RSH
CONSULTING

RACF Grouping Class Profiles

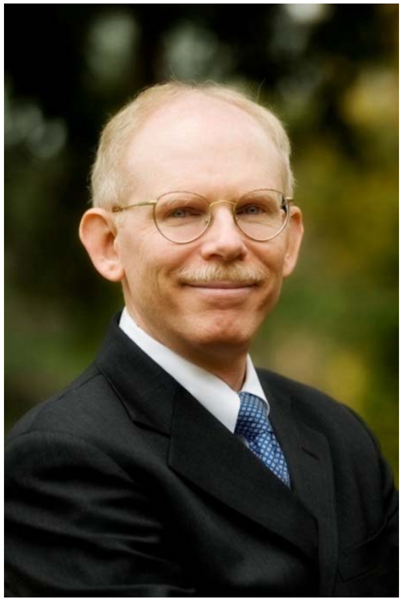
GARUG - May 2017

RSH CONSULTING, INC. • RACF SPECIALISTS • 617-969-9050 • WWW.RSHCONSULTING.COM

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

Grouping Class Profiles - Basics

- One-to-many relationship of profile to resources and enable resources with dissimilar names to be protected by a single profile (e.g., CICS transactions PAY1, RPAY, INQP)
- Defined in Grouping resource classes (e.g., GCICSTRN)
- Grouping profile names are merely labels for a set of resources
  - Need not match the names of the resources protected
  - Can conform to a naming standard related to a role (e.g., PAY.MGR.TRNS)
- Contain members, which are the resources they protect

```
RDEFINE  G$CTSTRN  PGT1.MGRS  ADDMEM( PAY1  RPAY  INQP  PX* )
```

- Access permissions and audit options assigned to a Grouping profile apply to all of its members
- Simplifies administration by replacing many individual Member class profiles with a fewer number of Grouping profiles

General Resource Profile - Basics

```
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

...

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
```

Grouping Class Definition

- Grouping classes are defined in the Class Descriptor Table (CDT) as part of a Member/Grouping pair
  - The GROUP and MEMBER parameters are specified to point to the companion class
- Both classes in a Member/Grouping pair should be defined with the same POSIT value
  - SETROPTS settings (e.g., GENERIC) will be applied to both classes
  - RACLIST REFRESH of the Member class will include its companion Grouping class
- The profile length for the Grouping class can be set to the maximum of 246 because the profile names are simply labels and not resource names
- IBM-supplied Member/Grouping class pairs - see CDT lists
  - http://www.rshconsulting.com/racfres.htm#RACFinfo

Class Descriptor Table (CDT) Macro and Profile

ICHRRCDE Table - ICHERCDE Macro

```
T$CTSTRN  ICHERCDE CLASS=T$CTSTRN,
                   GROUP=G$CTSTRN,
                   ID=145,
                   MAXLNTH=13,
                   FIRST=ANY,
                   OTHER=ANY,
                   POSIT=130,
                   DFTUACC=NONE,
                   OPER=NO

G$CTSTRN  ICHERCDE CLASS=G$CTSTRN,
                   MEMBER=T$CTSTRN,
                   ID=145,
                   MAXLNTH=246,
                   FIRST=ANY,
                   OTHER=ANY,
                   POSIT=130,
                   DFTUACC=NONE,
                   OPER=NO
```

CDT Class Profile (member class)

```
RLIST CDT T$CTSTRN CDTINFO NORACF
CLASS      NAME
-----      ----
CDT        T$CTSTRN

CDTINFO INFORMATION
-------------------
CASE = UPPER
DEFAULTRC = 004
DEFAULTUACC = NONE
FIRST = ALPHA,NUMERIC,NATIONAL,SPECIAL
GENLIST = DISALLOWED
GROUP = G$CTSTRN
KEYQUALIFIERS = 0000000000
MACPROCESSING = NORMAL
MAXLENGTH = 13
MAXLENX = NONE
MEMBER =
OPERATIONS = NO
OTHER = ALPHA,NUMERIC,NATIONAL,SPECIAL
POSIT = 0000000130
PROFILESALLOWED = YES
RACLIST = DISALLOWED
SECLABELSREQUIRED = NO
SIGNAL = NO
```

RACLIST

- All profiles for a General Resource class are copied to a dataspace in memory for shared use and rapid reference
- Required to exploit grouping class profiles (e.g., GDASDVOL)
  - Member and Grouping class profiles are merged
- Required for RACROUTE REQUEST=FASTAUTH processing

- Two techniques for RACLISTing a class
  - RACF command SETROPTS RACLIST(*class*)
    - CDT entry must specify RACLIST=ALLOWED
    - Class is RACLISTed on all z/OS systems sharing the RACF database

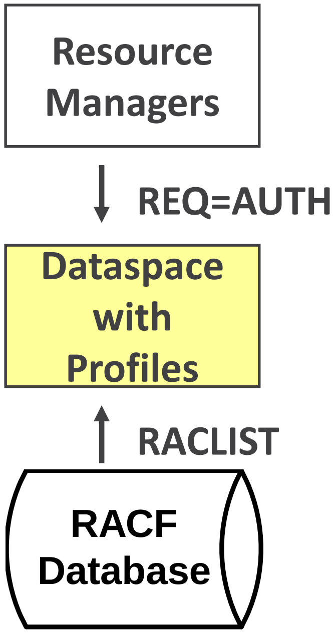
```
SETR RACLIST CLASSES = APPL CDT DSNR FACILITY STARTED
```

  - Resource Manager executes RACROUTE REQUEST=LIST,GLOBAL=YES

    CICS DB2 IMS VTAM MQ

    - Class is only RACLISTed on the z/OS system where the Resource Manager is running
    - RACROUTE RACLISTing ignores CDT RACLIST=DISALLOWED setting

```
GLOBAL=YES RACLIST ONLY = TCICSTRN
```



Resource Managers

REQ=AUTH

Dataspace with Profiles

RACLIST

RACF Database

RACLIST REFRESH

- Whenever profiles are created, changed, or deleted, the dataspace has to be refreshed to retrieve an updated copy of the profiles

  SETROPTS RACLIST(*class*) REFRESH

- REFRESH Considerations
  - Ensure REFRESH is performed on all systems sharing database
    - With RACF Sysplex Communications - one REFRESH does all systems
    - With RRSF Automatic Direction - one REFRESH does all RRSF nodes
  - One REFRESH does all classes with the same POSIT value (e.g., all IBM default CICS classes have POSIT 5)
  - REFRESH warning
    - For changes made to SETROPTS RACLISTed Member class profiles, RACF issues message

      ICH11009I RACLISTED PROFILES FOR *class* WILL NOT REFLECT THE UPDATE(S) UNTIL A SETROPTS REFRESH IS ISSUED.
    - No warning is given for ..
      - Changes to Grouping class profiles
      - Changes to profiles in classes RACLISTed by RACROUTE REQUEST=LIST,GLOBAL=YES

Grouping Profiles

- RACLISTing merges the all profiles in a paired set of Grouping and Member classes to create a combined list for determining access authorization

- Grouping and Member profiles

```
GCICSTRN FINCLK UACC(NONE)
        ADDMEM( F030 F234 FN* )
GCICSTRN FINMGR UACC(NONE)
        ADDMEM( F0A1 F234 FUPT )
TCICSTRN FN73 UACC(READ)
TCICSTRN FN8* UACC(NONE)
TCICSTRN F234 UACC(READ)
TCICSTRN ** UACC(READ)
```

- Merged profiles with UACCs after RACLISTing (lowest UACC applied)

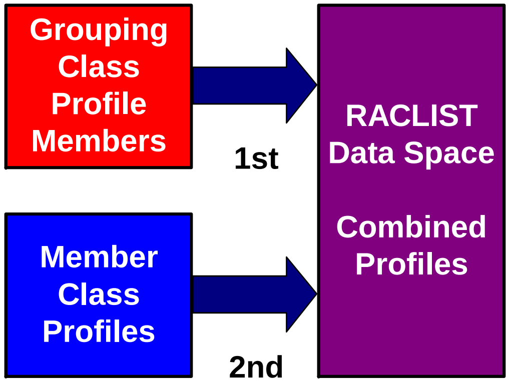
FN73	READ
FN8*	NONE
FN*	NONE
FUPT	NONE
F0A1	NONE
F030	NONE
F234	NONE
**	READ

- A resource may be defined in more than one Grouping class profile and as both a member of a Grouping class profile and a Member class profile; this increases complexity

Grouping Profiles

- Member class (e.g., TCICSTRN) must be RACLISTed for the Grouping class profiles to take effect

- During RACLISTing, RACF builds a combined list of profiles
  - A RACLIST profile is created first from each Grouping class profile member and then from each Member class profile
  - When a member is encountered more than once, the associated profile contents are merged
    - Access for each user and group is set to the highest permitted
    - UACC is set to the lowest UACC
    - Auditing settings are combined to be the most inclusive
    - First WARNING Mode setting encountered is applied



- If, in the process of merging profiles, the total number of access list entries for a single resource exceeds 7,200 entries, the RACLIST will abend

Grouping Profiles

HCICSFCT ACCTFIL1

ADDMEM(VENDMAST)

UACC(READ) AUDIT(FAILURE(READ))
NOWARNING

HCICSFCT ACCTFIL3

ADDMEM(VENDMAST)

UACC(NONE) AUDIT(ALL) WARNING

ID(ACCTPAY) ACC(UPDATE)

FCICSFCT VENDMAST

UACC(NONE) AUDIT(NONE) NOWARNING

ID(ACCTMGT ACCTPAY) ACC(READ)

Composite Profile VENDMAST after RACLISTing

UACC(NONE) AUDIT(ALL) NOWARNING

ID(ACCTMGT) ACC(READ)

ID(ACCTPAY) ACC(UPDATE)

Grouping Profiles - Exercise

```
GCICSTRN ACCTG1 ADDMEM( AC* )
   UACC( NONE )  AUDIT( FAILURE( READ ) ) WARNING
   ID( ACCTMGRS ) ACC( READ )

GCICSTRN ACCTPAY1 ADDMEM( ACX*  )
   UACC( NONE )  AUDIT( SUCCESS(READ) )  NOWARNING
   ID( ACCTPAY )  ACC( READ )

TCICSTRN ACX3
   UACC( NONE )  AUDIT( NONE )  NOWARNING
   ID( ACCTMGRS ) ACC( READ )

TCICSTRN AC*
   UACC( READ )  AUDIT( ALL )  NOWARNING
   ID( EXTUSER ) ACC( NONE )
```

What composite profiles and access lists would be built?

Who would get access to transaction ACX3, ACXA, and ACP3?

Grouping Profiles - Exercise

PROFILE	UACC	AUDIT	WARNING	PERMIT

Grouping Profiles - Design Strategies

- Grouping by User Role

PROFILE	MEMBERS	GROUP PERMITS
PAY.ADMN	PAY0 PYR0	PAYADM
PAY.CLKS	PAY0 PYU1 PYR0 PYXC	PAYCLK
PAY.MGRS	PAY0 PYU1 PYR0 PYXC PYU2	PAYMGR

- Grouping by Application Function

PROFILE	MEMBERS	GROUP PERMITS
PAY.QUERY	PAY0 PYR0	PAYADM PAYCLK PAYMGR
PAY.UPDTACCT	PYU1 PYXC	PAYCLK PAYMGR
PAY.OVERRIDE	PYU2	PAYMGR

CICS - RACF Classes and Prefixing

- Class configuration options for different CICS regions in a system or sysplex
  - Share default classes among CICS regions
    - SIT XTRAN=YES   TCICSTRN + GCICSTRN
  - Create locally-defined independent classes for each region or set of related regions (e.g., production/QA/test or specific application)
    - SIT XTRAN=$TTRN   T$TTRN + G$TTRN
  - Use some combination of the above

- Classes shared by dissimilar CICS regions (e.g., PROD and TEST)
  - May need to differentiate resources belonging to specific regions
  - Can assign prefix to resource names to differentiate resources
  - SIT Parameter - SECPRFX=<u>NO</u> | YES | *prefix*
    - NO   No prefix
    - YES   Prefix with CICS Region's ID (e.g., CICS01.PAY1)
    - *prefix*   Prefix with specified prefix (e.g., PROD.PAY1)
  - Selected prefix is appended as the first qualifier for Member class profiles or Grouping class members

CICS - RACF Classes and Prefixing

```
RLIST T$TTRN CEMT ALL                with SECPRFX=NO,XTRAN=$TTRN
CLASS      NAME
-----      ----
T$TTRN     C* (G)

GROUP CLASS NAME
----- ----- ----
G$TTRN

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

LEVEL  OWNER      UNIVERSAL ACCESS   YOUR ACCESS  WARNING
-----  --------   ----------------   ---- ------  -------
 00    CICSSPT         NONE              NONE       YES
```

```
RLIST G$TTRN CICS.CAT2 ALL
CLASS      NAME
-----      ----
G$TTRN     CICS.CAT2

MEMBER CLASS NAME
------ ----- ----
T$TTRN

RESOURCES IN GROUPS
--------- -- ------
CE* (G)

LEVEL  OWNER      UNIVERSAL ACCESS   YOUR ACCESS  WARNING
-----  --------   ----------------   ---- ------  -------
 00    CICSSPT         NONE              NONE       YES
```

CICS - RACF Classes and Prefixing

```
RLIST TCICSTRN CICT1.CEMT ALL          with SECPRFX=YES,XTRAN=YES
CLASS      NAME
-----      ----
TCICSTRN   CICT1.C* (G)

GROUP CLASS NAME
----- ----- ----
GCICSTRN

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

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

```
RLIST GCICSTRN CICS.CAT2.T1 ALL
CLASS      NAME
-----      ----
GCICSTRN   CICS.CAT2.T1

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

RESOURCES IN GROUPS
--------- -- ------
CICT1.CE* (G)

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

Grouping Class Profile Administration

- Grouping class profiles are always defined as discrete profiles
  - Generic characters used in grouping class profile names are treated as non-generic
- Class Authorization - User Attribute - ADDUSER/ALTUSER CLAUTH(*class*)
  - Allows a user to create new profiles
  - Applies to all classes with matching POSIT
    - LISTUSER only shows specified class added to the ID, not all applicable ones
  - Allows a user to issue a SETROPTS REFRESH for the class
  - Once the profile is created, other authority is required to administer it
- Group-SPECIAL, OWNER(*userid*), or ALTER access to an existing Grouping class profile
  - Allows a user to add a resource to the Grouping class profile if the user has one of these authorities over a profile currently protecting the resource
  - Allows a user to delete members from the profile and delete the profile
  - Allows a user to change the UACC or access list for a profile
  - Does not allow the user to issue a SETROPTS REFRESH

Grouping Class Profile Administration

- Any of the following actions could change the UACC, LEVEL, WARNING, AUDITING, and permissions for a resource
  - Adding a pre-existing Grouping profile resource to another Grouping class profile
  - Defining a Member class profile for pre-existing Grouping profile resource
  - Removing a resource from a Grouping class profile if it is defined in other Grouping profiles or as a Member class profile
  - Deleting a Grouping class profile whose resource(s) is defined in other Grouping profiles or as a Member class profile
  - Deleting a Member class profile if the profile is defined as a resource in a Grouping class profiles
  - Example:
    ```
    RDEF  GCICSTRN  MGRTRAN1  UACC(NONE)  ADDMEM(PAY1)
    RDEF  GCICSTRN  CLKTRANA  UACC(READ)  ADDMEM(PAY1)
    RALT  GCICSTRN  MGRTRAN1  DELMEM(PAY1)      - PAY1 UACC now ?
    ```

- A blocking access permit of NONE for a user or group can be overridden by a higher permit to a different profile protecting the same resource

Grouping Class Profile Tips

- To activate WARNING or AUDIT(ALL) for a single, specific resource defined in another profile with other resources, define and add it to a preceding profile

```
RDEF  GCICSTRN  $$WARN  WARNING  ADDMEM(TRNX)  UACC(CONTROL)
```

- ICH408I violation messages only show the member class; there is no indication of what, if any, grouping profiles the resource is defined to

- RLIST RESGROUP can be used to find discrete members in Grouping profiles

  RLIST *member-class resource* RESGROUP

- Members can either be discrete (e.g., PAY1) or generic (e.g., PX*, &CTRN)
  - Recommendation - define generics only as Member class profiles and not as members in Grouping class profiles to facilitate use of RLIST and RESGROUP

Grouping Class Profile Tips

- When using RLIST to list a Member class profile, specify NOYOURACC to avoid unnecessary RACLIST processing

  RLIST *member-class resource* NOY

- If a Member/Grouping class pair is RACLISTed by an application (e.g., CICS) using RACROUTE REQUEST=LIST,GLOBAL=YES, set RACLIST=DISALLOWED in their CDT definitions
  - Prevents use of SETROPTS RACLIST that needlessly RACLISTs the class on all systems
  - Class will be RACLISTed only on those systems where needed

- Conceptually, a Grouping class profile resource is a Member class profile and a Grouping class profile is a set of Member class profiles

"Special" Grouping Class

RSH RACF TIPS - July 2014

Several RACF classes are technically grouping classes even though we do not recognize them as such. As with other grouping classes, they have companion member classes and you manage the contents of their profiles using ADDMEM and DELMEM. Each of these classes is shown below with its associated member class.

PROGRAM	PMBR
GLOBAL	GMBR
NODES	NODMBR
RACFHC	RACHCMBR
RACFVARS	RVARSMBR

The member classes exist solely because RACF architecture requires every grouping class to have an associated member class. RACF does not allow profiles to be created in these classes.

Grouping Profiles - Exercise - Answers

PROFILE	UACC	AUDIT	WARNING	PERMIT
ACX3	NONE	NONE	NOWARN	ACCTMGRS- READ
ACX*	NONE	S(READ)	NOWARN	ACCTPAY- READ
AC*	NONE	ALL	WARN	ACCTMGRS- READ EXTUSER- NONE

Access:

- ACCTMGRS would get access to ACX3 through profile ACX3
- ACCTPAY would get access to ACXA through profile ACX*
- ACCTMGRS would get access to ACP3 through profile AC*; all other users would get access with WARNING