IBM Education Assistance for z/OS V2R2

Item: RACF Read-Only Auditor
Element/Component: RACF

Material current as of May 2015

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Migration & Coexistence Considerations
- Installation
- Presentation Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Presentation Objectives

- Identify the modifications to RACF that have been made to allow for a Read-Only Auditor: a RACF user to allowed to list information about profiles within the RACF database that can be also listed by a RACF user with the AUDITOR attribute, without granting that user any additional authority to any of the RACF profiles.
  - RACF R_admin Callable Service
  - RACF commands ADDUSER, ALTUSER, LISTDSD, LISTGRP, LISTUSER, RLIST, SETROPTS LIST, SEARCH
  - z/OS UNIX ck_access
  - DSMON, IRRUT100, and IRRXUTI2 utilities
- Function is installed as part of the standard RACF install procedure.
  - No extra or altered installation steps.
- Function is invoked through existing RACF commands and R_admin interfaces.
  - No new interfaces

Overview

- Problem Statement / Need Addressed
  - Allow a user to be defined (or altered) so that the user can list all information about any RACF profile without needing to grant that user additional authority to those profiles.
    - User is unable to set auditing controls on profiles, but may view information on them.
- Solution
  - Implement a new RACF user attribute: ROAUDIT.
    - Allow users to be defined or altered to have this attribute.
    - Similar to, but distinct from, the existing AUDITOR attribute – does not include the AUDITOR attribute's ability to control RACF profiles.
  - Modify existing “list” commands and utilities to permit users with ROAUDIT the same ability to list information that would be allowed to users with AUDITOR.
- Benefit / Value
  - Allows installations to create users that can view system information but not alter any system controls.
    - Ex: Suitable for use by an external auditor who may need to verify the current security state of a system – allows that user to view system information but does not unintentionally grant the user the ability to change (or sabotage) system settings.

Usage & Invocation

- ADDUSER and ALTUSER (plus the related R_admin functions and ISPF panels) are modified to set or reset the new Read-Only Auditor attribute depending on options provided to the command.
  - New command options: ROAUDIT Set Read-Only Auditor capability for user
    NOROAUDIT Remove Read-Only Auditor capability for user
  - SMF Record Type 80 entries generated for ADDUSER and ALTUSER indicate which option was provided – NOROAUDIT is the default if none is specified for ADDUSER.
  - SAF trace entries will indicate the option provided if any option was provided.
- "Listing" commands (plus related R_admin functions and ISP panels) are modified to test for the ROAUDIT attribute when determining the user's authority to list information about RACF profiles.
  - Commands: LISTDSD, LISTGRP, LISTUSER, RLIST, SETROPTS LIST, SEARCH
  - z/OS UNIX: ck_access
  - Utilities: DSMON, IRRUT100, IRRXUTI2
- ROAUDIT is distinct from the existing AUDITOR attribute.
  - Both flags may be set (or unset) for the same user.
  - If both flags are set, the AUDITOR attribute takes precedence in any authority checking.
    - Setting the ROAUDIT attribute on an existing user that already has the AUDITOR attribute set will not remove that user's authority to set or alter RACF controls.

Usage & Invocation (continued)

- Example: Creating and verifying a Read-Only Auditor user:

```
ADDUSER RRGROA ROAUDIT TSO(PROC(ISPFPROC)...) ...
READY
LISTUSER RRGROA
 USER=RRGROA  NAME=UNKNOWN  OWNER=IBMUSER   CREATED=14.164
  DEFAULT-GROUP=SYS1     PASSDATE=00.000 PASS-INTERVAL= 30 PHRASEDATE=N/A
  ATTRIBUTES=ROAUDIT
  REVOKE DATE=NONE   RESUME DATE=NONE
  LAST-ACCESS=UNKNOWN
  CLASS AUTHORIZATIONS=NONE
  NO-INSTALLATION-DATA
  NO-MODEL-NAME
  LOGON ALLOWED   (DAYS)          (TIME)
  ----------------------------------------
  ANYDAY                          ANYTIME
    :
   etc...
    :
```

Migration & Coexistence Considerations

No conditioning or toleration APARs are necessary for this new feature, but there are some items to consider from a compatibility standpoint.

- Forward migration
  Users defined in the RACF database from prior releases (ex: RACF V1R13 or V2R1) are not affected when the database is migrated forward to the new format for RACF V2R2. Since ROAUDIT is a new and distinct user attribute that makes uses of existing reserved space, existing users and prior releases of RACF are not affected. Any existing users with the AUDITOR attribute retain all the rights and privileges of that attribute when the RACF database is migrated forward, and no existin users are assigned the ROAUDIT attribute during a forward migration.

- Backward migration
  This is the situation that arises when, after a period of installing and using RACF V2R2, the installation “falls back” to a prior release of RACF or “backs off” RACF V2R2 and uses a prior RACF release instead.

  Any users defined with the ROAUDIT attribute retain this attribute in a backward migration, however, since prior releases do not test for this attribute (nor do they know of its existence), the user will have none of the rights and privileges given to a Read-Only Auditor. These users are not automatically promoted to AUDITOR status, and security administrators will need to explicitly grant AUDITOR access to any former ROAUDIT users that may require it. Administrators will be unable to see or alter the ROAUDIT attribute using RACF commands and utilities from prior releases.

  If a system that “backed off” RACF V2R2 should later reinstall RACF V2R2, any users that had been previously defined with the ROAUDIT attribute set will retain that attribute and have Read-Only Auditor authority privilege in the reinstalled RACF V2R2 system.

Installation

- No new installation steps
  - RACF templates are updated for the new ROAUDIT user attribute during the execution of the IRRMIN00 job.

Presentation Summary

- A new RACF user attribute is introduced for system auditing purposes.
  - ROAUDIT (Read-Only Auditor)
- A user can now be defined (or altered) so that the user can list all information about any RACF profile without granting that user additional authority to those profiles.
  - User is unable to set auditing controls on profiles, but may view information on them.
- Example usage: An external auditor who may need to verify the current security state of a system.
  - The attribute allows that user to view system information but does not unintentionally grant the user the ability to change (or sabotage) system settings.
- This new attribute is separate, and distinct, from the AUDITOR user attribute.
  - Both attributes may be granted to the same user, in which case the AUDITOR authority would take precedence in any authority checking.

Appendix

- z/OS Publications
  - ***z/OS V2R2 Security Server RACF Security Administrator's Guide*** (SA23-2289-01)
  - ***z/OS V2R2 Security Server RACF Auditor's Guide*** (SA23-2290-01)
  - ***z/OS V2R2 Security Server RACF System Programmer's Guide*** (SA23-2287-01)
  - ***z/OS V2R2 Security Server RACF Command Language Reference*** (SA23-2292-01)
  - ***z/OS V2R2 Security Server RACF Callable Services Reference*** (SA23-2293-01)
  - ***z/OS Security Server RACF Macros and Interfaces Reference*** (SA23-2288-01)
- z/OS Websites
  - **z/OS Resource Access Control Facility**
    http://www-03.ibm.com/systems/z/os/zos/features/racf/