

OPERATIONS Authority Considerations

OPERATIONS authority can grant a user ALTER access to a resource. This article explores conditions required for this to occur.

First, the resource class must be defined so that OPERATIONS is considered when checking authorization. This option is set using either the OPER=YES parameter in the ICHERCDE macro in the RACF Class Descriptor Table or the OPERATIONS(YES) operand in the CDTINFO segment of the CDT class profile. The default settings for the two methods differ. For the ICHERCDE macro, OPER=YES is the default. For the CDTINFO segment, OPERATIONS(NO) is the default. IBM supplies a number of classes that check OPERATIONS, including DATASET and DASDVOL. To find out what classes check OPERATIONS authority in your system, look at the "OPERATIONS ALLOWED" column of the DSMON RACF Class Descriptor Table Report.

We recommend the OPERATIONS option be set to NO for all installation-defined classes to avoid unintended access authority. On occasion, we have encountered 3rd party products whose documentation failed to specify OPER=NO in their suggested ICHERCDE entries, allowing them to default to YES. We have yet to find an instance where OPERATIONS was necessary to the successful implementation of these classes.

Second, the user must not already be permitted access. OPERATIONS authority is checked *after* the standard access list has been processed. If the USERID or any group of an OPERATIONS user is in the standard access list of a resource profile, the corresponding permitted level of access governs the user's authority and OPERATIONS is ignored.

This behavior can be used to limit the access of OPERATIONS users to selected resources. When RSH implements RACF, we typically create a group (e.g., #NOOPER) to which we connect all the OPERATIONS users. We then permit this group access at a level below ALTER to restrict their authority to sensitive resources such as APF-authorized libraries, payroll files, catalogs, and DASDVOL profiles.

This technique does not guarantee that an OPERATIONS user cannot access restricted datasets. It may surprise you to learn that OPERATIONS allows the user to create group dataset profiles. Hence, OPERATIONS users could define more specific dataset profiles to give themselves access. This can be prevented by connecting every OPERATIONS user to every group matching a dataset High Level Qualifier with USE authority, but this is generally not practical. A better approach is to restrict OPERATIONS users' use of RACF commands either with PROGRAM class profiles or the ICHCNX00 Command Pre-processing exit. Alternatively, you can activate SETROPTS OPERAUDIT or AUDIT(DATASET) to monitor their use of OPERATIONS to create profiles.

Avoiding Output Browse Violation Messages in SDSF

When a user attempts to browse the output of an entire job in SDSF, an authorization check is made for every output dataset associated with the job to see if the user has READ authority. If a user is permitted to browse two of five output datasets for a job and enters ‘S’ to select the job on the STATUS or OUTPUT panel, the user will see the two permitted datasets and three RACF ICH408I violation messages. Corresponding SMF violation records will also be generated.

A new SDSF option was introduced in z/OS 1.9 to suppress these violation messages and SMF records. Option "Security.Browse.LogNOFAIL" can be set to VALUE(TRUE) using PROPERTY and PROPLIST statements in SDSF Server statements. Unfortunately, the ISFPARMS assembler macro does not provide support for this option. For details, see IBM's z/OS 1.9 SDSF Operation and Customization manual.

z/OS Unix Use Control

One means of preventing a user from accessing z/OS Unix and using TCP/IP services is not to assign an OMVS uid to the user. If you have defined profile BPX.DEFAULT.USER in the FACILITY class to provide a default uid to users who have not been assigned one, you can still block a specific user from accessing z/OS Unix by giving the user an OMVS segment with *no* uid. To accomplish this, enter the command:

```
ALTUSER userid OMVS
```

The z/OS Unix System Services Planning manual describes the use of APPL class profile OMVSAPPL to restrict entry into z/OS Unix and lists various Unix service APIs that include this APPL in their RACROUTE calls. Our testing indicates none of these APIs are apparently used by the OMVS and ISHELL TSO commands and certain TCP/IP services (e.g., FTP) because access of NONE to OMVSAPPL has no effect.

Auditors: Review ALTER Access to the Catalogs

The catalogs function as a directory for z/OS, allowing users to find a dataset by name without knowing the disk or tape volume where it resides. The catalogs also contain certain information about each dataset's characteristics.

The catalogs are structured in a hierarchy with a Master Catalog at the top and User Catalogs beneath. The Master Catalog typically contains entries for SYS1 datasets and aliases. Each ALIAS entry includes a dataset name prefix (e.g., PAY) and a reference to the User Catalog where individual dataset entries with that prefix can be found. When a user attempts to locate a dataset, the system starts by searching the Master Catalog. If it does not find an entry for the dataset but finds a matching ALIAS instead, it then searches the corresponding User Catalog for the dataset.

Typically, all users are permitted READ access to the Master Catalog and UPDATE access to the User Catalogs. With UPDATE access, a user may create or delete a catalog entry *provided* the user is also permitted to create or delete the corresponding dataset.

ALTER access to a catalog grants a number of powerful privileges. They include:

- Delete a VSAM file or Storage Management Subsystem (SMS) managed dataset *without* ALTER access permission to the dataset
- Uncatalog a non-SMS-managed dataset
- Lock and unlock a catalog for maintenance if READ access is also permitted to FACILITY profile IGG.CATLOCK

Ordinarily, ALTER access should only be permitted to IDs belonging to the technical support staff responsible for catalog administration. Use of a group to block ALTER access by users with OPERATION authority is recommended (see article above.)

RSH News

Thinking of starting a ***RACF User Group*** (RUG) in your locale? Call RSH. We support several RUGs and can offer advice on organizing meetings as well as provide speakers.

Upcoming ***RSH RACF Training*****:**

- RACF - Intro and Basic Administration
  October 7-9, 2008 - Boston, MA
- RACF - Audit for Results
  October 28-30, 2008 - Boston, MA

See our website for details and registration form.

RSH offers ***in-house RACF training***. If you have four or more students, this may be a cost-effective alternative to a public seminar.

If you missed our ***presentations*** at the June RACF conference, visit our website for a copy of the handouts.

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