RSH CONSULTING

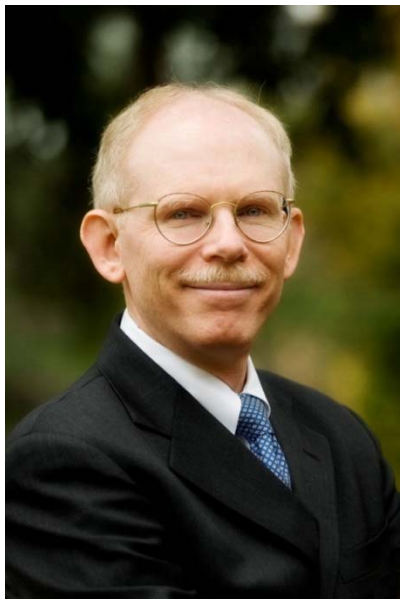
RACF - The Essentials For Systems Programmers

SPARTA - June 2017

RSH Consulting - Robert S. Hansel

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

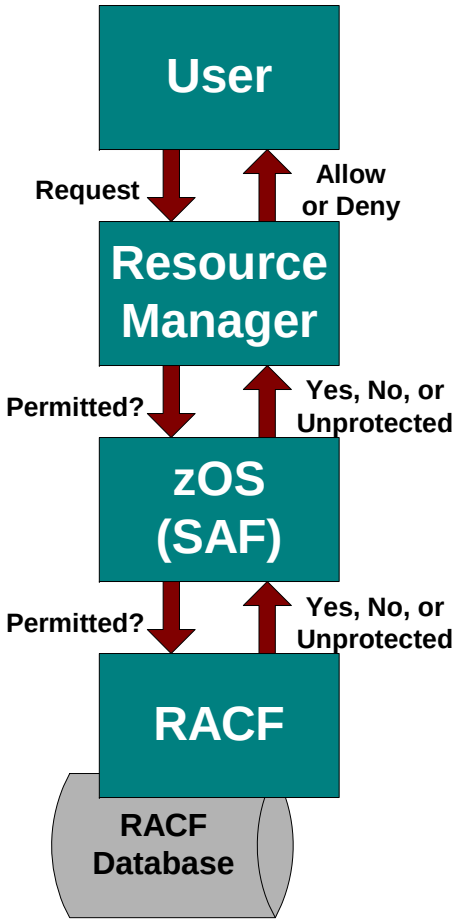
- Resource Access Control Facility (RACF)
- IBM's Security Software Product for MVS, OS/390, and z/OS
- First introduced in 1976
- Component of IBM's z/OS Security Server
- Comprised of:
  - Database (Primary and Backup Pair)
    - Profiles - Users, Groups, Datasets, General Resources
  - Software
    - Programs
    - Macros - RACROUTE
    - TSO Commands
    - Utilities

RACF Functions

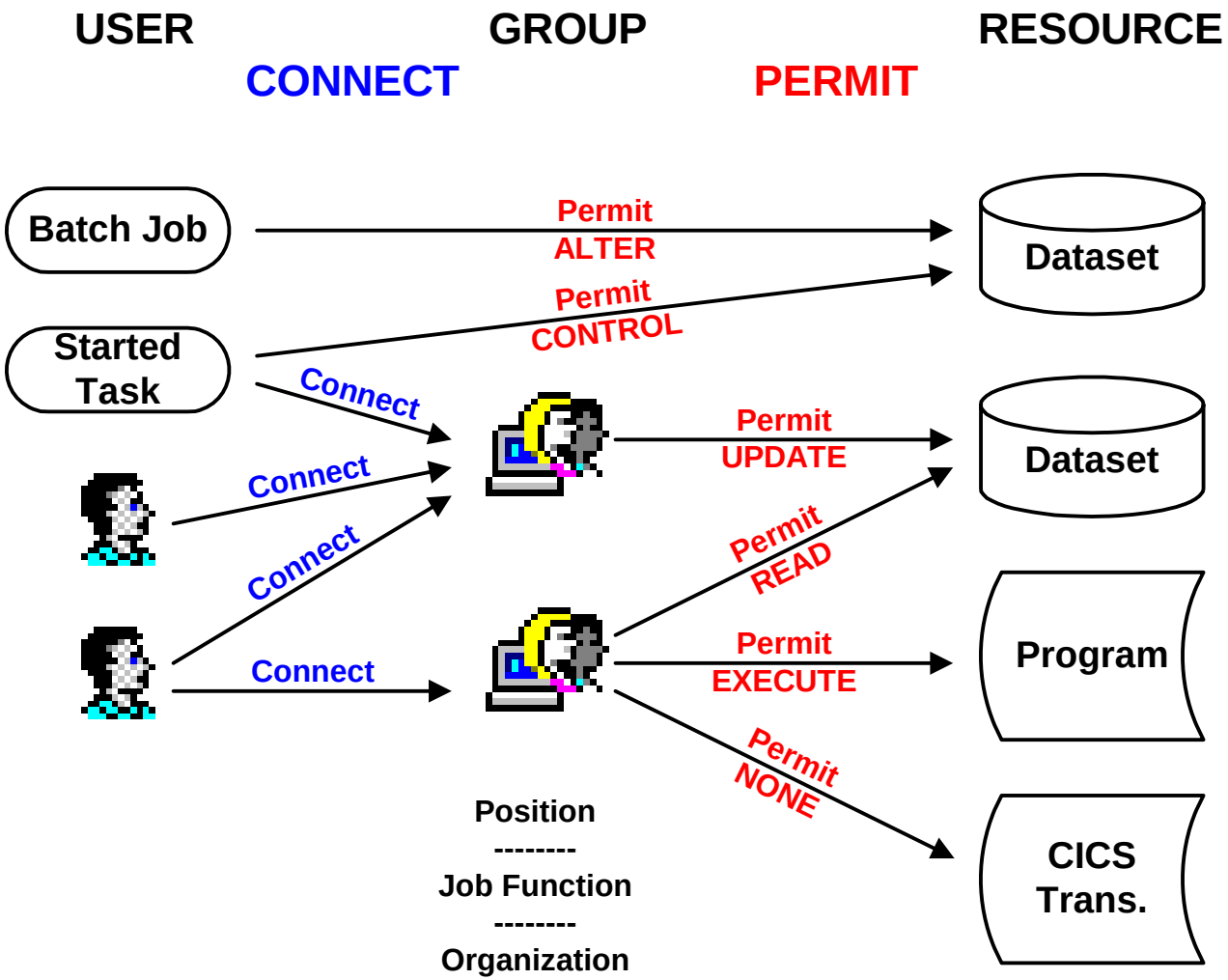
- User Identification and Authentication
- Resource Access Authorization
- Monitor User Activity
- Access Administration

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



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)

RACF Components - Database - RVARY LIST

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 ===>
                                                                More:
Data Set Name . . . . : SYS1.RACFPRM1

General Data                              Current Allocation
 Management class . . : **None**           Allocated cylinders : 3
 Storage class  . . . : **None**           Allocated extents . : 1
  Volume serial . . . : VPMVSH
  Device type . . . . : 3390
 Data class . . . . . : **None**
  Organization  . . . : PSU               Current Utilization
  Record format . . . : F                  Used cylinders  . . : 3
  Record length . . . : 4096               Used extents  . . . : 1
  Block size  . . . . : 4096
  1st extent cylinders: 3
  Secondary cylinders : 0                 Dates
  Data set name type  :                    Creation date . . . : 1993/06/20
                                           Referenced date . . : 2017/02/22
                                           Expiration date . . : ***None***
  SMS Compressible  . : NO
```

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 - ICHRRNG
  - 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 (RACLIST) 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

```
R A C F      E X I T S      R E P O R T
EXIT MODULE              MODULE
NAME                     LENGTH
-------------------------------------------------------------------------
ICHDEX01                    232
ICHRCX02                  4,248
```

RACF Components - Software - Commands

Profile TSO Commands			
User	**Group**	**Dataset**	**General Resource**
ADDUSER ALTUSER DELUSER LISTUSER PASSWORD PHRASE	ADDGROUP ALTGROUP DELGROUP LISTGRP	ADDSD ALTDSD DELDSD LISTDSD	RDEFINE RALTER RDELETE RLIST
CONNECT REMOVE		PERMIT	

Other TSO Commands		Console Commands
SETROPTS	IRRDPI00	DISPLAY
RVARY	RACDCERT	RESTART
SEARCH	RACLINK	SET
HELP	RACMAP	STOP
		TARGET

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

RACF Components - Software - Utilities

- 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

```
SETROPTS LIST
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
STATISTICS = DATASET GTERMINL TERMINAL
AUDIT CLASSES = DATASET USER GROUP DASDVOL GDASDVOL GTERMINL TERMINAL
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM ACICSPCT APPL BCICSPCT CCICSCMD
                 CDT CONSOLE DASDVOL DCICSDCT DSNR ECICSDCT FACILITY FCICSFCT
                 FSSEC GCICSTRN GDASDVOL GSDSF GTERMINL HCICSFCT JCICSJCT
                 KCICSJCT LOGSTRM MCICSPPT NCICSPPT OPERCMDS PCICSPSB
                 PMBR PROGRAM PROPCNTL QCICSPSB RACFVARS RRSFDATA RVARSMBR
                 SCICSTST SDSF SERVER STARTED SURROGAT TCICSTRN TEMPDSN
                 TERMINAL TSOAUTH TSOPROC UCICSTST UNIXPRIV VCICSCMD
GENERIC PROFILE CLASSES = DATASET DASDVOL FACILITY PROGRAM TCICSTRN TERMINAL
GENERIC COMMAND CLASSES = DATASET ACCTNUM DASDVOL FACILITY FIELD PERFGRP
                          PROGRAM T@TESTRN TCICSTRN TERMINAL TSOAUTH TSOPROC
GENLIST CLASSES = NONE
GLOBAL CHECKING CLASSES = DATASET FACILITY TERMINAL
SETR RACLIST CLASSES = APPL CDT DSNR FACILITY STARTED TSOAUTH TSOPROC
GLOBAL=YES RACLIST ONLY = TCICSTRN
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.
```

SETROPTS LIST

```
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.** ← **PAY.PROD.CHECKS.TAPE**
PAY.**

Profiles are sequenced based on EBCDIC characters rather than ASCII

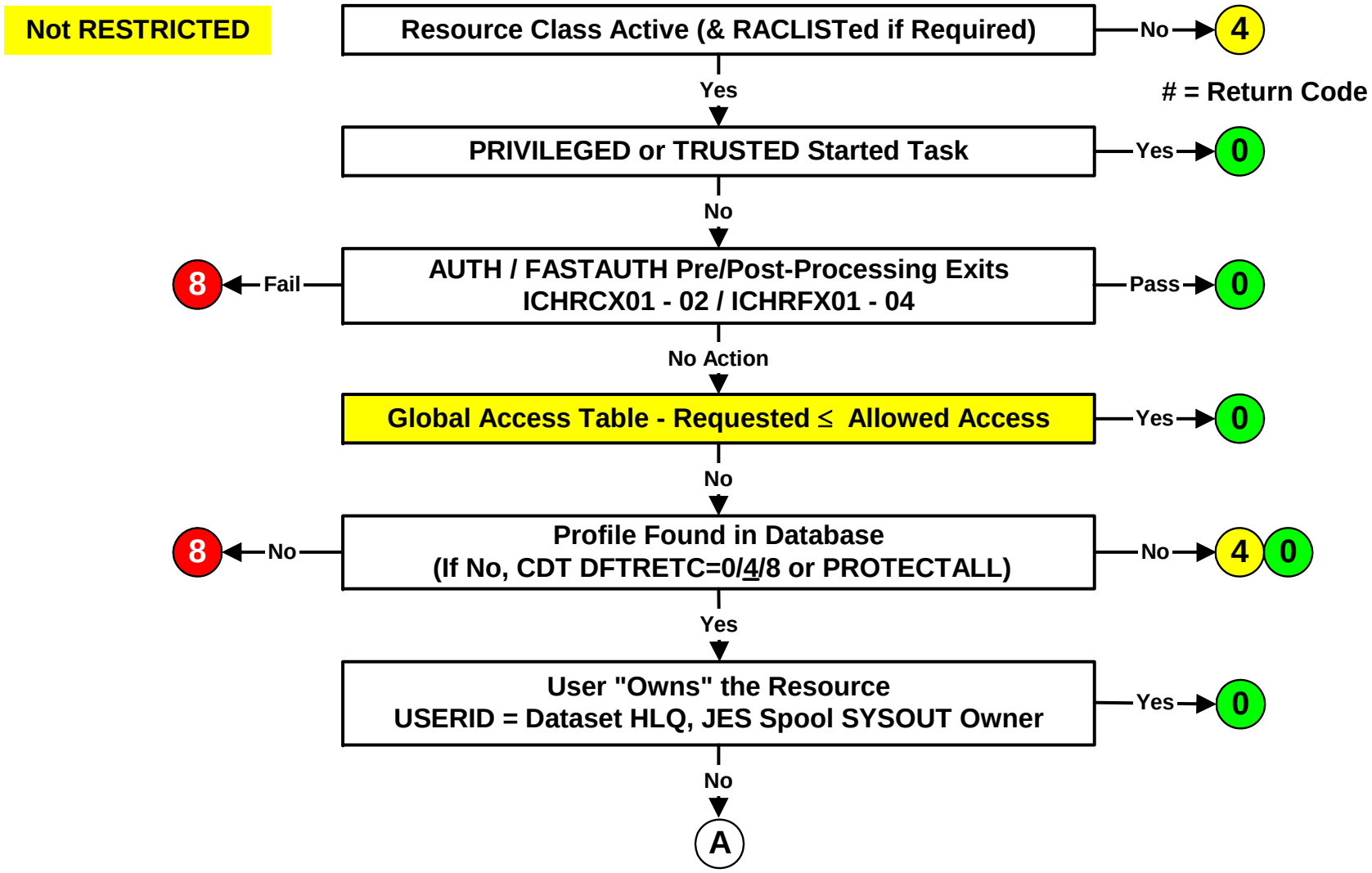
Generic Profiles

- 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

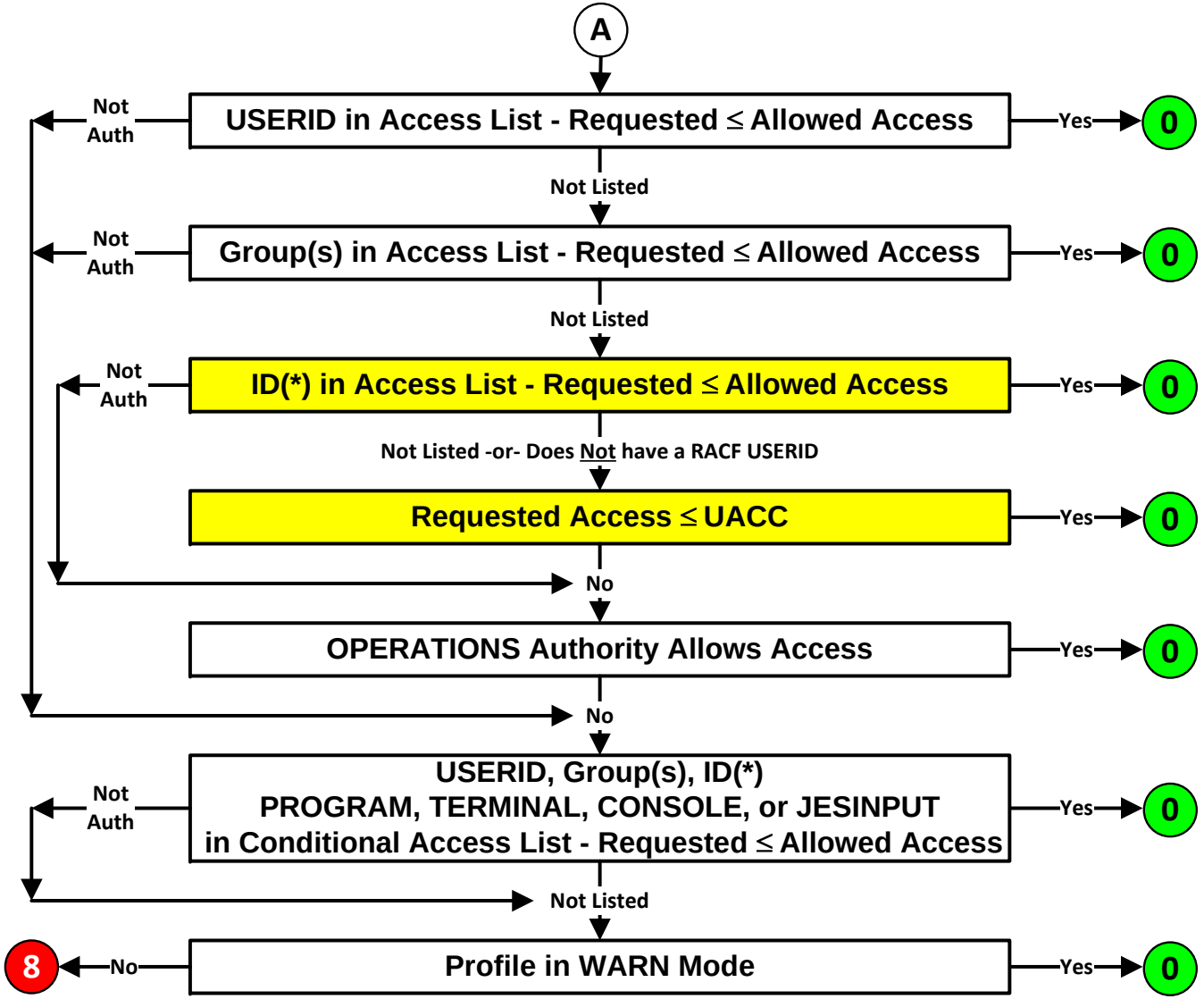
%	Single substitute character
*	Any set of substitute characters or one qualifier
**	Any set of substitute characters, zero or more qualifiers

  - 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



Access Authorization Decision Logic



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

(1) Optional (2) If using z/OSMF ISPF

APSWPROx(1)	CATALOG	CEA(2)	DFHSM(1)	DFS(1)
DUMPSRV	GPMSERVE(1)	HIS	IEEVMPCR	IOSAS
IXGLOGR	JESn	JESXCF	JES3AUX	LLA
NFS	OMVS(1)	RACF	RMF	RMFGAT
SMF	SMS	SMSPDSE1	SMSVSAM(1)	TCPIP
VLF	VTAM	WLM	XCFAS	ZFS(1)

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:
-------------------------------------------------------------------------------
PROFILE                 ASSOCIATED  ASSOCIATED
NAME                    USER        GROUP       PRIVILEGED  TRUSTED  TRACE
-------------------------------------------------------------------------------
CASAM                   CASAM                   NO          NO       NO
CICSP01.* (G)           CICSPRD1    STASKGP     NO          NO       NO
CICST01.CICSTEST        =MEMBER     STCTEST     YES         NO       NO
CICS* (G)               =MEMBER     CICSTSKS    NO          NO       YES
DUMPSRV.* (G)           MVSSYST     STASKGP     NO          YES      NO
HSERVER.* (G)                                   NO          NO       YES
NETA.* (G)              -STDATA NOT SPECIFIED, ICHRIN03 WILL BE USED-
** (G)                  DFLTSTC     STASKGP     NO          NO       YES
```

=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)
-------------------------------------------------------------------------------
PROCEDURE       ASSOCIATED      ASSOCIATED
NAME            USER            GROUP           PRIVILEGED     TRUSTED
-------------------------------------------------------------------------------
JES2            JES2                            YES            YES
CICSTOR         CICSPRD         CICSSYS         NO             NO
CICSAOR         CICSPRD         CICSSYS         NO             NO
NETA            $SNETA          NTWKSTC         NO             NO
NETB            $SNETB          NTWKSTC         NO             NO
RCVRY           SYSRCVRY                        YES            NO
*               =                               YES            NO
```

* - 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

```
R A C F     G L O B A L     A C C E S S      T A B L E     R E P O R T

CLASS              ACCESS            ENTRY
NAME               LEVEL             NAME
-------------------------------------------------------------------------
DATASET            ALTER             &RACUID.*
                   READ              CATLG.*
                   READ              ISP.*
                   READ              PROD.*.LIB
                   UPDATE            SYS1.BRODCAST
                   NONE              SYS1.RACF.*
                   READ              SYS1.*
DASDVOL            -- GLOBAL INACTIVE --
TERMINAL           -- NO ENTRIES --
FACILITY           READ              STGADMIN.ARC.ENDUSER.*
```

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)

APPCSERV	APPCTP	CBIND	CONSOLE
DCEUUIDS	DIRACC	DIRAUTH	DIRECTRY
DIRSRCH	FILE	FSOBJ	FSSEC
IPCOBJ	JESINPUT	JESJOBS	JESSPOOL
KEYSMSTR	MQADMIN*	MQCHAN*	MQCMDS
MQCONN	MQNLIST*	MQPROC*	MQQUEUE*
MXADMN*	MXNLIST*	MXPROC	MXQUEUE*
MXTOPIC*	PROCACT	PROCESS	PSFMPL
RACFHC	ROLE	SECLABEL	SFSCMD
SERVER	SOMDOBJS*	TEMPDSN	TMEADMIN
WRITER	XCSFKEY	XFACILIT*	

- Calling process decides how to react to Return Code

OPERATIONS Authority

- User and Group-connect attribute

```
LU RSHTEST
USER=RSHTEST   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	VMCMD	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

CLASS                                                    DEFAULT      OPERATIONS
NAME             STATUS      AUDITING      STATISTICS    UACC         ALLOWED
-------------------------------------------------------------------------------
ACCTNUM          ACTIVE        NO             NO         NONE           NO
APPL             ACTIVE        NO             NO         NONE           NO
DASDVOL          ACTIVE        YES            NO         ACEE           YES
RACFVARS         ACTIVE        NO             NO         NONE           NO
T@TESTRN   (D)   ACTIVE        NO             NO         NONE           NO
TCICSTRN         ACTIVE        NO             NO         NONE           NO
TERMINAL         ACTIVE        YES            YES        ACEE           NO
TESTAPP    (D)   INACTIVE      NO             NO         READ           YES
```

(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

USERID          ---------------- ATTRIBUTE TYPE ----------------  -----------
                SPECIAL          OPERATIONS     AUDITOR          REVOKE  NODE.USERID…
-------------------------------------------------------------------------  -----------
AHILL03                                                           SYSTEM
AUDITJH                                         SYSTEM
CICS01                           SYSTEM
CSTARR4         GROUP
JSMITH1         GROUP            SYSTEM                           GROUP
IBMUSER                          SYSTEM
RHOMES1                                                           GROUP
RJONES2         SYSTEM           SYSTEM         SYSTEM
SECUSR02        SYSTEM                          SYSTEM
```

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

Troubleshooting Access Problems

- 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

CHECK	FUNCTION
RACF_AIM_STAGE	Reports if RACF database is not AIM Stage 3
RACF_BATCHALLRACF	Verifies the SETROPTS option is active
RACF_CERTIFICATE_EXPIRATION	Reports certificates expiring in 90 days
RACF_class_ACTIVE	Verifies that the class is active: CFSKEYS, CFSSERV, FACILITY, JESJOBS, JESSPOOL, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV
RACF_ENCRYPTION_ALGORITHM	Checks password encryption algorithms in use
RACF_GRS_RLN	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
RACF_IBMUSER_REVOKED	Verifies that the user ID IBMUSER is revoked
RACF_ICHAUTAB_NONLPA	RACF_ICHAUTAB_NONLPA raises a SEV(MED) exception if a non-LPA resident ICHAUTAB is found
RACF_PASSWORD_CONTROLS	Checks mixed-case password and invalid password attempts settings
RACF_RRSF_RESOURCES	Confirms INMSG and OUTMSG datasets are defined and protected
RACF_SENSITIVE_RESOURCES	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 • Are not found on the indicated volume • Are improperly protected Examines key system general resources
RACF_UNIX_ID ZOSMIGV1R13_DEFAULT_UNIX_ID	Checks for existence of FACILITY BPX.DEFAULT.USER and BPX.UNIQUE.USER

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

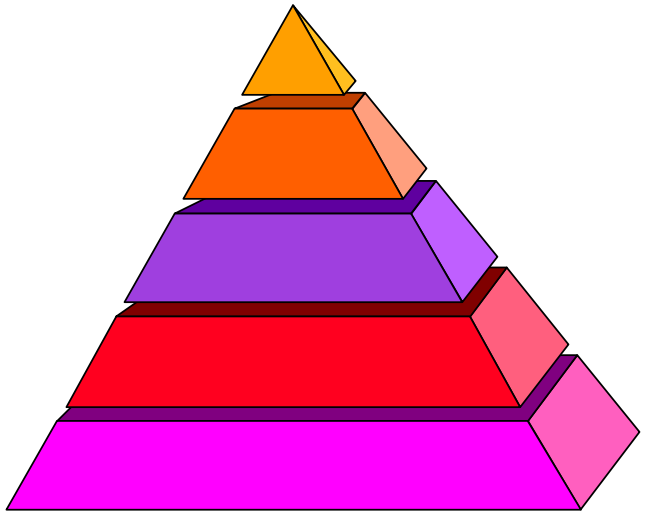
Common Issues and Concerns

- 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