RACF - The Essentials For Systems Programmers

SPARTA - June 2017
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
Introduction to RACF

- Resource Access Control Facility (RACF)

- IBM's Security Software Product for MVS, OS/390, and z/OS

- First introduced in 1976

- Component of IBM's z/OS Security Server

- Comprised of:
  - Database (Primary and Backup Pair)
    - Profiles - Users, Groups, Datasets, General Resources
  - Software
    - Programs
    - Macros - RACROUTE
    - TSO Commands
    - Utilities

RACF, z/OS, DB2, and CICS are Trademarks of the International Business Machines Corporation
RACF Functions

- User Identification and Authentication
- Resource Access Authorization
- Monitor User Activity
- Access Administration
RACF Functions

- RACF is called by a system resource manager (e.g. CICS) whenever a user tries to logon or attempts to access a resource

- RACF determines whether an action is authorized and *advises* the resource manager to allow or disallow the action

- RACF uses the profiles defined in its database to make these determinations

- The *resource manager* decides what action to take based on what RACF advises
Profiles and Relationships

USER

GROUP

RESOURCE

CONNECT

PERMIT

Batch Job

Started Task

Profile:

Dataset

CICS Trans.

Position:

Job Function:

Organization
RACF Components

- Database
- Software
- RACF Subsystem
- System Authorization Facility (SAF)
RACF Components - Database

- Primary and optional Backup pair (a database can be multi-dataset)

- Database structure
  - Basic Direct Access Method (BDAM)
  - 4K blocks
  - Sixteen (16) 256-byte segments per block
    - Profiles are allocated space in contiguous segments
  - A database dataset has a maximum size limit of 2GB

- Database blocks
  - Inventory Control Block (ICB) - SETROPTS Options
  - Index Blocks - Profile location pointers and Application Identify Mapping (AIM)
  - Profile Template Blocks - Profile record layouts
  - Block Availability Mask (BAM) Blocks - identify open segments in each data block
  - Data Blocks - User, Group, Dataset, and General Resource Profiles and Profile Segments (e.g., TSO, CICS, OMVS, STDATA)

- Requires very strict access control (UACC=None)
Without RACF Sysplex, single database pair ...

```
RVARY LIST
RACF DATABASE STATUS:
ACTIVE USE NUM VOLUME DATASET
------- ---- --- ------ ------- -------
YES PRIM 1 RACSY4 SYS1.PRIM.RACF
YES BACK 1 RACSY2 SYS1.BKUP.RACF
RVARY COMMAND HAS FINISHED PROCESSING.
```

With RACF Sysplex data communications and sharing, split database pairs ...

```
RVARY LIST
RACF DATABASE STATUS:
ACTIVE USE NUM VOLUME DATASET
------- ---- --- ------ ------- -------
YES PRIM 1 SYS907 SYS1.RACFPRD1
YES BACK 1 SYS906 SYS1.RACFBKP1
YES PRIM 2 SYS800 SYS1.RACFPRD2
YES BACK 2 SYS906 SYS1.RACFBKP2
MEMBER PRD1 IS SYSPLEX COMMUNICATIONS ENABLED & IN DATA SHARING MODE.
RVARY COMMAND HAS FINISHED PROCESSING.
```
RACF Components - Database - RVARY LIST

- RACF Database allocation
  - Physical Sequential, Unmovable (PSU)
  - Single extent
  - Non-SMS managed
  - Fixed Record Format (RECFM=F)
  - Logical Record Length 4096 (LRECL=4096,BLKSIZE=4096)

Data Set Information

Command ===>

Data Set Name . . . . : SYS1.RACFPRM1

General Data
  Management class . . : **None**
  Storage class . . . : **None**
  Volume serial . . . : VPMVSH
  Device type . . . . : 3390
  Data class . . . . . : **None**
  Organization . . . : PSU
  Record format . . . : F
  Record length . . . : 4096
  Block size . . . . . : 4096
  1st extent cylinders: 3
  Secondary cylinders : 0
  Data set name type :
  SMS Compressible . : NO

Current Allocation
  Allocated cylinders : 3
  Allocated extents . : 1

Current Utilization
  Used cylinders . . : 3
  Used extents . . . : 1

Dates
  Creation date . . . : 1993/06/20
  Referenced date . . : 2017/02/22
  Expiration date . . : ***None***
RACF Components - Software

- Programs
  - Perform authorization checking (ICH and IRR prefixes)
  - Reside in SYS1.LINKLIB and SYS1.LPALIB

- Tables

- Macros
  - RACROUTE - REQUEST=AUTH, FASTAUTH, VERIFY
  - Independent Macros - RACHECK, FRACHECK, RACINIT

- Supervisor Calls (SVC) - 130-133 - Invoked by Macros

- Exits

- TSO and Console Commands

- Utilities
RACF Components - Software - Tables

- **RACF Dataset Name Table - ICHRDSNT**
  - Defines RACF dataset names, number of resident data blocks (RDBs), backup options, and RACF SysPlex options

- **RACF Command Parsing Table - IRRDPI00**
  - Provides RACF with instructions for parsing segments entered with commands
  - Built in memory using program IRRDPI00 or TSO command IRRDPI00
  - Loaded at IPL by the RACF address space or a started task (e.g., IRRDPTAB)
  - Reloaded to incorporate CFIELD profile CFDEF segment additions and changes

- **Class Descriptor Table (CDT) - ICHRRCDx**
  - Defines classes and their characteristics
  - IBM-supplied table - ICHRRCDX
  - Installation-defined table - ICHRRCDE (macro ICHRRCDE)
  - CDT class profiles - Replace or supersede ICHRRCDx entries

- **Started Task Table - ICHRIN03**
  - Assigns ID, group, PRIVILEGED, and TRUSTED to a Started Task/Procedure
  - STARTED class profiles - Replace or supersede ICHRIN03 entries
RACF Components - Software - Tables

- Dataset Range Table - ICHRNRNG
  - Defines profile name ranges to be distributed across multiple database datasets
  - Used in combination with multiple database dataset definitions in ICHRDSNT

- Naming Convention Table - ICHNCV00
  - Enables rearranging dataset names
  - Can enforce dataset naming conventions
  - ICHNCONV macro

- RACF Router Table (RRT) - ICHRFRXx
  - IBM-supplied table (pre z/OS 1.6) - ICHRFR0X
  - Installations-defined table - ICHRFR01 (macro ICHRFRTB)
  - Required by RACF pre z/OS 1.6 (prior to the introduction of the CDT class)
  - Only needed for entries specifying RACF=NONE to skip RACF checking (rarely necessary)

- Authorized Callers Table - ICHAUTAB
  - Enables use of RACROUTE REQUEST=LIST and VERIFY without APF-authorization
  - Not recommended
RACF Exits

- ICHRDX01/02  REQUEST=DEFINE (RACDEF) Pre-/Post-Processing
- ICHRIX01/02  REQUEST=VERIFY{X} (RACINIT) Pre-/Post-Processing
- ICHRCX01/02  REQUEST=AUTH (RACHECK) Pre-/Post-Processing
- ICHRFX01-03/02-04 REQUEST=FASTAUTH (FRACHECK) Pre-/Post-Processing
- ICHRLX01/02  REQUEST=LIST (RACLST) Pre-/Post-Processing
- ICHDEX01/11  Password Encryption
- ICHPWX01/11  New Password / Password Phrase
- ICHCNX00     Command Pre-Processing for ADDSD, ALTDSD, DELDSD, LISTDSD, PERMIT, SEARCH, RLIST, RALTER, RDELETE, and Utility ICHUT100
- ICHCCX00     Command Pre-Processing DELUSER, DELGROUP, REMOVE
- IRREVX01     (Dynamic) Command Pre/Post-Processing
- IRRACX01/02  ACEE Compression/Expansion Pre/Post-Processing
- IRRVAF01     (Dynamic) Custom Field (CFIELD) Validation
- IRRSXT00     SAF Callable Services Router Installation
- ICHRTX00/01  SAF Router Post-/Pre-Master Scheduler Initialization

<table>
<thead>
<tr>
<th>EXIT MODULE</th>
<th>MODULENAME</th>
<th>LENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICHDEX01</td>
<td></td>
<td>232</td>
</tr>
<tr>
<td>ICHRX01/02</td>
<td></td>
<td>4,248</td>
</tr>
</tbody>
</table>
### Profile TSO Commands

<table>
<thead>
<tr>
<th>User</th>
<th>Group</th>
<th>Dataset</th>
<th>General Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDUSER</td>
<td>ADDGROUP</td>
<td>ADDSD</td>
<td>RDEFINE</td>
</tr>
<tr>
<td>ALTUSER</td>
<td>ALTGROUP</td>
<td>ALTDSD</td>
<td>RALTER</td>
</tr>
<tr>
<td>DELUSER</td>
<td>DELGROUP</td>
<td>DELDSD</td>
<td>RDELETE</td>
</tr>
<tr>
<td>LISTUSER</td>
<td>LISTGRP</td>
<td>LISTDSD</td>
<td>RLIST</td>
</tr>
<tr>
<td>PASSWORD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHRASE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CONNECT</td>
<td></td>
<td>PERMIT</td>
</tr>
<tr>
<td></td>
<td>REMOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Other TSO Commands

<table>
<thead>
<tr>
<th></th>
<th>Console Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>SETROPTS</td>
<td>DISPLAY</td>
</tr>
<tr>
<td>RVARY</td>
<td>RESTART</td>
</tr>
<tr>
<td>SEARCH</td>
<td>SET</td>
</tr>
<tr>
<td>HELP</td>
<td>STOP</td>
</tr>
<tr>
<td></td>
<td>TARGET</td>
</tr>
</tbody>
</table>

### Console Commands

<table>
<thead>
<tr>
<th></th>
<th>Console Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRRDPI00</td>
<td>DISPLAY</td>
</tr>
<tr>
<td>RACDCERT</td>
<td>RESTART</td>
</tr>
<tr>
<td>RACLINK</td>
<td>SET</td>
</tr>
<tr>
<td>RACMAP</td>
<td>STOP</td>
</tr>
<tr>
<td></td>
<td>TARGET</td>
</tr>
</tbody>
</table>
RACF Components - Software - Utilities

- IRRMIN00  RACF Initialization Utility (also use to update templates)
- IRRIRA00  RACF Internal Reorganize Alias Utility
- IRRUT100  RACF Cross Reference Utility
- IRRUT200  RACF Database Verification Utility (use for backup)
- BLKUPD   RACF Block Update Utility (a.k.a. IRRUT300)
- IRRUT400  RACF Database Split/Merge/Extend Utility
- ICHDSM00  RACF Data Security Monitor (a.k.a. DSMON)
- IRRDBU00  RACF Database Unload Utility
- IRRRID00  RACF Remove ID Utility
- IRRADU00  RACF SMF Data Unload Utility
- RACFRW   RACF Report Writer

- In environments where multiple z/OS systems share a RACF database, run utilities on the system with the latest z/OS release and maintenance
Unsupported RACF utilities

- Various programs provided “as is” with no formal support
- Available via the 'Downloads' link in the 'Resources' tab on the RACF webpage at www.ibm.com/racf
- Examples:
  - CDT2DYN - Convert installation ICHRRCDE defined classes to Dynamic CDT profiles
  - CUTPWHIS - Remove old password history entries (Obsolete with APAR AO43999)
  - DBSYNC - Builds RACF commands to synchronize databases
  - irrhfsu - C program to unload HFS FSPs, like IRRDBU00
  - IRRXUTIL - REXX programs using the IRRXUTIL R_admin callable service interface
  - PWDCOPY - Copy cyphered passwords between RACF data bases
  - RACFDB2 - Migrate DB2 access controls to RACF profiles
  - RACKILL - Unconditionally deletes profiles
- Detailed instructions included with each utility on website
RACF Components - RACF Subsystem

- Not required for ordinary RACF processing

- Provides support for ...
  - Entry of RACF commands via the console
  - RACF Remote Sharing Facility (RRSF)
  - APPC Persistent Verification (PV)
  - R_admin (IRRSEQ00) callable service
  - Key generation for the Network Authentication Server (IBM Kerberos)
  - Password and password phrase enveloping
  - LDAP event notification
  - SAFTRACE

- Recommend implementation to facilitate recovery by the entry of RACF commands via the console

- Recommend configuring RACF subsystem to load command parsing table IRRDPI00 at IPL
System Authorization Facility (SAF)

- SAF - System Authorization Facility
  - Receives and passes RACROUTE requests to the External Security Manager (e.g., RACF)
  - Issues a SAF Return Code (RC) to accompany the RACF Return Code (RC)

- SAF Exits
  - ICHRTX01 - Pre-MSI (Master Scheduler Initialization)
  - ICHRTX00 - Post-MSI (Master Scheduler Initialization)
  - Can optionally set RC and bypass further checking
  - Can optionally modify the RACROUTE parameters before further checking is performed
  - Not invoked for authorization checks which are made as part of RACF callable service checks
SETROPTS

- SETROPTS - SET RACF OPTIONS
  - Defines system-wide RACF security and auditing options
  - Options reside in RACF Database ICB (Inventory Control Block)

- TSO Command - SETROPTS option-operand(s) | LIST
  - LIST - display options
  - Use of command always logged

- Authority to execute
  - SPECIAL List and set security options only
  - AUDITOR List all options and set auditing options
  - ROAUDIT (z/OS 2.2) List all options
  - Group-AUDITOR List all options
  - OPERCMDS racf-subsystem.SETROPTS Execute commands via the console
    - READ LIST
    - UPDATE All other operands

- Setting options on a particular resource class (e.g., TCICSTRN) affects all classes with the same POSIT value
SETROPTS LIST

ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
STATISTICS = DATASET GTERMINL TERMINAL
AUDIT CLASSES = DATASET USER GROUP DASD VOL GDASD VOL GTERMINL TERMINAL
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM ACICSPCT APPL BCICSPCT CCICSCMD
                     CDT CONSOLE DASD VOL DCICSDCT DSNR ECICSDCT FACILITY FCICSFCT
                     FSSEC GCICSTRN GDASD VOL GSDSF GTERMINL HCICSFCT JCICSJCT
                     KCICSCJT LOGSTRM MCISCOPT NCICSPPT OPERCMDS PCICSPSB
                     PMBR PROGRAM PROPCTL QCICSPSB RACF VARS RRSFDATA RVARSMBR
                     SCICSTST SDFS SERVER STARTED SURROGAT TCI CSTRN TEMPDSN
                     TERMINAL TSOAUTH TSOPROC UCI CSTST UNIXPRIV VCICSCMD
GENERIC PROFILE CLASSES = DATASET DASD VOL FACILITY PROGRAM TCI CSTRN TERMINAL
GENERIC COMMAND CLASSES = DATASET ACCTNUM DASD VOL FACILITY FIELD PERFGRP
                     PROGRAM T@TESTRN TCI CSTRN TERMINAL TSOAUTH TSOPROC
GENLIST CLASSES = NONE
GLOBAL CHECKING CLASSES = DATASET FACILITY TERMINAL
SETR RACLST CLASSES = APPL CDT DSNR FACILITY STARTED TSOAUTH TSOPROC
GLOBAL=YES RACLST ONLY = TCI CSTRN
LOGOPTIONS "ALWAYS" CLASSES = SURROGAT
LOGOPTIONS "NEVER" CLASSES = NONE
LOGOPTIONS "SUCCESSES" CLASSES = NONE
LOGOPTIONS "FAILURES" CLASSES = FACILITY
LOGOPTIONS "DEFAULT" CLASSES = DATASET ACCTNUM ACICSPCT ALCSAUTH APPCLU
                     ... VTAMAPPL VXMBR WIMS WRITER
AUTOMATIC DATASET PROTECTION IS IN EFFECT
ENHANCED GENERIC NAMING IS IN EFFECT
REAL DATA SET NAMES OPTIONS IS INACTIVE
JES-BATCHALLRACF OPTION IS INACTIVE
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
PROTECT-ALL OPTION IS NOT IN EFFECT
TAPE DATA SET PROTECTION IS INACTIVE
SECURITY RETENTION PERIOD IN EFFECT IS 9999 DAYS.
ERASE-ON-SCRATCH IS INACTIVE
SINGLE LEVEL NAME PREFIX IS LVL1X
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
NO DATA SET MODELLING IS BEING DONE.
PASSWORD PROCESSING OPTIONS

THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
New - APAR OA43999 and z/OS 2.2

PASSWORD CHANGE INTERVAL IS 45 DAYS.
PASSWORD MINIMUM CHANGE INTERVAL IS 3 DAYS.
MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
SPECIAL CHARACTERS ARE ALLOWED.
10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
AFTER 4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
A USERID WILL BE REVOKED.
PASSWORD EXPIRATION WARNING LEVEL IS 5 DAYS.

INSTALLATION PASSWORD SYNTAX RULES:
RULE 1 LENGTH(5:8)  ********
RULE 2 LENGTH(6:8)  LLLLLLLL

LEGEND:
A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING
C-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-SPECIAL
x-MIXEDALL

INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
SECLEVELAUDIT IS INACTIVE
SECLABEL AUDIT IS NOT IN EFFECT
SECLABEL CONTROL IS NOT IN EFFECT
GENERIC OWNER ONLY IS NOT IN EFFECT
COMPATIBILITY MODE IS NOT IN EFFECT
MULTI-LEVEL QUIET IS NOT IN EFFECT
MULTI-LEVEL STABLE IS NOT IN EFFECT
NO WRITE-DOWN IS NOT IN EFFECT
MULTI-LEVEL ACTIVE IS NOT IN EFFECT
CATALOGUED DATA SETS ONLY, IS NOT IN EFFECT
USER-ID FOR JES NJEUSERID IS : ????????
USER-ID FOR JES UNDEFINEDUSER IS : ++++++++ 
PARTNER LU-VERIFICATION SESSIONKEY INTERVAL DEFAULT IS 30 DAYS.
APPLAUDIT IS IN EFFECT
ADDCREATOR IS NOT IN EFFECT
KERBLVL = 0
MULTI-LEVEL FILE SYSTEM IS NOT IN EFFECT
MULTI-LEVEL INTERPROCESS COMMUNICATIONS IS NOT IN EFFECT
MULTI-LEVEL NAME HIDING IS NOT IN EFFECT
SECURITY LABEL BY SYSTEM IS NOT IN EFFECT
PRIMARY LANGUAGE DEFAULT : ENU / ENGLISH
SECONDARY LANGUAGE DEFAULT : ENU / ENGLISH
Access Authorization

- RACF determines whether a user is authorized to access a resource at the requested level of access (e.g., READ) based on resource profiles defined in its database.

- Resource Managers use RACF authorization macros to call RACF:
  - RACHECK or FRACHECK
  - RACROUTE REQUEST=AUTH or FASTAUTH

    RACROUTE REQUEST=AUTH,USERID='GSMITH',ENTITY='$RSH.PRIV',
    CLASS='FACILITY',ATTR='READ',LOG=NONE

- RACF sends a Return Code (RC) back to the calling Resource Manager indicating the results of the authorization check:
  - 0  Authorized
  - 4  Not-Protected
  - 8  Not-Authorized
Access Authorization

- Resource profile types
  - Discrete - Fully qualified resource name match
  - Generic - Partially qualified resource name masking
  - Grouping - Set of dissimilar full and masked resource names

- RACF uses the most specific profile (i.e., closest match to the resource name) for determining access authorization
  - First Discrete, then Generic
  - Generic with most matching non-masking characters, from left to right

PAY.PROD.MASTER.EMPLOYEE
PAY.PROD.MASTER.* ← PAY.PROD.MASTER.BKUP
PAY.PROD.*.EMPLOYEE ← PAY.PROD.CHECKS.TAPE
PAY.PROD.**
PAY.**

Profiles are sequenced based on EBCDIC characters rather than ASCII
Generic Profiles

- Offer one-to-many relationship of profile to resource protected
- Use masking characters to match multiple resources

Masking characters - in order of precedence in specificity

- % Single substitute character
- * Any set of substitute characters or one qualifier
- ** Any set of substitute characters, zero or more qualifiers

- For Datasets, use of ** requires SETROPTS EGN (Enhanced Generic Naming) option be activated
- Usage and behavior of the masking characters differs based on whether the profile is a Dataset or General Resource

- RACF Variables - defined in the RACFVARS class
  - Have an & prefix (e.g., &RACLNDE) - considered more specific than %, *, or **
  - Can be incorporated into General Resource profiles (e.g., JESSPOOL &RACLNDE.**)
  - Are assigned character string values used in matching resource names
Access Authorization Decision Logic

Not RESTRICTED

Resource Class Active (& RACLISTed if Required)

Yes → PRIVILEGED or TRUSTED Started Task

Yes → 0

No → 4

AUTH / FASTAUTH Pre/Post-Processing Exits
ICHRCX01 - 02 / ICHRFX01 - 04

Pass → 0

Fail → 8

Global Access Table - Requested ≤ Allowed Access

Yes → 0

No

Profile Found in Database
(If No, CDT DFTRETC=0/4/8 or PROTECTALL)

No → 4

Yes → 0

User "Owns" the Resource
USERID = Dataset HLQ, JES Spool SYSOUT Owner

Yes → 0

No → A
Access Authorization Decision Logic

1. USERID in Access List - Requested ≤ Allowed Access
   - Not Auth
   - Not Listed
   - Yes → 0

2. Group(s) in Access List - Requested ≤ Allowed Access
   - Not Auth
   - Not Listed
   - Yes → 0

3. ID(*) in Access List - Requested ≤ Allowed Access
   - Not Auth
   - Not Listed
   - Not have a RACF USERID
   - Yes → 0

4. Requested Access ≤ UACC
   - Yes → 0
   - No

5. OPERATIONS Authority Allows Access
   - Yes → 0
   - No

6. USERID, Group(s), ID(*) PROGRAM, TERMINAL, CONSOLE, or JESINPUT in Conditional Access List - Requested ≤ Allowed Access
   - Not Auth
   - Not Listed
   - No → 0

7. Profile in WARN Mode
   - Yes → 0
   - No → 8
PRIVILEGED and TRUSTED Authority

- Grants unrestricted access to all resources and assigns z/OS UNIX Superuser (uid 0) authority
- Only applies to Started Tasks
  - Assigned via STARTED class profiles or ICHRIN03 table entries
  - Authority is assigned to the task itself, not to its ID
  - Authority does not transfer to batch jobs submitted by the Started Task
- TRUSTED can be logged via UAUDIT or SETROPTS LOGOPTIONS
- TRUSTED should always be used instead of PRIVILEGED

IBM recommended TRUSTED Started Tasks

<table>
<thead>
<tr>
<th>APSWPROx(^{(1)})</th>
<th>CATALOG</th>
<th>CEA(^{(2)})</th>
<th>DFHSM(^{(1)})</th>
<th>DFS(^{(1)})</th>
</tr>
</thead>
<tbody>
<tr>
<td>DUMPSRV</td>
<td>GPMSERVE(^{(1)})</td>
<td>HIS</td>
<td>IEEVMPCR</td>
<td>IOSAS</td>
</tr>
<tr>
<td>IXGLOGR</td>
<td>JESn</td>
<td>JESXCF</td>
<td>JES3AUX</td>
<td>LLA</td>
</tr>
<tr>
<td>NFS</td>
<td>OMVS(^{(1)})</td>
<td>RACF</td>
<td>RMF</td>
<td>RMFGAT</td>
</tr>
<tr>
<td>SMF</td>
<td>SMS</td>
<td>SMSPDSE1</td>
<td>SMSVSAM(^{(1)})</td>
<td>TCPIP</td>
</tr>
<tr>
<td>VLF</td>
<td>VTAM</td>
<td>WLM</td>
<td>XCFAS</td>
<td>ZFS(^{(1)})</td>
</tr>
</tbody>
</table>

\(^{(1)}\) Optional
\(^{(2)}\) If using z/OSMF ISPF
### DSMON - Started Task Report

**R A C F  S T A R T E D  P R O C E D U R E S  T A B L E  R E P O R T**

**FROM PROFILES IN THE STARTED CLASS:**

<table>
<thead>
<tr>
<th>PROFILE NAME</th>
<th>ASSOCIATED USER</th>
<th>ASSOCIATED GROUP</th>
<th>PRIVILEGED</th>
<th>TRUSTED</th>
<th>TRACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASAM</td>
<td>CASAM</td>
<td></td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>CICSP01.* (G)</td>
<td>CICSPRD1</td>
<td>STASKGP</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>CICST01,CICTEST</td>
<td>=MEMBER</td>
<td>STCTEST</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>CICS* (G)</td>
<td>=MEMBER</td>
<td>CICSTSKS</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>DUMPSRV.* (G)</td>
<td>MVSSYST</td>
<td>STASKGP</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>HSERVER.* (G)</td>
<td></td>
<td></td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>NETA.* (G)</td>
<td>=STDATA NOT SPECIFIED, ICHRIN03 WILL BE USED-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>** (G)</td>
<td>DFLTSTC</td>
<td>STASKGP</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

=MEMBER - assign ID matching PROC name

If assigned USERID does not exist, runs with no ID

Report not generated if STARTED is not active

**R A C F  S T A R T E D  P R O C E D U R E S  T A B L E  R E P O R T**

**FROM THE STARTED PROCEDURES TABLE (ICHRIN03)**

<table>
<thead>
<tr>
<th>PROCEDURE NAME</th>
<th>ASSOCIATED USER</th>
<th>ASSOCIATED GROUP</th>
<th>PRIVILEGED</th>
<th>TRUSTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>JES2</td>
<td>JES2</td>
<td></td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>CICSTOR</td>
<td>CICSPRD</td>
<td>CICSSYS</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>CICSAOR</td>
<td>CICSPRD</td>
<td>CICSSYS</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>NETA</td>
<td>$SNETA</td>
<td>NTWKSTC</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>NETB</td>
<td>$SNETB</td>
<td>NTWKSTC</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>RCVRY</td>
<td>SYSRCVRY</td>
<td></td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>*</td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

* - all PROCs not specified above

= - assign ID matching PROC name
Global Access Table

- Performance enhancement tool
  - Grants immediate access to resources without checking profiles or logging access
  - Used to grant all users access to common shared resources
- Comprised of GLOBAL class profiles which contain access granting entries
  - GLOBAL class profiles are the names of other classes
    - RDEF GLOBAL DATASET
  - Entries are defined as GLOBAL profile members
    - RALT GLOBAL DATASET ADDMEM('CATLG.*'/READ)
    - Entries
      - Discrete or Generic - follows generic profile rules for General Resources
      - Need not match profile(s) protecting the resource(s)
      - For datasets, if not enclosed in quotes, appends user's USERID as the first qualifier
    - Access-levels - ALTER | CONTROL | UPDATE | READ | NONE (not EXECUTE)
    - Use DELMEM to delete entries
- Special Variables - Used in resource names
  - &RACUID Substitute with requesting user's USERID
  - &RACGPID Substitute with requesting user’s current connect group
## DSMON - Global Access Table

<table>
<thead>
<tr>
<th>CLASS</th>
<th>ACCESS</th>
<th>ENTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATASET</td>
<td>ALTER</td>
<td>&amp;RACUID.*</td>
</tr>
<tr>
<td></td>
<td>READ</td>
<td>CATLG.*</td>
</tr>
<tr>
<td></td>
<td>READ</td>
<td>ISP.*</td>
</tr>
<tr>
<td></td>
<td>READ</td>
<td>PROD.*.LIB</td>
</tr>
<tr>
<td></td>
<td>UPDATE</td>
<td>SYS1.BRODCAST</td>
</tr>
<tr>
<td></td>
<td>NONE</td>
<td>SYS1.RACF.*</td>
</tr>
<tr>
<td></td>
<td>READ</td>
<td>SYS1.*</td>
</tr>
<tr>
<td>DASDVOL</td>
<td>--</td>
<td>-- GLOBAL INACTIVE --</td>
</tr>
<tr>
<td>TERMINAL</td>
<td>--</td>
<td>-- NO ENTRIES --</td>
</tr>
<tr>
<td>FACILITY</td>
<td>READ</td>
<td>STGADMIN.ARC.ENDUSER.*</td>
</tr>
</tbody>
</table>

Access Level of NONE to SYS1.RACF.* causes RACF to skip the GAT and check the profile

**Concern:** There may be SYS1-prefixed profiles with UACCs less than READ, and the SYS1.* entry would allow access.
Profile Not Found

- The Return Code (RC) for a profile ‘not found’ is determined by the CDT
  - DFTRETC parameter 0 | 4 | 8 (Allow | Not Protected | Deny)
  - DFTRETC=8 Classes (* - includes grouping class)

<table>
<thead>
<tr>
<th>Class</th>
<th>Class</th>
<th>Class</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPCSERV</td>
<td>APPCTP</td>
<td>CBIND</td>
<td>CONSOLE</td>
</tr>
<tr>
<td>DCEUUIDS</td>
<td>DIRACC</td>
<td>DIRAUTH</td>
<td>DIRECTRY</td>
</tr>
<tr>
<td>DIRSRCH</td>
<td>FILE</td>
<td>FSOBJ</td>
<td>FSSEC</td>
</tr>
<tr>
<td>IPCOBJ</td>
<td>JESINPUT</td>
<td>JESJOBS</td>
<td>JESSPOOL</td>
</tr>
<tr>
<td>KEYSMSTR</td>
<td>MQADMIN*</td>
<td>MQCHAN*</td>
<td>MQCMDS</td>
</tr>
<tr>
<td>MQCONN</td>
<td>MQNLIST*</td>
<td>MQPROC*</td>
<td>MQQUEUE*</td>
</tr>
<tr>
<td>MXADMIN*</td>
<td>MXNLIST*</td>
<td>MXPROC</td>
<td></td>
</tr>
<tr>
<td>MXTOPIC*</td>
<td>PROCACT</td>
<td>PROCESS</td>
<td>PSFMPL</td>
</tr>
<tr>
<td>RACFHC</td>
<td>ROLE</td>
<td>SECLABEL</td>
<td>SFSCMD</td>
</tr>
<tr>
<td>SERVER</td>
<td>SOMDOBJS*</td>
<td>TEMPDSN</td>
<td>TMEADMIN</td>
</tr>
<tr>
<td>WRITER</td>
<td>XCSFKEY</td>
<td>XFACILIT*</td>
<td></td>
</tr>
</tbody>
</table>

- Calling process decides how to react to Return Code
OPERATIONS Authority

- User and Group-connect attribute
  
  ```
  LU RSHTES
  USER=RSHTES  NAME=RSH RACF TEST ID  OWNER=RACFTEST  CREATED=09.292
  ATTRIBUTES=OPERATIONS
  ```

- Grants ALTER level access when the user has **not** been permitted access

- Only applies to resources whose classes have been defined with OPER=YES in RACF's Class Descriptor Table (CDT)

- IBM provided classes with OPER=YES - z/OS and z/VM:
  
  ```
  DATASET  DASDVOL  DIRECTORY  FILE  GDASDVOL
  PSFMPL   NETCMDS  NETSPAN   RODMMGR  TAPEVOL
  VMBATCH  VMCMDB   VMMDISK   VMNODE   VMRDR
  ```

- Can be restricted by explicitly permitting the ID or a connect group of an OPERATIONS user a lower level of access
DSMON - OPERATIONS Authority

R A C F C L A S S D E S C R I P T O R T A B L E R E P O R T

<table>
<thead>
<tr>
<th>CLASS NAME</th>
<th>STATUS</th>
<th>AUDITING</th>
<th>STATISTICS</th>
<th>DEFAULT</th>
<th>OPERATIONS ALLOWED</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCTNUM</td>
<td>ACTIVE</td>
<td>NO</td>
<td>NO</td>
<td>NONE</td>
<td>NO</td>
</tr>
<tr>
<td>APPL</td>
<td>ACTIVE</td>
<td>NO</td>
<td>NO</td>
<td>NONE</td>
<td>NO</td>
</tr>
<tr>
<td>DASDVOL</td>
<td>ACTIVE</td>
<td>YES</td>
<td>NO</td>
<td>ACEE</td>
<td>YES</td>
</tr>
<tr>
<td>RACFVARS</td>
<td>ACTIVE</td>
<td>NO</td>
<td>NO</td>
<td>NONE</td>
<td>NO</td>
</tr>
<tr>
<td>T@TESTRN</td>
<td>ACTIVE</td>
<td>NO</td>
<td>NO</td>
<td>NONE</td>
<td>NO</td>
</tr>
<tr>
<td>TCICSTRN</td>
<td>ACTIVE</td>
<td>NO</td>
<td>NO</td>
<td>NONE</td>
<td>NO</td>
</tr>
<tr>
<td>TERMINAL</td>
<td>ACTIVE</td>
<td>YES</td>
<td>YES</td>
<td>ACEE</td>
<td>NO</td>
</tr>
<tr>
<td>TESTAPP</td>
<td>INACTIVE</td>
<td>NO</td>
<td>NO</td>
<td>READ</td>
<td>YES</td>
</tr>
</tbody>
</table>

(D) signifies installation class defined by CDT class profile

S E L E C T E D U S E R A T T R I B U T E R E P O R T

<table>
<thead>
<tr>
<th>USERID</th>
<th>ATTRIBUTE TYPE</th>
<th>REVOKE</th>
<th>NODE.USERID...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHILL03</td>
<td>SPECIAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDITJH</td>
<td>OPERATIONS</td>
<td></td>
<td>SYSTEM</td>
</tr>
<tr>
<td>CICS01</td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSTMARR4</td>
<td>GROUP</td>
<td></td>
<td>SYSTEM</td>
</tr>
<tr>
<td>JSMITH1</td>
<td>GROUP</td>
<td></td>
<td>GROUP</td>
</tr>
<tr>
<td>IBMUSER</td>
<td>SYSTEM</td>
<td></td>
<td>GROUP</td>
</tr>
<tr>
<td>RHOMES1</td>
<td>SYSTEM</td>
<td></td>
<td>GROUP</td>
</tr>
<tr>
<td>RJONES2</td>
<td>SYSTEM</td>
<td></td>
<td>SYSTEM</td>
</tr>
<tr>
<td>SECUSR02</td>
<td>SYSTEM</td>
<td></td>
<td>SYSTEM</td>
</tr>
</tbody>
</table>
Monitoring

- **RACF terminology - AUDITING**

- **Monitoring options can be specified in**
  - User profile: `UAUDIT`
  - Resource profile: `AUDIT(options(access-level)), GLOBALAUDIT(-same-)`
    - Audit options: SUCCESS, FAILURES, ALL, NONE
    - Default: `AUDIT(FAILURES(READ))`
  - SETROPTS Options: `AUDIT(class), LOGOPTIONS(level(class))`
    - Levels: ALWAYS, NEVER, SUCCESSES, FAILURES, DEFAULT
  - RACROUTE Macro `LOG=` parameter (e.g., `AUTH: NONE | NOSTAT | NOFAIL | ASIS`)

- System AUDITOR authority is required to change most monitoring options

- **RACF auditing generates System Management Facilities (SMF) records**
  - 80 RACF Processing - Logon and access events
  - 81 RACF Initialization - IPL
  - 83 RACF Audit - Subtypes 1 (Dataset SECLABEL), 2 (EIM), 3 (LDAP), 4 (R-auditx), 5 (WebSphere), 6 (TKLM)
Administrative Authorities

- **System and Group Authorities**
  - **SPECIAL** Administer RACF profiles, view non-audit options, and set control options
  - **AUDITOR** View RACF profiles, view all options, and set audit options
  - **ROAUDIT** (z/OS 2.2) View RACF profiles and view all options - System level only
  - **OPERATIONS** Access resources, create group datasets, and define group dataset profiles
  - Group authorized limited by "Scope of Groups" (follows profile ownership chain)

- **Profile Owner** - change, delete profile

- **Group Connect Authorities** - **USE, CREATE, CONNECT, JOIN**

- **Other Authorities**
  - **ALTER** access to a Discrete profile - change, delete, permit access
  - Class Authorization - CLAUTH(class) - delegate user or resource profile creation
  - FACILITY class IRR profiles - password reset (e.g., IRR.PWRESET.TREE.group)
  - FIELD class profile - delegate profile segment administration (e.g., USER.OMVS.UID)
Troubleshooting Access Problems

- Access violations ordinarily result in the generation of an ICH408I message
  - Messages are suppressed if RACROUTE parameters specify either MSGSUPP=YES or a LOG= option other than ASIS

- ICH408I messages are displayed on the console and in the system log (SYSLOG), and can be viewed via the LOG command in SDSF or with an equivalent product (e.g., EJES)
  - ICH408I messages appear in the log of the system where the event occurred, and it may be necessary to check the system logs of all systems to find an event

- The violation message displayed to the user is determined by the calling resource manager and may not be as informative as the associated ICH408I message

- RACF messages are listed and explained in the Security Server (RACF) Messages and Codes manual
• ICH408I Message

  USER(userid) GROUP(group) NAME(user-name) -- or --
  JOB(jobname) STEP(stepname) (no ACEE)
  [ SUBMITTER(submitter's-userid) ]
  [ resource-name ]
  [ CL(class-name) ]
  [ VOL(volser) ] [ FID(file-identifier) ] [ ID(IPC-identifier) ]
  [ reason-for-failure ]
  [ FROM(generic-profile) (G) ]
  [ ACCESS INTENT(access) ACCESS ALLOWED(access) ]
  [ EFFECTIVE UID(uid#) ]
  [ EFFECTIVE GID(gid#) ]

  VOL for VSAM files is the volser of the catalog, not its location

  For Member/Grouping classes, only the Member class is shown
Troubleshooting Access Problems

- Common *reason-for-failure* messages
  - INSUFFICIENT ACCESS AUTHORITY
  - DEFINE - INSUFFICIENT AUTHORITY (create dataset)
  - RESOURCE NOT PROTECTED (PROTECTALL)
  - PROFILE NOT FOUND. IT IS REQUIRED FOR AUTHORIZATION CHECKING (DFTRETC=8)
  - WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED (WARNING)
  - RENAME - INSUFFICIENT AUTHORITY
  - LOGON/JOB INITIATION -
    - INVALID PASSWORD ENTERED AT TERMINAL *terminal-id*
    - EXCESSIVE PASSWORDS OR INACTIVE USER
    - REVOKED USER ACCESS ATTEMPT
    - NOT AUTHORIZED TO APPLICATION (APPL)
    - SUBMITTER NOT AUTHORIZED BY USER (SURROGAT)
    - NOT AUTHORIZED TO SUBMIT JOB *jobname* (JESJOBS)
Troubleshooting Access Problems

- Sample ICH408I Messages

ICH408I USER(RSMITH ) GROUP(DEPTJ ) NAME(R.L.SMITH )
ICH408I FIN.CLIST.CNTL CL(DATASET ) VOL(TSO042)
ICH408I INSUFFICIENT ACCESS AUTHORITY
ICH408I FROM FIN.CLIST.** (G)
ICH408I ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )

ICH408I USER($FIN01 ) GROUP(#BATCH ) NAME(FIN PROD )
ICH408I PAY.MASTER.FILE CL(DATASET ) VOL(RSV064)
ICH408I SUBMITTER(CA7 )
ICH408I WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED
ICH408I FROM PAY.MASTER.*.** (G)
ICH408I ACCESS INTENT(UPDATE ) ACCESS ALLOWED(READ )

ICH408I USER(RSHTEST ) GROUP(RSHDFTST) NAME(RSH TEST ID )
LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL TCP00017
## RACF Health Checks

<table>
<thead>
<tr>
<th>CHECK</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF_AIM_STAGE</td>
<td>Reports if RACF database is not AIM Stage 3</td>
</tr>
<tr>
<td>RACF_BATCHALLRACF</td>
<td>Verifies the SETROPTS option is active</td>
</tr>
<tr>
<td>RACF_CERTIFICATE_EXPIRATION</td>
<td>Reports certificates expiring in 90 days</td>
</tr>
<tr>
<td>RACF_class_ACTIVE</td>
<td>Verifies that the class is active: CFSKEYS, CFSSERV, FACILITY, JESJOBS, JESSPOOL, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV</td>
</tr>
<tr>
<td>RACF_ENCRYPTION_ALGORITHM</td>
<td>Checks password encryption algorithms in use</td>
</tr>
<tr>
<td>RACF_GRS_RLN</td>
<td>Checks to see if any of the RACF ENQ names are on a GRS resource name exclusion list which changes the scope of the RACF ENQ</td>
</tr>
<tr>
<td>RACF_IBMUSER_REVOKED</td>
<td>Verifies that the user ID IBMUSER is revoked</td>
</tr>
<tr>
<td>RACF_ICHAUTAB_NONLPA</td>
<td>RACF_ICHAUTAB_NONLPA raises a SEV(MED) exception if a non-LPA resident ICHAUTAB is found</td>
</tr>
<tr>
<td>RACF_PASSWORD_CONTROLS</td>
<td>Checks mixed-case password and invalid password attempts settings</td>
</tr>
<tr>
<td>RACF_RRSF_RESOURCES</td>
<td>Confirms INMSG and OUTMSG datasets are defined and protected</td>
</tr>
<tr>
<td>RACF_SENSITIVE_RESOURCES</td>
<td>Looks at the current APF data sets, PARMLIB, the System REXX data sets, LINKLIST, and the RACF database data sets and flags those that are improperly protected</td>
</tr>
<tr>
<td></td>
<td>• Are not found on the indicated volume</td>
</tr>
<tr>
<td></td>
<td>• Are improperly protected</td>
</tr>
<tr>
<td></td>
<td>Examines key system general resources</td>
</tr>
<tr>
<td>RACF_UNIX_ID ZOSMIGV1R13_DEFAULT_UNIX_ID</td>
<td>Checks for existence of FACILITY BPX.DEFAULT.USER and BPX.UNIQUE.USER</td>
</tr>
</tbody>
</table>
Common Issues and Concerns

- Implementation and Configuration
  - Resource managers not configured to call RACF
  - Inconsistent access controls protecting resources shared by multiple z/OS images having separate RACF databases

- Users Controls
  - Stronger password protection not used (KDFAES encryption or Mixed-case)
  - PROTECTED attribute not assigned to Batch and Started Task IDs
  - NOINTERVAL assigned to IDs inappropriately
  - SURROGAT access permission allow non-process users to submit jobs with surrogate IDs, especially with high-authority IDs
  - IDs shared by unrelated Started Tasks rather than individual IDs
  - Different types of IDs (e.g., batch, Started Task, FTP, end-user) mixed in same groups, especially those granting access
Common Issues and Concerns

- Resource Protection
  - Generic profile coverage too broad; not sufficiently refined
  - Inappropriate access granted, especially for UACC and ID(*)
  - Excessive use of Started Task TRUSTED authority
  - OPERATIONS authority used instead of storage administrator authority profiles
  - WARNING not monitored or grants use of high powered functions
  - RESTRICTED attribute not used with default or foreign IDs
  - Global Access Table allows access prohibited by resource profiles

- Dataset Protection
  - Tape dataset protection is not active
  - Temporary dataset protection TEMPDSN class is not active
  - BLP and tape dataset protection bypass permissions too liberal
  - Inappropriate ALTER access is granted to catalogs
  - Excessive access granted system datasets, especially UPDATE
  - Erase-on-Scratch is not used
Common Issues and Concerns

- General Resource Protection
  - Classes are not active
  - RACLIST-required classes not RACLISTed
  - All resources in a class are not protected comprehensively - no ** profile
  - Locally-defined resource classes have OPERATIONS authority access enabled

- Monitoring/Auditing
  - Profile AUDIT options are not set to capture important events (e.g., violations)
  - SETROPTS AUDIT not active for all classes
  - SETROPTS LOGOPTIONS(FAILURES(class)) not set for UNIX classes
  - SETROPTS LOGOPTIONS(SUCCESS(SURROGAT FSSEC)) not set
  - Reporting tools not used effectively
Common Issues and Concerns

- **Administration**
  - SPECIAL and AUDITOR assigned too liberally or to process IDs (e.g., Batch)
  - Profiles owned by users instead of groups
  - OPERATIONS not restricted with access exclusion group
  - Group connect, CLAUTH, FIELD, and IRR profiles assigned inappropriately

- **Maintenance**
  - Entry of RACF commands via console not tested regularly
  - PROGRAM profiles are outdated - reference libraries that are no longer valid and therefore do not protect the program
  - RACF Database not backed up properly or checked regularly for integrity
  - Healthchecks not monitored regularly
  - Resource owners not assigned or involved in granting access
  - No formal Mainframe/RACF security policy or standards exist
  - RACF admin function understaffed and under trained
RACF In Relation To Other Security

- Security Hierarchy (descending)
  - Application Level Security
  - System Software Security
  - RACF
  - z/OS Integrity
  - Software Change Control
  - Physical Security
  - Policies, Standards, and Procedures

- RACF can be circumvented or incapacitated by security failures at other levels