RSH CONSULTING

RACF Administrator Toolkit

RUGONE+KOIRUG+GARUG+CHIRUG
May 2022

RSH Consulting - Robert S. Hansel

RSH CONSULTING

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- http://twitter.com/RSH_RACF

RACF Administrator Toolkit

- The intent of this presentation is to list all the resources and permissions RACF Administrators should have and use to fulfill their responsibilities

- RACF Administrators should be able to examine all the components and configuration options of z/OS and installed system software products as they either may affect security or need to be identified to ensure they are protected. This includes the ability to display configuration options currently in effect in a live system.

Topics

- RACF
- Datasets
- Health Checker
- Unix
- Operator Commands
- SDSF
- Storage Administration
- Miscellaneous

RACF

- System SPECIAL
- System AUDITOR or ROAUDIT
  - Consider assigning System AUDITOR to a managed privileged ID
- Authority to execute RACF Command Parsing Load program IRRDPI00 for Custom Field maintenance
  - SPECIAL (only if not protected by a FACILITY or PROGRAM profile)
  - FACILITY IRRDPI00 - READ access (only if not protected by a PROGRAM profile)
  - PROGRAM IRRDPI00 - READ access (define as a discrete profile)
- Authority to execute DSMON program ICHDSM00 to generate reports
  - AUDITOR (only if not protected by a PROGRAM profile)
  - PROGRAM ICHDSM00 - READ access (define as a discrete profile)
  - FACILITY ICHDSM00.SYSCAT - READ access (access is allowed if not defined)
    - Controls ability to list catalogs in Selected Data Sets Report

RACF

- RACF Database - both live and backup/archival copies - READ access
- RACF IRRDBU00 Database Unload - READ access
  - Unloads of the Primary database should be generated daily
- RACF Remove ID program IRRRID00 - Generate user and group purge commands
  - Requires READ access to an IRRDBU00 unload
  - RACF adjunct product equivalents
- FACILITY IRR.RADMIN.*racf-commands* - READ access
  - Allows use of R_admin callable service
  - Required to manage Custom Fields via RACF ISPF panels
- ***RVARY passwords - Know what they are or where to find them!!!***

RACF

- Unsupported RACF utilities
  - Various programs provided “as is” with no formal support
  - Software and detailed instructions available via:
    - Github https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-RACF/Downloads
    - IBM FTP ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/
  - Examples:
    - RacfUnixCommands - Unix security administration REXX EXECs
    - CDT2DYN - Convert installation ICHRRCDE defined classes to Dynamic CDT profiles
    - DSNT2PRM - Converts ICHRDSNT and ICHRRNG into a RACF PARMLIB member
    - DBSYNC - Builds RACF commands to synchronize databases
    - IRRHFSU - C program to unload Unix File Security Packets (FSPs), like IRRDBU00
    - IRRXUTIL - REXX program using the IRRXUTIL R_admin callable service interface
    - LISTCDT - Lists the contents of the RACF Class Descriptor Table (CDT)
    - PWDCOPY - Copy cyphered passwords between RACF data bases
    - RACFDB2 - Migrate DB2 access controls to RACF profiles
    - RACKILL - Unconditionally deletes profiles
    - RACSEQ - Invokes R_admin (IRRSEQ00) and displays every profile field

Datasets

- READ access
  - Nucleus program library
  - Configuration parameter (PARMLIB) libraries
  - Link-Pack Area (LPA) program libraries
  - Supervisor Call (SVC) program libraries
  - Authorized Program Facility (APF) program libraries
  - Link List (LNKLST) program libraries
  - ISPF program and panel libraries
  - Master and User Catalogs
  - Started Task and Batch JCL Procedure (PROCLIB) libraries
  - SMF datasets - live and archives
  - Software product configuration libraries (e.g., CICS System Initialization Table)
  - RACF table source code libraries
  - Exit source code libraries
  - Application Production JOBLIBs and PROCLIBs

Health Checker

- View all Health Checks - READ access
  - XFACILIT HZS.sysid.*function* MESSAGES | QUERY
- Run RACF Health Checks - UPDATE access
  - XFACILIT HZS.sysid.IBMRACF.*function* ACTIVATE | UPDATE | RUN
- Run other security-related Health Checks - UPDATE access
  - XFACILIT HZS.sysid.IBMJES.JES_NJE_SECURITY.*function*
  - XFACILIT HZS.sysid.IBMJES.JES_NJE_SECURITY_*ssname*.*function* (Secondary Subsystem)
  - XFACILIT HZS.sysid.IBMSDSF.SDSF_CLASS_SDSF_ACTIVE.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_CAT3_CONFIGURATION.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_CEDA_ACCESS.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_JOBSUB_SPOOL.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_JOBSUB_TDQINTRDR.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_REGION_CONFIGURATION.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_RESOURCE_CONFIGURATION.*function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_RESOURCE_SECURITY. *function*
  - XFACILIT HZS.sysid.IBMCICS.CICS_USS_CONFIGURATION.*function*

Unix

- /etc directory - READ (r--) to all objects, or at least the following
  - /etc/init.options
  - /etc/inittab
  - /etc/rc
  - /etc/inetd.conf
  - /etc/auto.master - and all corresponding map files
  - /etc/hosts
  - /etc/profile
  - /etc/protocol
  - /etc/services
  - /etc/sudoers
- READ (r--) to the following
  - BPXPRMxx AUTHPGMLIST file - usually /etc/authfile
  - BPXPRMxx USERIDALIASTABLE file - usually /etc/tablename
  - Unix syslog daemon log files
- READ access to any dataset equivalents to the above

Unix

- System AUDITOR and ROAUDIT
  - Examine all directories and view all File Security Packets (FSPs)
  - Overrides FSACCESS restrictions
- Allow reading all files as alternative to granting individual file access permissions
  - UNIXPRIV SUPERUSER.FILESYS - READ access
  - UNIXPRIV SUPERUSER.FILESYS.ACLOVERRIDE - READ access (only if defined)
  - Only if no sensitive data is kept in the Unix file system (consider digital keys)
- Administering file and directory permissions (not UID(0) or FACILITY BPX.SUPERUSER)
  - UNIXPRIV SUPERUSER.FILESYS.DIRSRCH - READ access
    - Only needed if RACF Administrator does not have AUDITOR, ROAUDIT, or SUPERUSER.FILESYS access
  - UNIXPRIV SUPERUSER.FILESYS.CHOWN - READ access
  - UNIXPRIV SUPERUSER.FILESYS.CHANGEPERMS - READ access
- UNIXPRIV SUPERUSER.PROCESS.GETPSENT - 'ps' (process status) command to monitor Unix activity - READ access
- IRRHFSU - Hierarchical File System Unload (see RSH presentation for details)

Operator Commands

- Commands entered via a Console
  - CONSOLE class - console logon
  - OPERCMDS class - command protection
    - '*jes*' = JES subsystem name

- Consoles
  - CONSOLE *console-profiles* - READ access
  - TSOAUTH CONSOLE - READ access
    - OPERCMDS MVS.MCSOPER.*yourid*[*] - READ access
  - SDSF ISFOPER.SYSTEM - / command - READ access
  - (Optional) OPERCMDS *jes*.VS - JES2 $VS command - CONTROL access

- Display commands - READ access
  - OPERCMDS MVS.DISPLAY.*commands*
  - OPERCMDS *jes*.DISPLAY.*commands*
  - OPERCMDS *jes*MON.DISPLAY.*commands*

Operator Commands

- RACF Subsystem - Entry of RACF commands via a console
  - OPERCMDS profile prefix *racfssn* is the RACF Subsystem name (e.g., RACF)
    - PARMLIB(IEFSSNxx) definition - subsystem name, command scope, and command prefix
  - OPERCMDS *racfssn.profile-commands* - READ access
  - OPERCMDS *racfssn*.SETROPTS - UPDATE access
  - OPERCMDS *racfssn*.DISPLAY.SIGNON - READ access
  - OPERCMDS *racfssn*.SET.LIST - READ access
  - OPERCMDS *racfssn*.SET.GENERICANCHOR - READ access
  - OPERCMDS *racfssn*.SET.TRACE - READ access
  - OPERCMDS *racfssn*.TARGET.LIST - READ access
  - If RACF Administrators also maintain the RRSF configuration, ...
    - OPERCMDS *racfssn*.RESTART - READ access
    - OPERCMDS *racfssn*.STOP - READ access
    - OPERCMDS *racfssn*.SET.*options* - READ access
    - OPERCMDS *racfssn*.TARGET.*options* - READ access
  - ***Know your RACF command console prefix!!!***
    - Operator command "Display Opdata,PREFIX" will show prefix if set (if not, it is "*racfssn* ")

SDSF

- Display commands - READ access
  - SDSF ISFCMD.DSP.*command.jes*
  - SDSF ISFCMD.DSP.SYMBOL.*sysid*
  - SDSF ISFCMD.ODSP.*command.sysid*
  - SDSF ISFCMD.FILTER.*option*
  - SDSF ISF.CONNECT.*sysid* - gather information from system(s) via SDSFAUX task

- View all Job processing results without JESSPOOL authority - READ access
  - SDSF ISFOPER.DEST.*jes* - Destination operator
  - SDSF ISFAUTH.DEST.*.DATASET.JESJCL
  - SDSF ISFAUTH.DEST.*.DATASET.JESMSGLG
  - SDSF ISFAUTH.DEST.*.DATASET.JESYSMSG

- View SYSLOG - READ access
  - SDSF ISFCMD.ODSP.SYSLOG.*sysid*
  - JESSPOOL *nodeid.*+MASTER+.SYSLOG.*jobid.dsidneitifier.*?

SDSF

- Display action characters - READ access
  - ISFAPF.dsname
  - ISFAPPL.devicename.jes-name
  - ISFCFC.connectionname
  - ISFCFS.structurename
  - ISFDEV.volser
  - ISFDYNX.exitname
  - ISFENQ.majorname.system
  - ISFEMCS.consolename
  - ISFFS.filesystemname
  - ISFGT.eventowner
  - ISFINIT.Iinitname.jes-name
  - ISFJDD.CF.system
  - ISFJDD.IP.system
  - ISFJES.subsysname
  - ISFJOB.DDNAME.owner.jobname.system
  - ISFJOB.STORAGE.owner.jobname.system
  - ISFJOB.TASK.owner.jobname.system
  - ISFJOBCL.class.jes-name
  - ISFLINE.device-name.jes-name
  - ISFLNK.dsname
  - ISFLPA.dsname
  - ISFMEMB.membername.jes-name
  - ISFNETACT.jobname
  - ISFNODE.node-name.jes-name
  - ISFNS.device-name.jes-name
  - ISFOMVS.option-name
  - ISFPAGE.dsname
  - ISFPARM.dsname
  - ISFPLIB.dsname
  - ISFPROC.owner.jobname
  - ISFRDR.device-name.jes-name
  - ISFRES.resource.system
  - ISFSE.sched-env.system
  - ISFSMSVOL.filesystemname
  - ISFSO.device-name.jes-name
  - ISFSOCK.devicename.jes-name
  - ISFSP.volser.jes-name
  - ISFSTORGRP.storagegroupname
  - ISFSUBSYS.subsystemname
  - ISFSYM.symbolname.system
  - ISFSYS.sysplexname.system
  - ISFXCFM.membername

Storage Administration

- DFHSMSrmm - Removable Media Manager
  - FACILITY STGADMIN.EDG.LISTCONTROL - List configuration - CONTROL access
  - FACILITY STGADMIN.EDG.MASTER - LIST commands - READ access

- DFHSMShsm - Hierarchical Storage Manager
  - FACILITY STGADMIN.ARC.LIST - List HSM dataset details - READ access

Storage Administration - Alias Administration

- If RACF Administration or an identity Management (IDM) product maintains catalog aliases for TSO users, permit either ...
  - ALTER access to the Master Catalog (not recommended)
    - Allows creation and deletion of aliases
      - Deletion not limited to aliases for users
      - Deletion not prevented if there are cataloged datasets
    - Allows other actions associated with catalog ALTER access (e.g., delete SMS-managed datasets)
  - READ access to FACILITY STGADMIN.IGG.DEFDEL.UALIAS
    - Allows creation and deletion of aliases
      - Deletion not limited to aliases for users
      - Deletion not prevented if there are cataloged datasets
  - UPDATE access to the Master Catalog to create aliases
    - Allows creation of aliases
    - Allows cataloging datasets in the Master Catalog if permitted ALTER access to the datasets
    - Alias deletion is handled by Catalog Administrators
  - ALTER access to the User Catalog containing the TSO user dataset entries
    - Allows deletion of aliases related to that catalog
      - Deletion not limited to aliases for users
      - Deletion not prevented if there are cataloged datasets
    - Allows other actions associated with catalog ALTER access (e.g., delete TSO user dataset)

Miscellaneous

- TSO
  - TSOAUTH PARMLIB - Use TSO PARMLIB command
    - List TSO configuration - READ access
  - TSOAUTH ACCT - Use TSO ACCOUNT command - READ access
    - List and administer TSO user definitions in SYS1.UADS - READ access
      - To allow view only, instead permit READ access to SYS1.UADS
    - Execute SYNC command to synchronize SYS1.BRODCAST with TSO segments when the RACF database is shared by multiple systems but SYS1.BRODCAST is not shared
  - SYS1.BRODCAST - Administer TSO segments - UPDATE access
- CICS
  - {TCICSTRN} CEDC transaction - View CICS resource definitions - READ access
  - DFHCSDUP utility - List CICS resource definitions
    - Requires READ access to CICS System Definition (CSD) files
  - CICS Explorer - GUI - View System Initialization Table (SIT) parms
- Sysplex - RMF
  - FACILITY ERBSDS.MON2DATA - Display info on SDSF DA panel - READ access

Miscellaneous

- Logon authority - APPL profiles - READ access
  - TSO
  - CICS
  - z/OSMF - default IZUDFLT

- SMF
  - IFASMFDP program Dump SMF datasets
    - Requires READ access to SMF dump datasets
  - IFASMFDL program Dump SMF Logstreams
    - Requires READ access to SMF logstreams - LOGSTRM IFASMF.*lsname*
  - RACF SMF unload programs - SMF user exits IRRADU00 and IRRADU86
  - RACFRW - TSO command - RACF Report Writer (obsolete - stabilized 1992)

- z/OS Communication Server - NETSTAT command - display TCP/IP info
  - SERVAUTH EZB.NETSTAT.*sysname.tcpname.netstat_option* - READ access

Miscellaneous

- ISRDDN - TSO command - Verify existence and examine program modules
- IPLINFO - Mark Zeldon REXX EXEC - List system configuration information
- Dynamic Exits - CSVDYNAM macro
  - FACILITY CSVDYNAM.LIST - List exits - READ access
- z/OSMF - ISPF plug-in
- FDR - FDRZAPOP program - List FDR configuration options
  - Requires READ access to FDR's load library
- CA-1 - TMSSTATS program - List CA-1 configuration options
  - Requires READ access to CA-1's load library
- JOB output archive viewing software tools (e.g., $AVRS)
  - Examine job results post-execution
- RACF-L internet discussion list - subscribe
  - https://www.rshconsulting.com/racftips/RSH_Consulting__RACF-L.pdf