RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 9
Issue 3
July
2015

Coming in z/OS 2.2 - ROAUDIT

Currently, users who merely need to list profiles and SETROPTS options must be given AUDITOR authority, which also enables them to change audit settings. As the result of a requirement submitted by RSH, in z/OS 2.2, IBM added a new authority to RACF called ROAUDIT (Read-Only AUDIT) that allows users to list profiles and options but not make changes. *Thank you IBM!*

Helpful TSO PROFILE Options

If you make a mistake when entering a RACF command such as specifying an invalid class, TSO will prompt you for a correction. To avoid being prompted, enter TSO command:

PROFILE NOPROMPT

By default, TSO displays the text of a system message without its message identifier code. To have TSO also display the code, enter command:

PROFILE MSGID

When coding RACF commands for dataset profiles, TSO automatically prefixes the profile with your USERID unless you enclose the profile in quotes. To stop the prefixing, enter command:

PROFILE NOPREFIX

These settings are saved in your TSO segment and will be in effect for subsequent logons. To check your current settings, enter command:

PROFILE

Protecting Datasets with Single Qualifier DSNAMEs

A few installations still process datasets with single qualifier DSNAMEs (e.g., ACHTAPE). To protect these datasets, you can use SETROPTS option PREFIX(*prefix*). PREFIX specifies a High Level Qualifier (HLQ) that is added to the DSNAME for the RACF authorization check. For example, if PREFIX is set to $SL, permission to $SL.ACHTAPE is required to access ACHTAPE. PREFIX must be set to a value that is valid for use as a dataset HLQ. NOPREFIX is the default.

If you have Enhanced Generic Naming (EGN) active in combination with NOPREFIX, you can instead protect these datasets with profiles like *dsname*.** (e.g., ACHTAPE.**). If PREFIX is set, it takes precedence and these profiles are not used.

SETROPTS PROTECTALL(FAILURE) will not allow access to a single qualifier DSNAME if there is no related profile. With NOPREFIX, the violation is for *dsname*. With PREFIX, it is *prefix.dsname*.

'Best Practice' is to create a RACF group whose sole purpose is to be used as the prefix, and set PREFIX to this group name. Define *prefix.dsname* profiles to protect known datasets and a *prefix*.** profile with no permissions to trap any others.

Profile CONNECT Entries

When you connect a user to a group, an entry is made in the group profile to record the user's membership and group AUTHORITY, which is either USE (the default), CREATE, CONNECT, or JOIN. A corresponding entry is made in the user profile to indicate the user is a member of the group, and a second entry is made to record connect attributes other than AUTHORITY such as OWNER, SPECIAL, and REVOKE. These entries correspond to the 0102, 0203, and 0205 records in the IRRDBU00 RACF database unload.

No entry is made in a UNIVERSAL group profile for a user given only AUTHORITY(USE) and no other attributes. This enables more than 5,957 users to be connected to the group.

Each CONNECT and REMOVE makes three separate updates (two for a Universal group connect). Updates can tie up the RACF database, so avoid executing large batches of these commands during the day, especially during periods with heavy logon activity.

If a TSO session or batch job executing a CONNECT or REMOVE is cancelled before all updates are completed, a partial or 'broken'

connect may result. Depending on the nature of the break, either a CONNECT or a REMOVE command will repair it, but it may be necessary to specify the AUTHORITY keyword or temporarily recreate a formerly existing user or group.

Prior to the restructured database introduced with RACF 1.9 (circa 1990), the connect information recorded in the second user profile entry was stored in its own separate database record. These were to have been the IRRDBU00 0300 records.

Auditors: RACF Staffing Levels

RACF can provide a z/OS system with near ironclad security, but significant effort is required to attain and sustain this level of protection. Every software component has its own strategy for using RACF to protect its resources, and the initial implementation is often complicated and time consuming. Each subsequent configuration change or component upgrade requires careful review to determine what adjustments to security may be needed. This work requires a high level of technical skill and can be labor intensive. Add to this the time-consuming, high-priority, day-to-day tasks of RACF administration and troubleshooting.

As you compile your list of RACF audit findings, make a rough estimate of the staff hours it will take to remediate them. If it is clear that the current RACF team is not staffed to handle the additional work, point this out to management.

RSH RACF reviews frequently find insufficient staffing at the root of many deficiencies. We often recommend adding RACF staff, and several hires are directly attributable to our recommendations.

For more on auditing RACF, attend RSH's RACF - Audit and Compliance Roadmap course.

Missing TMON Resources

The RACF interface for ASG's TMON products is documented in the manual "ASG-TMON Products for z/OS Common Components Reference Guide". A few resources are missing from the manual's function tables (e.g., TMON for z/OS - JOBSACT). Review TMON's DETAIL PROFILE DEFINITION panels online to identify them.

USER.OMVS.UID & SHARED.IDS

A user permitted UPDATE access to FIELD class resource USER.OMVS.UID can assign UID(0) to themselves or another user. Before permitting such access, upgrade your RACF database to the Application Identity Mapping (AIM) structure and implement UNIXPRIV class profile SHARED.IDS to prevent them from doing so.

For more on protecting z/OS Unix, attend RSH's RACF - Securing z/OS Unix course.

RSH News

If you are not asking for funding, management will think z/OS security is not important and everything is fine. Grab management's attention by asking for funding for RACF professional services during this year's upcoming budget cycle. Emphasize the enormous value of z/OS data to your organization and why its protection is critical. If you know what improvements are needed, list them and describe the risks they will mitigate. If not, ask for funds to cover an in depth review as well as anticipated follow-on remediation work. Boldly ask for a large sum to alert management to the seriousness of the situation and to ensure some funding will survive the budget cuts. ***If you need help formulating or justifying a budget, call RSH.***

Upcoming ***RSH RACF Training*:**

- RACF - Securing z/OS Unix
  September 22-25, 2015 - WebEx
- RACF - Audit & Compliance Roadmap
  November 10-13, 2015 - Boston, MA
- RACF - Intro and Basic Administration
  December 7-11, 2015 - WebEx

Many thanks to all who participate in our surveys!