RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 8
Issue 2
April
2014

z/OS 2.1 TRUSTED Tasks

As indicated in the MVS Initialization and Tuning Reference, z/OS 2.1 added these three Started Tasks to the list of those to be made TRUSTED.

JES3AUX
SMSPDSE1
WLM

Furthermore, CEA now only requires TRUSTED when running z/OSMF ISPF applications; otherwise, TRUSTED is optional. Also newly designated as optional for TRUSTED is zFS.

SDSF Destination Operators

To view and manage jobs and output in JES, the typical SDSF user needs permission to the associated JESSPOOL profiles. This is not the case for SDSF Destination Operators. They have access to all jobs and output sent to a specific destination, which might be a certain printer.

A user becomes a Destination Operator when permitted READ access to SDSF class resource ISFOPER.DEST.*jesx*, where '*jesx*' is the name of the JES subsystem (e.g., JES2).

To view and manage jobs or output sent to a particular destination, a Destination Operator needs access to one of the following SDSF class resources. The specific action being attempted determines which resource is required. READ access permission allows viewing; whereas, ALTER access allows changing and deleting.

ISFAUTH.DEST.*destname*.DATASET.*dsname*
ISFAUTH.DEST..DATASET.*dsname*
ISFAUTH.DEST.*destname*
ISFAUTH.DEST.

Note that the resource with the embedded double period '..' is incorrectly shown with a single period in the most recent version of the manual. RSH has notified IBM of this discrepancy.

Be aware that SDSF suppresses logging for the use of these resources.

Access to these resources should be strictly limited. A Destination Operator with access to a profile like ISFAUTH.DEST.* could potentially have access to all jobs and output.

On a related note, see article "*Sharing Output in SDSF (Without JESSPOOL Permission)*" in the April 2008 issue of our RSH RACF Tips.

For more information, refer to the SDSF Operation and Customization manual for your z/OS release.

z/OS 2.1 APPL CBDSERVE

In z/OS 2.1, users need READ access to APPL resource CBDSERVE to log onto the Hardware Configuration Definition (HCD) agent.

Visit the RACF Center webpage on our website for a copy of our presentation on the APPL Class.

FSSEC and ACL Activation

The Unix setfacl command will let you add Access Control Lists (ACLs) to files and directories even though the FSSEC class is inactive. These ACLs remain dormant until you activate the class. Be sure to check your Unix File Systems for existing ACLs before activating FSSEC. For any ACLs you find, evaluate their effect on access when FSSEC is activated. It might be safest to delete them.

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

TRUSTED UAUDIT SURROGAT

Contrary to statements in the RACF Security Administrator's Guide, UAUDIT does not result in the logging of SURROGAT access by TRUSTED Started Tasks. See APAR OA44481.

z/OS 2.1 JES2 Modify Service

JES2 in z/OS 2.1 has added function code 85 to the Subsystem Interface (SSI). SSI 85, also known as the Job Modify interface, allows other processes to call JES2 via the SSI to manage jobs and output. It uses JESJOBS class resources to govern use of modify actions.

JESJOBS already controls job submission and use of the TSO CANCEL command to cancel jobs. The relevant resource names are:

SUBMIT.localnodeid.jobname.userid	READ
CANCEL.nodename.userid.jobname	ALTER

SSI 85 checks the aforementioned CANCEL resource as well as the following new resources, whose prefixes correspond to SSI actions.

HOLD.nodename.userid.jobname	UPDATE
MODIFY.nodename.userid.jobname	UPDATE
PURGE.nodename.userid.jobname	ALTER
RELEASE.nodename.userid.jobname	UPDATE
REROUTE.nodename.userid.jobname	UPDATE
RESTART.nodename.userid.jobname	CONTROL
SPIN.nodename.userid.jobname	CONTROL
START.nodename.userid.jobname	CONTROL

If you have already defined JESJOBS profiles, you may need to redesign them to accommodate users of Job Modify SSI 85.

Auditors: Ensure OPERATIONS is Controlled, Part 3

The preceding two newsletters introduced you to the powerful OPERATIONS authority attribute and how to identify OPERATIONS users. Now we will tell you how their access can be restricted.

OPERATIONS users are only given unrestricted ALTER-level access when they have not been permitted access. When an OPERATIONS user attempts to access a resource, RACF looks for the user's USERID and groups in the access list of the guarding profile. If it finds either of them, RACF allows access based solely on the level of access they have been permitted and OPERATIONS authority is ignored. This behavior can be used to limit their access.

If you find a dataset containing sensitive data that a certain OPERATIONS user should not be able to view or update, inspect the dataset's guarding profile to verify that either the user's USERID or one of the user's groups is in the access list with an appropriately restrictive level of permission such as READ or NONE.

Best practice is to create a group to which all the OPERATIONS users are connected and use this group in making access blocking permissions.

There are certain system resources where it is best to limit the access of OPERATIONS users. Included are catalogs and DASDVOL profiles.

In future articles, we will describe how to monitor use of OPERATIONS authority and examine alternatives to its use.

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

RSH News

"If you can remain calm while all those about you are panicking, perhaps you don't understand the situation." ***Replacing BPX.DEFAULT.USER*** is neither a quick nor simple task in many situations. If you think you might need our help, ***call today!*** Our schedule is filling fast, so do not delay.

Upcoming ***RSH RACF Training*:**

- RACF - Audit & Compliance Roadmap
  April 22-25, 2014 - Boston, MA
  October 27-30, 2014 - Boston, MA
- RACF - Intro and Basic Administration
  June 9-13, 2014 - WebEx
  December 8-12, 2014 - WebEx
- RACF - Securing z/OS Unix
  September 30 - October 3, 2014 - WebEx

Ask about ISACA and ISSA Chapter discounts.

April 8th is the mainframe's 50th anniversary!