RSH

CONSULTING

Introduction to RACF

IBM Systems TechU - May 2019

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

z/OS Security

- How important is the z/OS mainframe's data and services to your organization

- How would your organization be affected if data on the mainframe was ...
  - Stolen or publicly disclosed
  - Inappropriately modified
  - Deleted
  - Rendered unavailable because the operation of the system was disrupted

- Working in conjunction with z/OS and installed system software products (e.g., CICS), RACF can help guard against bad outcomes by preventing users from accessing data and software functions they are not supposed to use *if it is fully and properly implemented*

Topics

- Concepts
- Users
- Groups
- Resource Protection
- Dataset Protection
- General Resources
- Monitoring
- Administration
- ICH408I Message

RACF

Concepts

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

RACF Components

- Database (Primary and Backup Pair)
  - Options - SETROPTS (SET RACF OPTIONS)
  - Profiles - Users, Groups, Datasets, General Resources
  - Indices - Profile location and Application Identity Mapping (AIM) cross-references

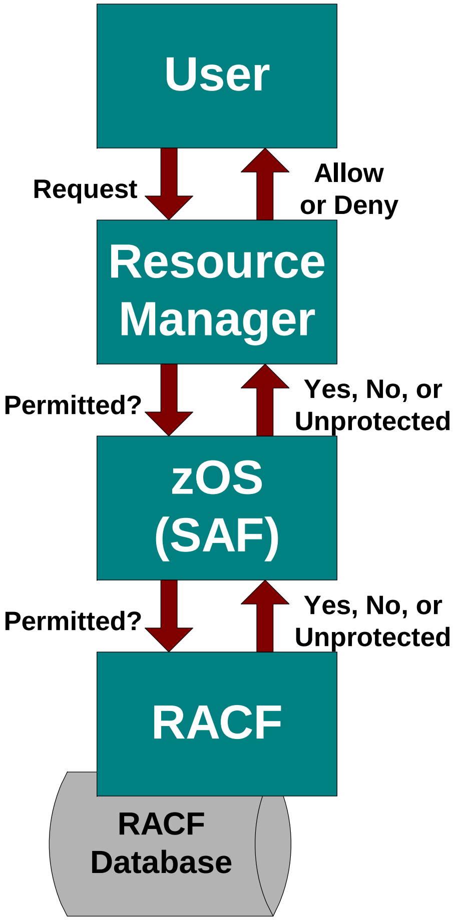
- Software
  - Programs - Query Database and make security decisions (loaded into z/OS Link Pack Area)
  - Tables - Specify the Databases and define Classes (e.g., Class Descriptor Table (CDT))
  - Exits - Optional Installation-written programs that modify RACF's behavior
  - Macros - Assembly routines used by a Resource Manager to call RACF (e.g., RACROUTE)
  - Commands - TSO programs used to create and administer options and profiles
  - ISPF Panels - TSO ISPF menus used to create and administer options and profiles
  - Utilities - Programs used for backup, maintenance, unload, and control reports
  - Subsystem - RACF Address Space used to support optional communication functions like RACF Remote Sharing Facility (RRSF) used for cross-system synchronization

RACF Functions

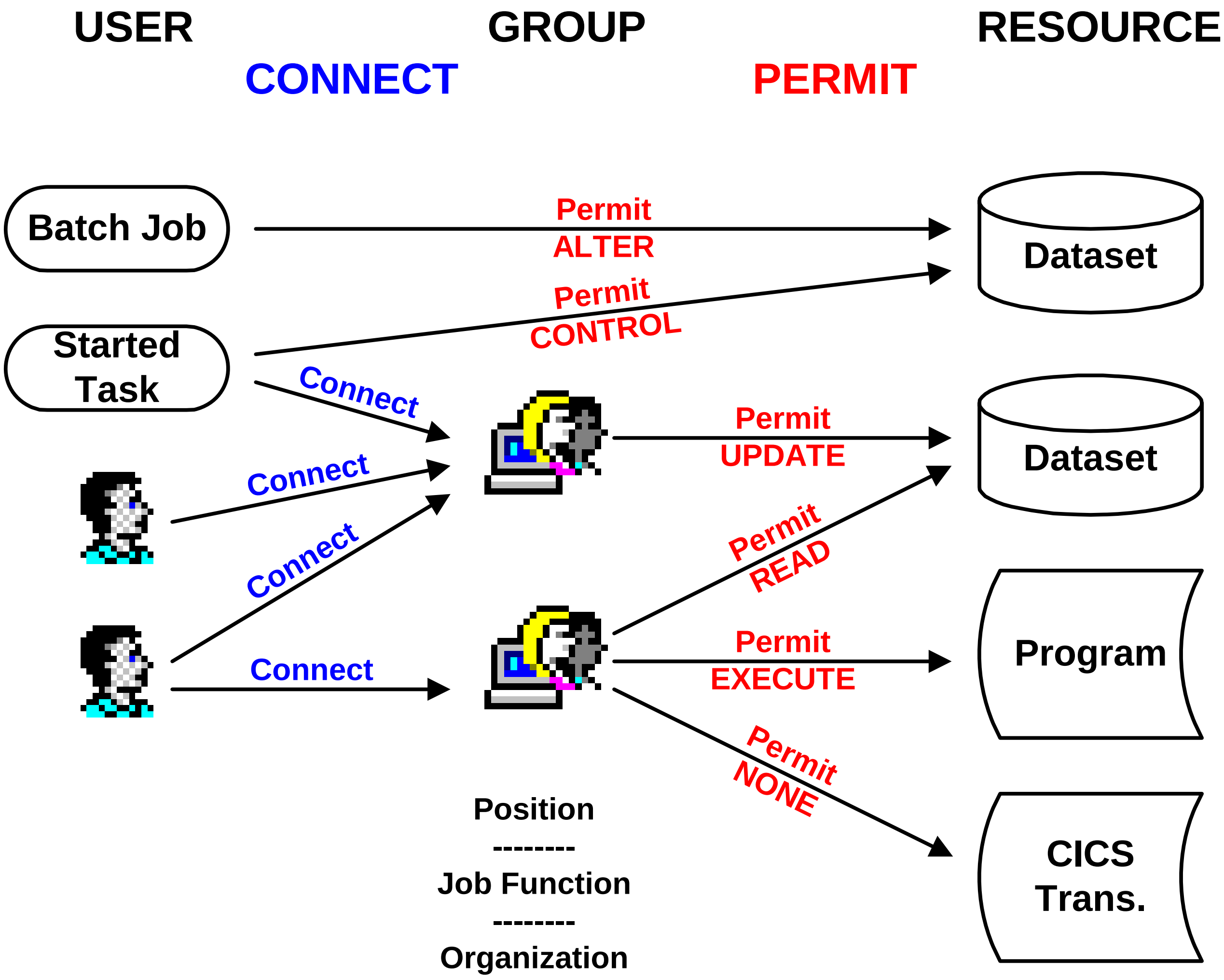
- User Identification and Authentication
- Resource Access Authorization
- User Activity Monitoring
- Access Administration

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
  - Most calls are made using the RACROUTE macro, which is directed at the System Authorization Facility (SAF)
- 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 Commands

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

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

RSH CONSULTING

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
  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
```

Users

RACF Identification and Authentication

- User - person or process (e.g., Started Task, Batch Job) accessing the system

- USERID (often abbreviated as just "ID") - identifier for a user
  - Up to 8 characters in length
  - Comprised of letters, numbers, or national characters (U.S. - @, #, $)
  - Must be unique - cannot match another USERID or a Group

- A User Profile defines an ID to RACF along with its characteristics

- User Authentication
  - Password: 1-8 characters - letters, numbers, and national characters
  - Password Phrase: 9-100 characters - mixed-case letters, numbers, and special characters
  - Pass-Ticket: One-time password generated by an application at logon time
  - Digital Certificate: Public Key x509 certificate
  - Multifactor Authentication (MFA): PIN and dynamic token

RACF Identification and Authentication

- At logon, the Resource Manager passes the ID and authenticator entered by the user (e.g., password) to RACF for validation using either a RACINIT macro or a RACROUTE macro with REQUEST=VERIFY or VERIFYX

- If logon is successful, RACF builds an Accessor Environment Element (ACEE) control block in memory
  - ACEE Contents
    - USERID
    - User Attributes (e.g. SPECIAL, OPERATIONS)
    - User Name and Installation-Data
    - Current Connect Group
    - Current Connect Group UACC
    - List of User's Groups
  - The ACEE is referenced for all subsequent resource access authorization checks
  - The ACEE must be refreshed via re-logon to acquire new attributes

USERID Controls

- Controls on individual IDs
  - REVOKE / RESUME [(date)] - deactivate / activate, with optional future date
  - WHEN(DAYS(days) TIME(time)) - Day-of-Week, Time-of-Day logon limits
  - PROTECTED - Disallows logon with a password; for Batch and Started Task IDs
  - NOINTERVAL - User never required to change password; for file transfer IDs, etc.

USERID Controls

- Controls over all USERIDs - SETROPTS
  - INITSTATS - Record last logon and password change date/time
  - INACTIVE(#) - Automatic revoke after prolonged inactivity - # days (1 - 255)
  - PASSWORD(Options)
    - ALGORITHM Encryption algorithm - LEGACY or KDFAES
      - LEGACY - DES - Data Encryption Standard
      - KDFAES - Key Derivation Function with Advanced Encryption Alogrithm
    - INTERVAL(#) Frequency of mandatory periodic change - # days (1 - 254)
    - MINCHANGE(#) Minimum # days before next password change (0 - 254)
    - MIXEDCASE Mixed case passwords in use
    - SPECIALCHAR National **$ @ #** plus **. < + | & ! * - % _ > ? : =**
    - HISTORY(#) Prevent reuse of # prior passwords (1 - 32)
    - REVOKE(#) Revoke ID after # attempts with bad password (1 - 255)
    - WARNING(#) # days advance notice of next password expiration (1 - 255)
    - RULE#(…) Minimum/Maximum length and composition format - up to 8 rules
      - Most common rule - 8 alphanumeric characters

User Profile

USERID

User Name
Default Group
Profile Owner
Last Access Date/Time
Password / Phrase
Password / Phrase Date
Password / Phrase Interval
Password / Phrase History
User Attributes
Revoke/Resume Dates
Installation-Data
Day/Time Logon Limits

Group Connects
- Connect Owner
- Last Connect Date/Time
- Connect Attributes
- Connect Revoke/Resume Dates

Segments
- CICS
- OMVS
- TSO

User Profile

```
LISTUSER JSMITH1 TSO
USER=JSMITH1  NAME=JOHN SMITH            OWNER=SECGRP1   CREATED=05.067
 DEFAULT-GROUP=USRGRPA  PASSDATE=19.030 PASS-INTERVAL= 30 PHRASEDATE=N/A
 ATTRIBUTES=OPERATIONS
 ATTRIBUTES=UAUDIT
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=19.035/11:35:22
 CLASS AUTHORIZATION=DASDVOL
 INSTALLATION-DATA=SSN234-12-3990  TECHSPT DASD MANAGEMENT
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)           (TIME)
 -------------------------------------------------
 ANYDAY                            ANYTIME
  GROUP=USRGRPA   AUTH=USE       CONNECT-OWNER=SECUSR02  CONNECT-DATE=05.067
    CONNECTS= 5,234  UACC=NONE      LAST-CONNECT=19.035/11:35:22
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=TECHSPT1  AUTH=CONNECT   CONNECT-OWNER=RJONES2   CONNECT-DATE=05.070
    CONNECTS=    00  UACC=READ      LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=OPERATIONS
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=SYS1      AUTH=CREATE    CONNECT-OWNER=SYS1      CONNECT-DATE=08.144
    CONNECTS=    00  UACC=ALTER     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=DASDMGT   AUTH=USE       CONNECT-OWNER=RJONES2   CONNECT-DATE=10.081
    CONNECTS=    00  UACC=NONE      LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=SPECIAL
    REVOKE DATE=02.030 RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGOTY-AUTHORIZATION
 NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
TSO INFORMATION
 ACCTNUM= JJK001
 HOLDCLASS= M
 ...
```

Groups listed in the order the user was connected to them

User Profile Segments

- Segments are extensions of the User profile containing system software product-specific control information

CICS	SNT identification information (e.g., OPIDENT)
CSDATA	Customer-defined custom data field
DCE	Associates DCE Principle Identity (e.g., uuid) to RACF USERID
DFP	SMS data management and DASD storage (e.g., MGMTCLAS)
EIM	LDAP profile
KERB	Kerberos user attributes
LANGUAGE	Preferred National Language
LNOTES	Lotus Notes user (e.g., SNAME)
NDS	Map Novell Directory Service user name to RACF USERID
NETVIEW	Application access information
OMVS	UNIX user attributes (e.g., UID)
OPERPARM	Extended MCS Console Session attributes (e.g., AUTH)
PROXY	LDAP characteristics (e.g., LDAPHOST)
TSO	TSO UADS logon and authority information (e.g., ACCTNUM)
WORKATTR	APPC User characteristics (e.g., WANAME for SYSOUT)

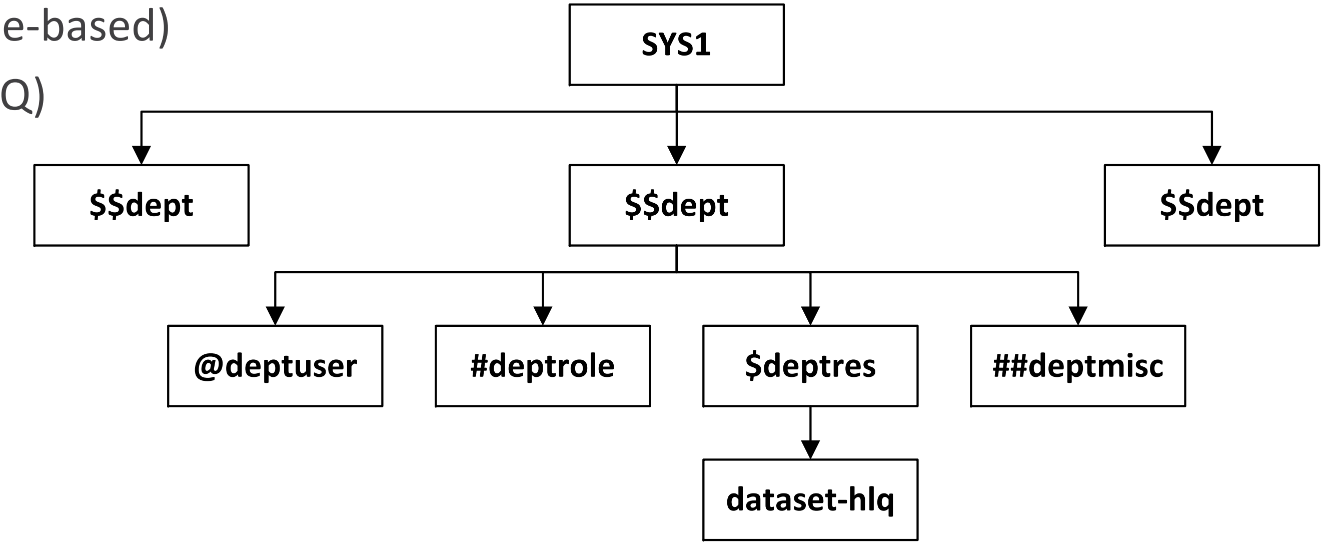
Groups

Group Concept

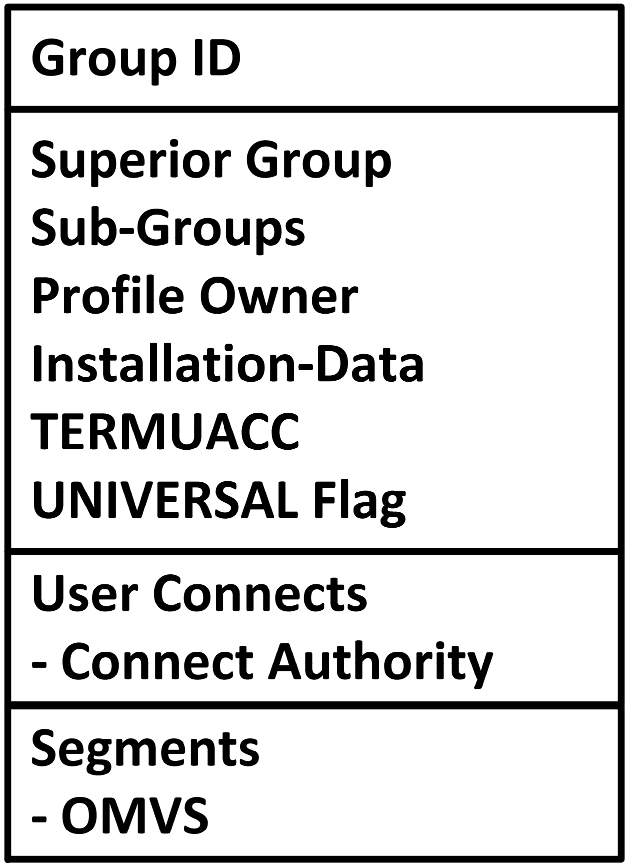
- A Group is a collection of users with similar access needs and common attributes
- Users are "connected" (i.e., joined) to groups and "removed" from groups
- Every user has a logon default group (DFLTGRP), and therefore, is connected to at least one group
- A user can be connected to multiple groups
- Groups can be permitted access to resources, and the users who are connected to the group are granted this access
- Groups simplify RACF administration; it is easier to manage the access of 100 groups than 10,000 individual users
- Group names have the same format as USERIDs
- Group names must be unique; cannot match a USERID or another group
- Groups defined as UNIVERSAL allow more than 5,957 IDs to be connected

Group Architecture

- Group Structure
  - Groups are organized in a hierarchy with SYS1 at the top
  - Every group except SYS1 has a superior group (SUPGROUP)
  - RACF comes with one group - SYS1
- Groups are the primary tool for organizing the RACF database and can serve different purposes
  - Organization
  - User Logon/Default
  - Access Granting (role-based)
  - Dataset Owning (HLQ)
  - Resource Owning
  - Other
    - Miscellaneous
    - Administrative
    - Documentation



Group Profile



Group ID

Superior Group
Sub-Groups
Profile Owner
Installation-Data
TERMUACC
UNIVERSAL Flag

User Connects
- Connect Authority

Segments
- OMVS

CONNECT Authorities: USE, CREATE, CONNECT, and JOIN

Group Profile

```
LISTGRP DASDMGT OMVS
INFORMATION FOR GROUP DASDMGT
    SUPERIOR GROUP=TECHSPT1         OWNER=RJONES2     CREATED=02.305
    INSTALLATION DATA=DASD MANAGEMENT SECTION
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= DASDTEST
    USER(S)=         ACCESS=         ACCESS COUNT=   UNIVERSAL ACCESS=
      RJONES2          CREATE           000000                   READ
         CONNECT ATTRIBUTES=SPECIAL
         REVOKE DATE=NONE                       RESUME DATE=NONE
      JSMITH1          USE              000000                   NONE
         CONNECT ATTRIBUTES=SPECIAL
         REVOKE DATE=19.320                     RESUME DATE=NONE
      SREST03          CONNECT          000000                   NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                       RESUME DATE=NONE
      RHOMES1          USE              000000                   NONE
         CONNECT ATTRIBUTES=REVOKED
         REVOKE DATE=NONE                       RESUME DATE=NONE
      HWILLS2          USE              000000                   NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                       RESUME DATE=NONE
      JWINDS4          JOIN             000000                   NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                       RESUME DATE=NONE
OMVS INFORMATION
 GID = 0000000339
```

Users are listed in the order by which they were connected to the group

Group Profile Segments

- Segments are extensions of the Group profile containing system software product-specific control information

CSDATA	Customer-defined custom data field
DFP	SMS data management and DASD storage
OMVS	UNIX group attributes (e.g., GID)
TME	Tivoli group roles

Resource Protection

Resource Protection Concepts

- 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 profiles contain ...
  - The logical name of the resource (e.g., the DSNAME)
  - The type of resource or 'Class' (e.g., PROGRAM)
  - Control options (e.g., WARNING)
  - Auditing specifications (e.g., AUDIT(FAILURES(READ)))
  - Access permissions

- Resource categories
  - Dataset
  - General Resource (e.g., TSOPROC)

Resource Protection Concepts

- 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 uses the name and class of the resource to locate the corresponding profile in its database

- 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

Resource Profiles

```
RLIST DASDVOL SYS* ALL
CLASS      NAME
-----      ----
DASDVOL    SYS* (G)

GROUP CLASS NAME
----- ----- ----
GDASDVOL

RESOURCE GROUPS
-------- ------
NONE

LEVEL  OWNER      UNIVERSAL ACCESS   YOUR ACCESS  WARNING
-----  --------   ----------------   -----------  -------
 00    STGADM          NONE                NONE    YES

INSTALLATION DATA
---------------------------------------------------
NONE

APPLICATION DATA
----------------
NONE

SECLEVEL
--------
NO SECLEVEL

CATEGORIES
----------
NO CATEGORIES

SECLABEL
--------
NO SECLABEL
```

Resource Profiles

```
AUDITING
--------
SUCCESSES(UPDATE),FAILURES(READ)

GLOBALAUDIT
-----------
NONE

NOTIFY
--------
NO USER TO BE NOTIFIED

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY) (YEAR)        (DAY) (YEAR)      (DAY) (YEAR)
-------------  -------------------  ----------------
 270    02           270    02         270    02

ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
-----------  -------------  ------------  ----------
  000000        000000         000000        000000

USER      ACCESS    ACCESS COUNT
----      ------    ------ -----
RJONES2   ALTER
APPLSPT   UPDATE
DASDMGT   READ
JWILLS2   NONE

   ID     ACCESS ACCESS COUNT  CLASS                  ENTITY NAME
-------- ------- ------------ -------- --------------------------------
NO ENTRIES IN CONDITIONAL ACCESS LIST
```

IDs are listed in the order by which they were permitted access

Permission of NONE for JWILLS2 prevents access even if user is a member of APPLSPT or DASDMGMT

Resource Profiles

- Resource profile types
  - Discrete - Fully qualified resource name - exact match
  - Generic - Partially qualified resource name with masking
  - Grouping - Set of discrete and generic profiles with identical attributes

- 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

- Generic masking characters may be used in combination

  SYS2.%%%%.LIB.**   FIN.*.**   ACCTG.**.MASTER.*

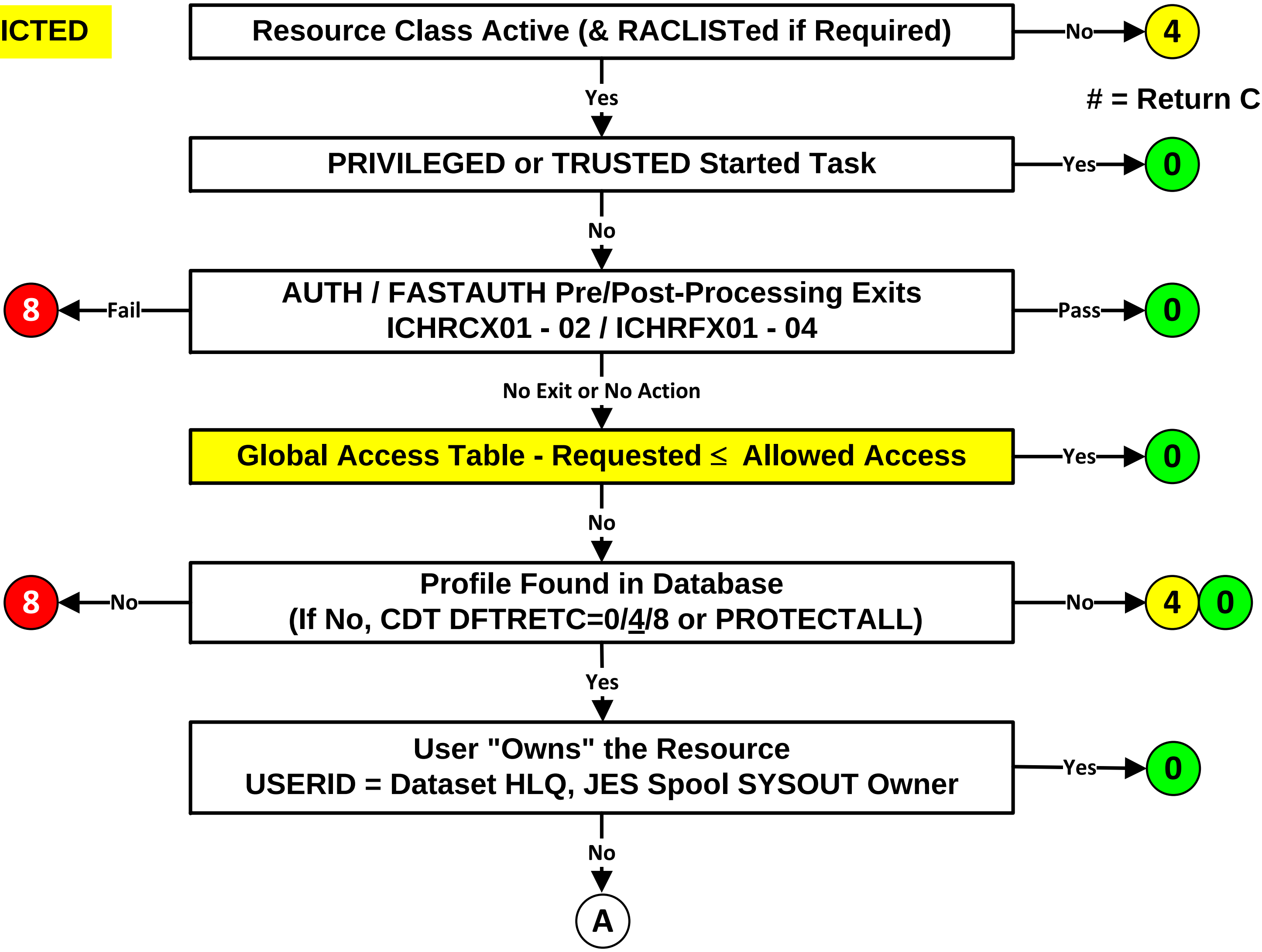
- Usage and behavior of the masking characters differs slightly based on whether the profile is a Dataset or a General Resource

Access Authorization

- RACF considers the following in deciding whether access is permitted
  - Is the Class active
  - Is the user a Started Task with PRIVILEGED or TRUSTED authority
  - Does an installation exit program grant or deny access
  - Does an entry in the Global Access Table grant access
    - The GAT is used to grant access to resources needed by all users
  - Is there a profile that protects the resource; if not, what default RC is to be issued
  - Does the user own the resource
  - Does the profile's Standard Access List have an entry granting access to ...
    - The user's USERID
    - One of the user's groups - assumes SETROPTS GRPLIST (List of Groups) is active
    - ID(*) - all RACF-defined users
  - Does the profile's Universal Access (UACC) grant access (default access)
  - Does the class accept OPERATIONS authority, and does the user have OPERATIONS
  - Does the profile's Conditional Access List have an entry granting access
  - Is the profile in WARNING
  - Is the user RESTRICTED - ignores GAT, ID(*), and UACC permissions

Access Authorization Decision Logic

Not RESTRICTED



# = Return Code

Resource Class Active (& RACLISTed if Required) — No → 4

Yes ↓

PRIVILEGED or TRUSTED Started Task — Yes → 0

No ↓

AUTH / FASTAUTH Pre/Post-Processing Exits
ICHRCX01 - 02 / ICHRFX01 - 04 — Pass → 0; Fail → 8

No Exit or No Action ↓

Global Access Table - Requested ≤ Allowed Access — Yes → 0

No ↓

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

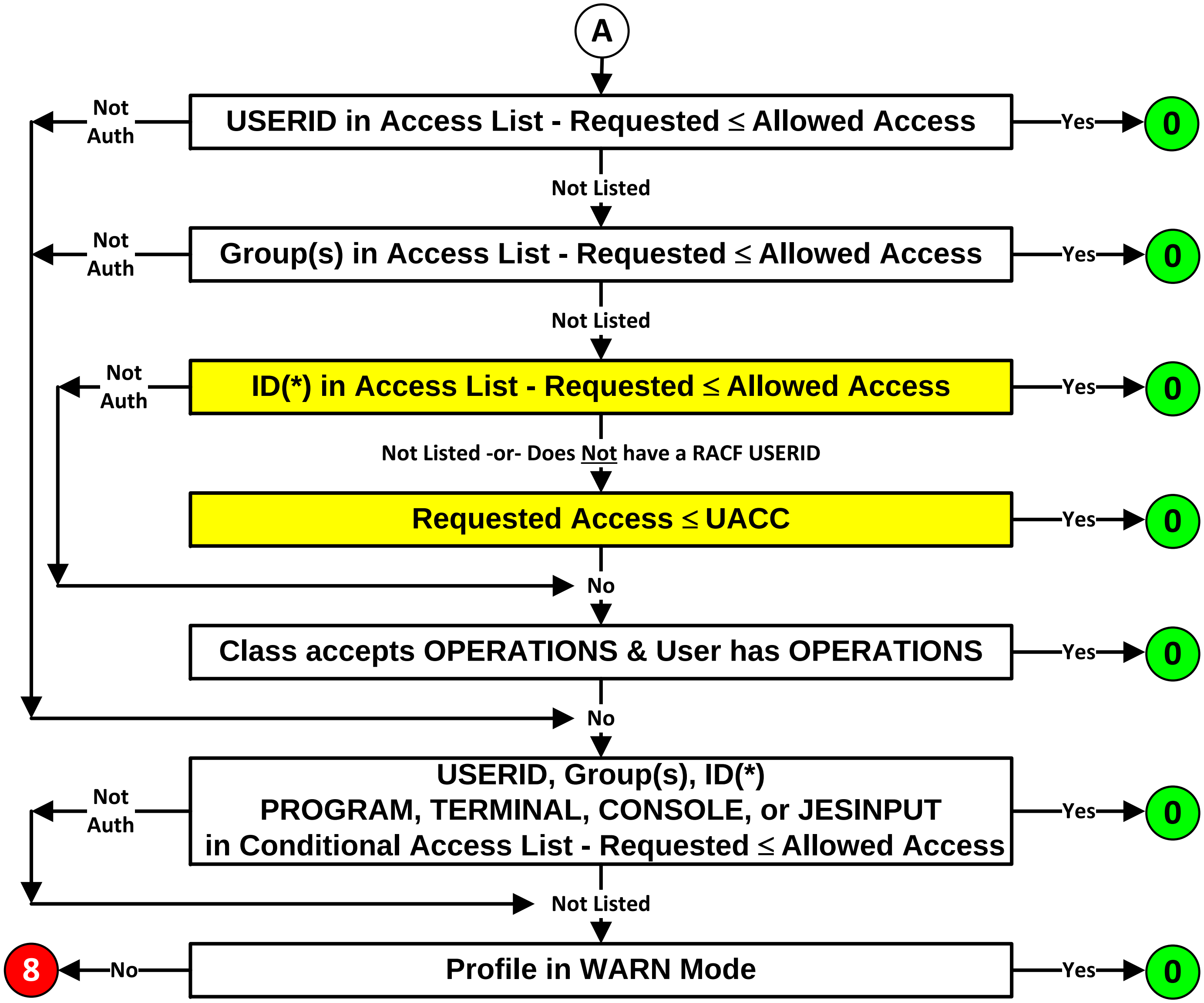
Yes ↓

User "Owns" the Resource
USERID = Dataset HLQ, JES Spool SYSOUT Owner — Yes → 0

No ↓

A

Access Authorization Decision Logic



A

USERID in Access List - Requested ≤ Allowed Access

Yes → 0

Not Auth

Not Listed

Group(s) in Access List - Requested ≤ Allowed Access

Yes → 0

Not Auth

Not Listed

ID(*) in Access List - Requested ≤ Allowed Access

Yes → 0

Not Auth

Not Listed -or- Does Not have a RACF USERID

Requested Access ≤ UACC

Yes → 0

No

Class accepts OPERATIONS & User has OPERATIONS

Yes → 0

No

USERID, Group(s), ID(*)
PROGRAM, TERMINAL, CONSOLE, or JESINPUT
in Conditional Access List - Requested ≤ Allowed Access

Yes → 0

Not Auth

Not Listed

Profile in WARN Mode

Yes → 0

No → 8

Access Permissions

- Access List entries and UACC specify the permitted level of access
  - Access levels (listed from highest to lowest access authority)
    - ALTER
    - CONTROL
    - UPDATE
    - READ
    - EXECUTE
    - NONE
  - Higher level access authorities include lower level authorities
  - The meaning of an access level differs by the class of resource protected

- Conditional Access List entries grant access only when a condition is met
  - WHEN(CONSOLE(*console-id*))
  - WHEN(JESINPUT(*port-of-entry*))
  - WHEN(PROGRAM(*program*))
  - WHEN(SERVAUTH(*servauth-profile*))
  - WHEN(SYSID(*smf-id*))
  - WHEN(TERMINAL(*terminal-id*))

Dataset Protection

Dataset Protection

- RACF protection is provided by Dataset Profiles

- Dataset Profile name
  - Incorporates the name(s) of the dataset(s) it protects
    - Dataset PAY.PROD.MASTER HLQ = PAY
    - Profile PAY.PROD.**
  - The High Level Qualifier (HLQ) <u>must</u> match an existing RACF user or group

- Dataset profile types
  - Discrete
    - Protects a single dataset on a specific DASD volume identified by its VOLSER
    - The RACF-Indicator bit in the DASD volume VTOC flags the dataset as having a Discrete profile
    - Profile is deleted when the corresponding dataset is deleted
  - Generic
    - Protects multiple dataset using masking characters
    - Can be 'fully qualified' (no masking characters) to protect a single dataset
    - SETROPTS EGN (Enhanced Generic Naming) enables use of the ** masking character
    - Unaffected by dataset deletion and RACF-indicator bit is not set

Access Levels

ALTER — Allows anything, to include creating, scratching (i.e., deleting), cataloging, uncataloging, and renaming[1]

CONTROL — For VSAM datasets, allows use of high-performance control-interval processing (enhanced form of UPDATE)

UPDATE — Allows writing and reading, but not creating and scratching

READ — Allows reading, to include copying

EXECUTE — Allows the execution of programs from a specified library, but will not allow reading, copying, or dumping of the programs

NONE — Denies all access

[1] Renaming requires ALTER to both the old and new dataset name

Dataset Profile

Dataset Name/Mask

Profile Type
DASD Volume (Discrete)
Profile Owner
WARN mode flag
Erase-on-Scratch
Auditing
UACC
Installation-Data

Standard Access List
- User(s)   - Access
- Group(s) - Access
- *   - Access

Conditional Access List - WHEN
- User(s)   - Access - Condition
- Group(s) - Access - Condition
- *   - Access - Condition

Dataset Profile

```
LISTDSD DATASET('SYS1.LIBS*') ALL
INFORMATION FOR DATASET SYS1.LIBS* (G)

LEVEL  OWNER    UNIVERSAL ACCESS   WARNING   ERASE
-----  -------- ----------------   -------   -----
 00    TECHSPT1       NONE           NO      NO

AUDITING
--------
FAILURES(UPDATE)

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
   READ         TECHSPT1       NON-VSAM

GLOBALAUDIT
-----------
NONE

INSTALLATION DATA
---------------------------------------------------
MVS LIBRARIES

              SECURITY LEVEL
--------------------------------------------
NO SECURITY LEVEL
```

Dataset Profile

```
CATEGORIES
----------
NO CATEGORIES

SECLABEL
--------
NO SECLABEL

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY) (YEAR)        (DAY) (YEAR)      (DAY) (YEAR)
-------------  -------------------  ----------------
 270    02     NOT APPLICABLE FOR GENERIC PROFILE

ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
-----------  -------------  ------------  ----------
NOT APPLICABLE FOR GENERIC PROFILE

   ID     ACCESS
--------  -------
RJONES2    ALTER
TECHSPT1  UPDATE
*          READ
DASDMGT    ALTER
JWILLS2    NONE

   ID    ACCESS   CLASS              ENTITY NAME
-------- ------- -------- -----------------------------------
APPPGMR   UPDATE PROGRAM  PVAL01
APPPGMR   UPDATE PROGRAM  PVAL04
```

Dataset Protection Options

- SETROPTS PROTECTALL option - prevents access to unprotected datasets

- SETROPTS ERASE option - overwrites data when deleted to prevent scavenging of residual data

- Tape datasets are only protected if either …
  - SETROPTS TAPEDSN option is active
  - PARMLIB(DEVSUPnn) option TAPEAUTHDSN=YES
  - CA-1 option OCEOV=YES

- Pervasive Encryption - encrypt contents of a dataset
  - CSFKEY class encryption-key-label profile is specified in a dataset profile's DFP segment

General Resource Protection

General Resources

- RACF protection is provided by General Resource Profiles
- A General Resource is anything other than a dataset

  Terminals
  CICS Transactions
  DASD Volumes
  Application APPLIDs
  TSO Logon Attributes
  General Purpose Facility

  Programs
  JES Spool
  NJE Nodes
  DB2 System Connections
  MVS and JES Commands
  3rd Party or Locally Defined

- General Resources are identified by their logical names within a specific class
- The construct of the resource name is determined by the resource manager

General Resources

RESOURCE-TYPE	CLASS / GROUPING-CLASS	RESOURCE-NAME
Program	PROGRAM	AMASPZAP
TSO Authority	TSOAUTH	OPER
DASD Volumes	DASDVOL / GDASDVOL	SYS001
CICS APPLID	APPL	CICSPRD1
DB2 TSO Connect	DSNR	DB2P.BATCH
Storage Admin	FACILITY	STGADMIN.ADR.DEFRAG
JES2 RJE Reader	JESINPUT	R213.RD1
SDSF Command	SDSF / GSDSF	ISFCMD.DSP.OUTPUT.JES2
MVS Command	OPERCMDS	MVS.HALT.NET
CICS Transaction	TCICSTRN / GCICSTRN	CEMT

General Resource Protection

- General Resource Profile names incorporate the class and name of the resource
  - DASD Volume TSO003
  - Class and Profile DASDVOL TSO*

- General Resource classes are defined in RACF's Class Descriptor Table (CDT)
  - A class must be defined before profiles can be created
  - CDT entries define the length and character composition of profile names and other attributes about each class
  - CDT is comprised of IBM-provided classes and optional installation-defined classes

- Classes must be activated to enable protection
  - SETROPTS CLASSACT(*class*)
  - SETROPTS WHEN(PROGRAM)

- SETROPTS RACLIST(*class*) - Loads all profiles into memory for rapid reference
  - Some classes are required to be RACLISTed (e.g., OPERCMDS)

General Resource Profiles

- General Resource Class types
  - Member - Standalone or paired with a Grouping class
  - Grouping (optional) - Paired with Member class
  - Examples:
    - Standalone Member APPL FACILITY JESSPOOL SURROGAT TSOAUTH
    - Member/Grouping TCICSTRN-GCICSTRN DASDVOL-GDASDVOL TIMS-GIMS

- General Resource Profile types
  - Discrete TCICSTRN CEMT
  - Generic TCICSTRN C*
  - Grouping (members) GCICSTRN CICSCMD1 ADDMEM(CEDF X12 C*)

- Generics must be activated via SETROPTS
  - SETROPTS GENCMD(*class*) - Enables creation of profiles
  - SETROPTS GENERIC(*class*) - Activates profiles

General Resource Profile

Class
General Resource Name/Mask

Profile Type
Resource Members (Grouping)
Profile Owner
WARN mode flag
Auditing
UACC
Installation-Data
Application-Data

Standard Access List
- User(s)   - Access
- Group(s) - Access
- *   - Access

Conditional Access List - WHEN
- User(s)   - Access - Condition
- Group(s) - Access - Condition
- *   - Access - Condition

Segment
- STDATA (STARTED profiles)
- CDTINFO (CDT profiles)

General Resource Profile

```
RLIST GCICSTRN TSPT$CMD ALL
CLASS      NAME
-----      ----
GCICSTRN   TSPT$CMD

MEMBER CLASS NAME
------ ----- ----
TCICSTRN

RESOURCES IN GROUP
--------- -- -----
CEMT
CEDA
CEDF
CSM*

LEVEL  OWNER      UNIVERSAL ACCESS   YOUR ACCESS  WARNING
-----  --------   ----------------   -----------  -------
 00    CICSSPT         NONE                NONE    NO

INSTALLATION DATA
---------------------------------------------------
CICS TECH SPT SYSTEM COMMANDS

APPLICATION DATA
----------------
NONE

SECLEVEL
--------
NO SECLEVEL

CATEGORIES
----------
NO CATEGORIES
```

General Resource Profile

```
SECLABEL
--------
NO SECLABEL

AUDITING
--------
FAILURES(READ)

GLOBALAUDIT
-----------
NONE

NOTIFY
--------
NO USER TO BE NOTIFIED

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY) (YEAR)        (DAY) (YEAR)      (DAY) (YEAR)
-------------  -------------------  ----------------
 270    92           282    92         282    92

ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
-----------  -------------  ------------  ----------
  000000        000000         000000        000000

USER      ACCESS    ACCESS COUNT
----      ------    ------ -----
BRSMITH   READ
CICSSPT   READ
SYSPROGS  READ
JWILLS2   NONE

   ID     ACCESS ACCESS COUNT  CLASS         ENTITY NAME
-------- ------- ------------ -------- -----------------------
NO ENTRIES IN CONDITIONAL ACCESS LIST
```

Monitoring

Monitoring Basics

- RACF terminology - AUDITING

- Monitoring options can be specified in
  - User profile - UAUDIT - records all user activity
  - Resource profile - AUDIT and GLOBALAUDIT settings
  - SETROPTS Options - SAUDIT, OPERAUDIT, CMDVIOL, AUDIT, LOGOPTIONS

- 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)

Resource Monitoring

- Dataset and General Resource Profile
  - Command parameters
    - AUDIT(*options*(*level*))
      - Set by Profile Owner / SPECIAL
      - Default: FAILURES(READ)
    - GLOBALAUDIT(*options*(*level*))
      - Set by AUDITOR
      - Default: NONE
    - Used in combination - event is logged if either requires it
  - Auditing *options*

SUCCESS	Authorized Access
FAILURES	Violation
ALL	Both
NONE	No Logging

  - Auditing *levels* - at or above
    - ALTER
    - CONTROL
    - UPDATE
    - READ

SETROPTS Audit Options

- SAUDIT - Audit all RACF commands executed by SPECIAL user
- OPERAUDIT - Audit all resource access using OPERATIONS authority
- CMDVIOL - Audit all violations using RACF commands
- AUDIT(*class*) - Audit all changes to RACF profiles in the designated class
- LOGOPTIONS (*level* (*class*)) - Audit resource access at the designated level
  - Levels ...
    - ALWAYS - Log all access
    - NEVER - Do not log
    - SUCCESSES - Log all authorized access
    - FAILURES - Log all violations
    - <u>DEFAULT</u> - Use resource profile log options
  - Every class has a designated level

Administration

System and Group Authorities

- System and Group Administrative Attributes
  - SPECIAL - Administer RACF profiles, view non-audit options, and set control options
  - AUDITOR - View RACF profiles, view all options, and set audit options
  - ROAUDIT - View RACF profiles and view all options - System level only
  - OPERATIONS - Access resources, create group datasets, and define group dataset profiles
  - Authority scope
    - SYSTEM - USER-Attribute - Authority applies across entire RACF system
    - GROUP - CONNECT-Attribute - Authority limited by Scope-of-Groups

- Group CONNECT AUTHORITY(authority)
  - Authority levels - listed in ascending authority order
    - USE Use access granted to Group
    - CREATE Create Group datasets and dataset profiles
    - CONNECT Connect and Remove users for Group
    - JOIN Create users (with CLAUTH(USER)) and create subgroups
  - Authorities are cumulative
  - Scope-of-Groups does not extend authority

Other Administrative Authorities

- Profile ownership
  - Every profile has an owner
  - When owned by a Group, a user with Group-SPECIAL can administer the profile
  - When owned by a User, the User can administer the profile

- Class Authorization - CLAUTH(*class*) - assigned to a user to allow the user to create profiles in the designated class

- Password reset authority - granted by permissions to FACILITY class profiles
  - IRR.PASSWORD.RESET - All users
  - IRR.PWRESET.*owner* - All users owned by this user or group
  - IRR.PWRESET.*group-tree* - All users within the scope of this group

- Profile segment administration - granted by permissions to FIELD class profiles
  - *profile-type.segment.segment-field* (e.g., USER.OMVS.UID)

- ALTER access to a discrete profile allows deleting and modifying the profile

RACF Administrative Tools

- Data Security Monitor Utility (DSMON) - ICHDSM00
  - Various reports on RACF exits, options, user attributes, and dataset protection

- Database Unload Utility - IRRDBU00
  - Creates text copy of RACF database
  - Can be processed with REXX and DFSORT / ICETOOL - See SYS1.SAMPLIB(IRRICE)
  - Comes with DB2 load and query SQL samples

- Remove ID Utility - IRRRID00
  - Builds commands to delete obsolete permits, owners, and profiles

- SMF Unload Utility - SMF Dump IFASMFDx User Exits IRRADU00 and IRRADU86
  - Creates text copy of RACF-related SMF records
  - Can be processed with REXX and DFSORT / ICETOOL - See SYS1.SAMPLIB(IRRICE)
  - Comes with DB2 load and query SQL samples

ICH408I Message

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 LOG=NONE or NOFAIL
- 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 DASD 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 PASSWORD OR PASS PHRASE ATTEMPTS
    - REVOKED USER ACCESS ATTEMPT
    - INACTIVE USER HAS BEEN REVOKED (INACTIVE)
    - NOT AUTHORIZED TO APPLICATION (APPL)
    - SUBMITTER NOT AUTHORIZED BY USER (SURROGAT)
    - NOT AUTHORIZED TO SUBMIT JOB *jobname* (JESJOBS)
    - USER AT TERMINAL(*terminal-id*) NOT RACF-DEFINED

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        )
ICH408I LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL TCP00017
```

References

- IBM z/OS manuals
  - z/OS Security Server RACF Command Language Reference
  - z/OS Security Server RACF Security Administrator's Guide
  - z/OS Security Server RACF System Programmer's Guide
  - z/OS Security Server RACF Auditor's Guide

- RSH Consulting - RACF Center - www.rshconsulting.com/racfres.htm
  - Presentations
  - Tips Newsletters
  - Surveys
  - White Papers
  - … etc …

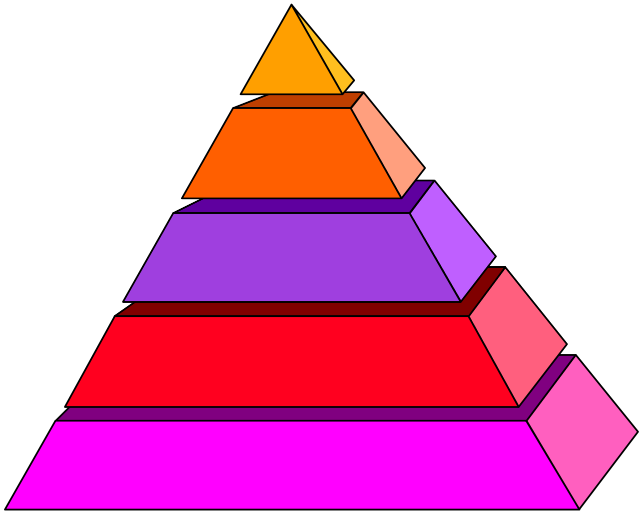
- Internet Discussion Lists - racf-l

- Mainframe Basics for Security Professionals: Getting Started with RACF; Mark Nelson, et al; IBM Press, 2008

RACF In Relation To Other Security

- RACF is but one component of a z/OS security program

- 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