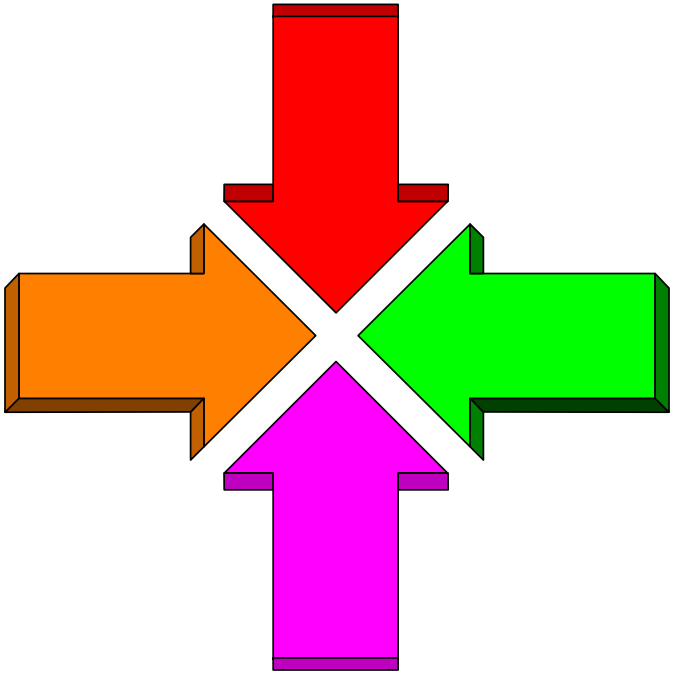
HOW GROUPING & MEMBER PROFILES ARE MERGED DURING RACLIST

November 2011



Robert S. Hansel

Lead RACF Specialist - RSH Consulting, Inc.

R.Hansel@rshconsulting.com - 617-969-9050 - www.rshconsulting.com

RSH INSTRUCTOR

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., a firm he 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. He has worked with IBM mainframes since 1976 and in information systems security since 1981. Mr. Hansel began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

Contact and background information:

- **617-969-8211**
- **R.Hansel@rshconsulting.com**
- **www.linkedin.com/in/roberthansel**

GROUPING PROFILES

One-to-many relationship of profile to resources

Defined in the Grouping resource classes (e.g., GCICSTRN)

Enable resources with dissimilar names to be protected by a common profile (e.g., CICS transactions PAY1, RPAY, INQP)

Contain members, which are the resources they protect

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

Simplifies administration by replacing many individual member class profiles with a fewer number of grouping profiles

GROUPING PROFILES

Grouping profile names

- **Need not match the names of the resources protected**
- **Can conform to a naming standard meaningful to the organization (e.g., PAY.MGR.TRNS)**

A resource can be a member of more than one Grouping profile (caution - increases complexity)

Member entries can either be discrete (e.g., PAY1) or generic (e.g., PX*)

Grouping profiles can be used in combination with Discrete and Generic profiles in the resource class (caution - increases complexity)

GROUPING PROFILES

```
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

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

USER      ACCESS    ACCESS COUNT
----      ------    ------ -----
RJONES2   ALTER
CICSSPT   UPDATE
DASDMGT   READ
JWILLS2   NONE
```

GROUPING PROFILES - STRATEGIES

Grouping by User Role

```
PAY.ADMN      ADDMEM( PAY0 PYR0 )
    PERMIT ID(PAYADM) ACC(READ)
PAY.CLKS      ADDMEM( PAY0 PYR0 PYU1 PYXC )
    PERMIT ID(PAYCLK) ACC(READ)
PAY.MGRS      ADDMEM( PAY0 PYR0 PYU1 PYXC PYU2 )
    PERMIT ID(PAYMGR) ACC(READ)
```

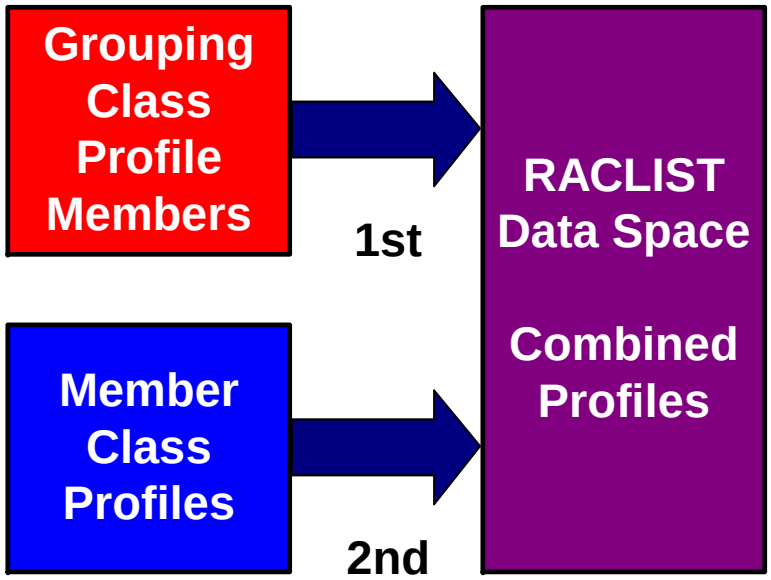
Grouping by Application Function

```
PAY.MAIN      ADDMEM( PAY0 PYR0 )
    PERMIT ID(PAYADM PAYCLK PAYMGR) ACC(READ)
PAY.UPDTA     ADDMEM( PYU1 PYXC )
    PERMIT ID(PAYCLK PAYMGR) ACC(READ)
PAY.UPDTM     ADDMEM( PYU2 )
    PERMIT ID(PAYMGR) ACC(READ)
```

RACLIST PROFILE MERGE

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

- **SETROPTS RACLIST(*class*) [REFRESH]**
- **RACROUTE REQUEST=LIST,GLOBAL=YES (issued by caller - e.g., CICS)**



RACLIST PROFILE MERGE

During RACLISTing, RACF builds a combined list of profiles

- **A RACLIST profile is created from each grouping class profile Member and member class Discrete and Generic profile**
- **Grouping class profiles are processed first**
- **When a member is encountered more than once, the associated profile contents are merged**
  - **Access for each user and group is based on the highest permitted**
  - **UACC is based on the lowest UACC**
  - **Auditing is set to be the most inclusive**
  - **First WARNING Mode setting encountered is applied**
- **If the total number of access list entries for a set of profiles that are to be merged exceeds 7200 entries, the RACLIST will abend**

RACLIST PROFILE MERGE

Grouping & Member profiles with UACC

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

Composite Profile List with UACC after RACLISTing

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

RACLIST PROFILE MERGE

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(ACCTPAY) ACC(READ)
ID(ACCTMGT) ACC(READ)

Profile after RACLISTing ...

FCICSFCT VENDMAST

UACC(NONE) AUDIT(ALL) NOWARNING
ID(ACCTMGT) ACC(READ)
ID(ACCTPAY) ACC(UPDATE)

PROFILE MERGE - 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

DETERMINING PROTECTING PROFILE(S)

Finding the protecting profile may require executing the following commands

- **SEARCH CLASS(*mbr-class*)** **- discrete & generic profiles**
- **RLIST *mbr-class resource* RESGROUP** **- grouping with discrete**
- **RLIST *grp-class* *** **- grouping with generics**

Analyze resulting profiles and members to determine protection

GROUPING PROFILES - EXERCISE ANSWER

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

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

AC* UACC(NONE) AUDIT(ALL) WARNING
ID(ACCTMGRS) ACC(READ)
ID(EXTUSER) ACC(NONE)

- **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**