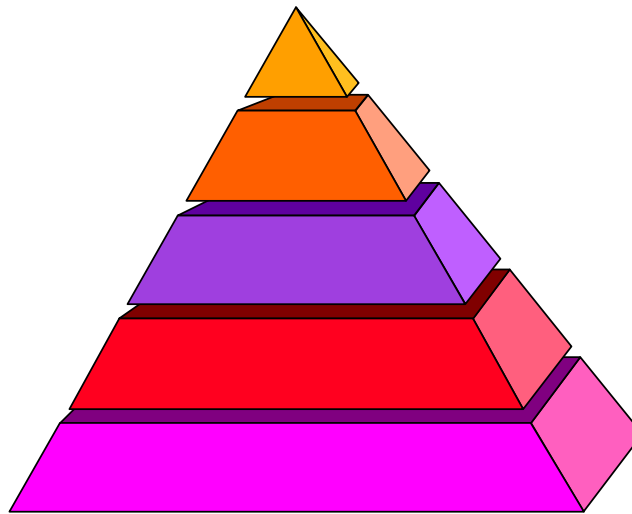


RACF ADMINISTRATIVE AUTHORITIES

KOIRUG - October 2005



Robert S. Hansel

RACF Specialist - RSH Consulting, Inc.

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

ADMINISTRATION

Administrative Capabilities

System and Group Attributes

Profile Ownership

Group Connect Authorities

Class Authorization

FACILITY Class IRR Profiles

FIELD Class Profiles

Access Enabled Authority

Miscellaneous Authorities

Implementation Suggestions

ADMINISTRATIVE CAPABILITIES

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD	RLIST	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER	ALTGROUP	ALTDSD	RALTER	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

Highlights:

- Green - yes
- Yellow - yes but with footnote caveats listed beneath each chart

SYSTEM AND GROUP ATTRIBUTES

AUDITOR	View RACF profiles & set audit options
SPECIAL	Administer RACF profiles & set control options
OPERATIONS	Access resources & define group dataset profiles

SYSTEM AND GROUP ATTRIBUTES

SYSTEM / USER-Attribute

ALU userid attribute

```
USER=JSMITH1  NAME=JOHN SMITH          OWNER=SECGRP1  CREATED=01.067
DEFAULT-GROUP=USRGRPA  PASSDATE=00.351  PASS-INTERVAL= 30
ATTRIBUTES=OPERATIONS
```

Authority applies across entire RACF system

GROUP / CONNECT-Attribute

CO userid GROUP(groupid) attribute

```
GROUP=DASDMGT  AUTH=USE  CONNECT-OWNER=RJONES2  CONNECT-DATE=92.181
CONNECTS=      00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=SPECIAL
```

Authority limited by Scope-of-Groups

SCOPE-OF-GROUPS

Determines scope of authority for:

- **Group-AUDITOR**
- **Group-SPECIAL**
- **Group-OPERATIONS**

Based on Profile Ownership, not Group Structure

Cache group tree in Virtual Lookaside Facility (VLF) to avoid repetitive retrieval of group profiles to determine scope-of-groups tree structure for Group-level authorities

- **Implement only if group authority is used extensively**
- **SYS1.PARMLIB(COFVLFxx) entry**

CLASS NAME(IRRGTS)

EMAJ(GTS)

SCOPE-OF-GROUPS

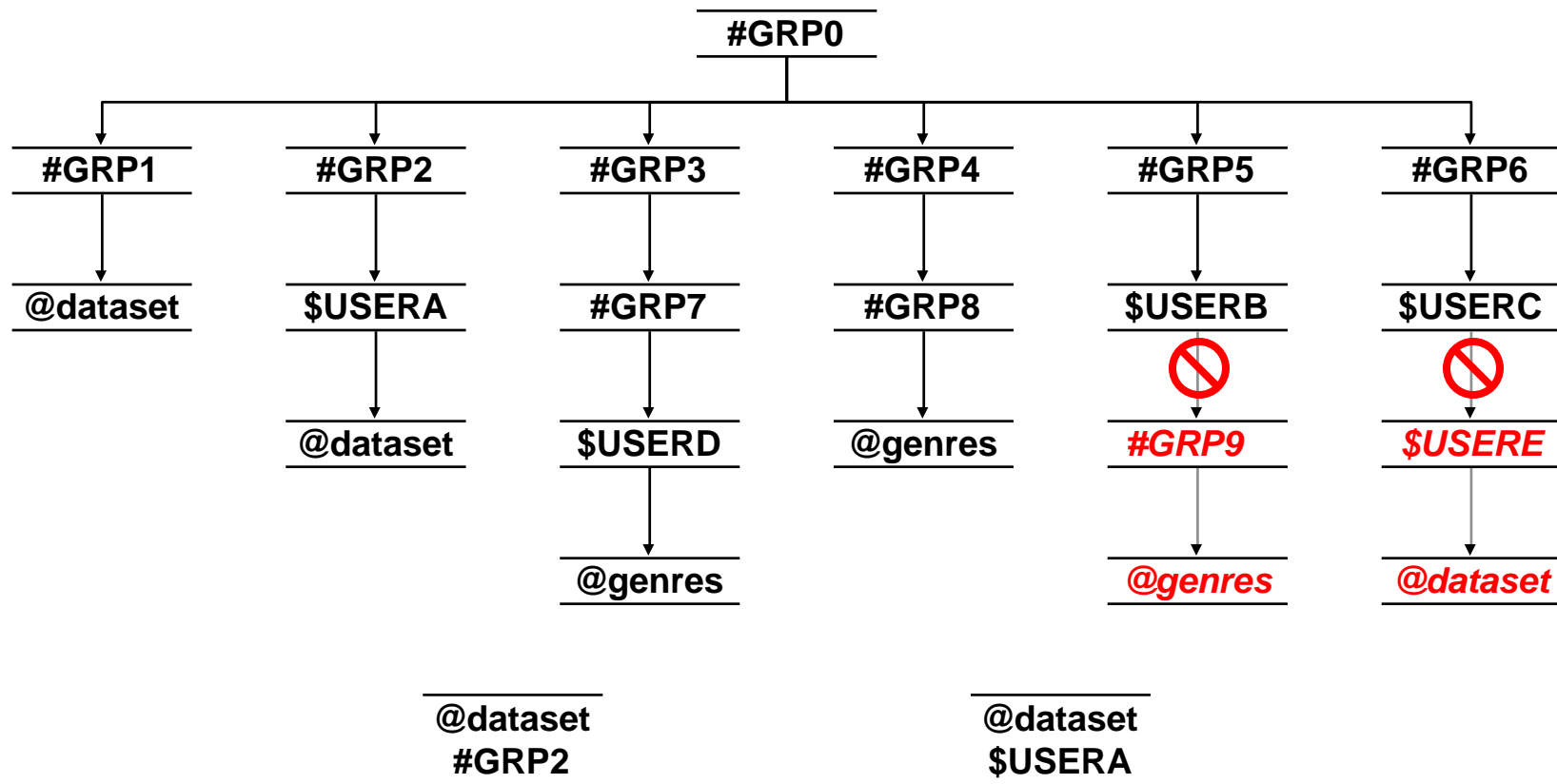
Included:

- Profiles owned by the Group
- Profiles owned by Subgroups owned by the Group
- Profiles owned by Subgroups owned by Subgroups (etc.) owned by the Group
- Resource Profiles owned by Users owned by the Group or its Subgroups
- Dataset Profiles with HLQ is same as a User or Group owned by the Group or its Subgroups

Excluded:

- User and Group Profiles owned by Users within the Scope-of-Groups
- Profiles owned by either Users or Groups owned by Users within the Scope-of-Groups (dataset exception)
- Profiles owned by either Users or Groups outside the Scope-of-Groups (dataset exception)

SCOPE-OF-GROUPS



AUDITOR - System

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD	RLIST	DSMON
Set Options ⁽¹⁾	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER ⁽²⁾	ALTGROUP	ALTDSD ⁽³⁾	RALTER ⁽³⁾	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Audit Options only: SAUDIT OPERAUDIT CMDVIOL AUDIT
 LOGOPTIONS SECLEVELAUDIT SECLABELAUDIT APPLAUDIT

(2) UAUDIT only

(3) GLOBALAUDIT only

AUDITOR - Group

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER ⁽¹⁾	LISTGRP ⁽¹⁾	LISTDSD ⁽¹⁾	RLIST ⁽¹⁾	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER ⁽²⁾	ALTGROUP	ALTDSD ⁽³⁾	RALTER ⁽³⁾	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Excluding profile segments

(2) UAUDIT only

(3) GLOBALAUDIT only

SPECIAL - System

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST ⁽¹⁾	LISTUSER	LISTGRP	LISTDSD	RLIST	DSMON
Set Options ⁽¹⁾	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER ⁽²⁾	ALTGROUP	ALTDSD ⁽³⁾	RALTER ⁽³⁾	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Excluding Audit Options

(2) Excluding UAUDIT

(3) Excluding GLOBALAUDIT

SPECIAL - Group

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST ⁽¹⁾	LISTUSER ⁽²⁾	LISTGRP ⁽²⁾	LISTDSD ^(2,3)	RLIST ^(2,3)	DSMON
Set Options	ADDUSER ^(2,4,5,6)	ADDGROUP ⁽²⁾	ADDSD ⁽¹²⁾	RDEFINE ^(9,12)	IRRUT100
GLOBAL REFRESH	ALTUSER ^(2,5,6,7,11)	ALTGROUP ⁽⁸⁾	ALTDSD ⁽³⁾	RALTER ^(3,10)	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT ⁽⁶⁾	PERMIT ⁽¹²⁾	PERMIT ⁽¹²⁾	PROTECT-ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Excluding Audit Options

(2) Excluding Profile Segments

(3) Excluding GLOBALAUDIT

(4) Require CLAUTH(USER)

(12) If specify FROM, must have admin authority to FROM profile

(5) Excludes System-level attributes

(6) Only assign held attributes

(7) Excluding UAUDIT

(8) To change SUPGROUP, requires admin authority new group

(9) Create profiles from group profile members

(10) ADDMEM resources from member profiles

(11) Excludes NOEXPIRE on password change

OPERATIONS - System

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD ⁽¹⁾	RLIST ⁽¹⁾	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD ⁽²⁾	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER	ALTGROUP	ALTDSD	RALTER	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS ^(3,4)	GENRES ACCESS ^(3,5)	TEMPDSN ACCESS

(1) Excluding segments & GLOBALAUDIT

(2) Group datasets only

(3) If permitted accesses, access capped at the permitted level

(4) Create Group datasets unless connected to the Group with USE authority

(5) Classes defined with OPER=YES

OPERATIONS - Group

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD ⁽¹⁾	RLIST ⁽¹⁾	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD ⁽²⁾	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER	ALTGROUP	ALTDSD	RALTER	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS ^(3,4)	GENRES ACCESS ^(3,5)	TEMPDSN ACCESS

(1) Excluding segments & GLOBALAUDIT

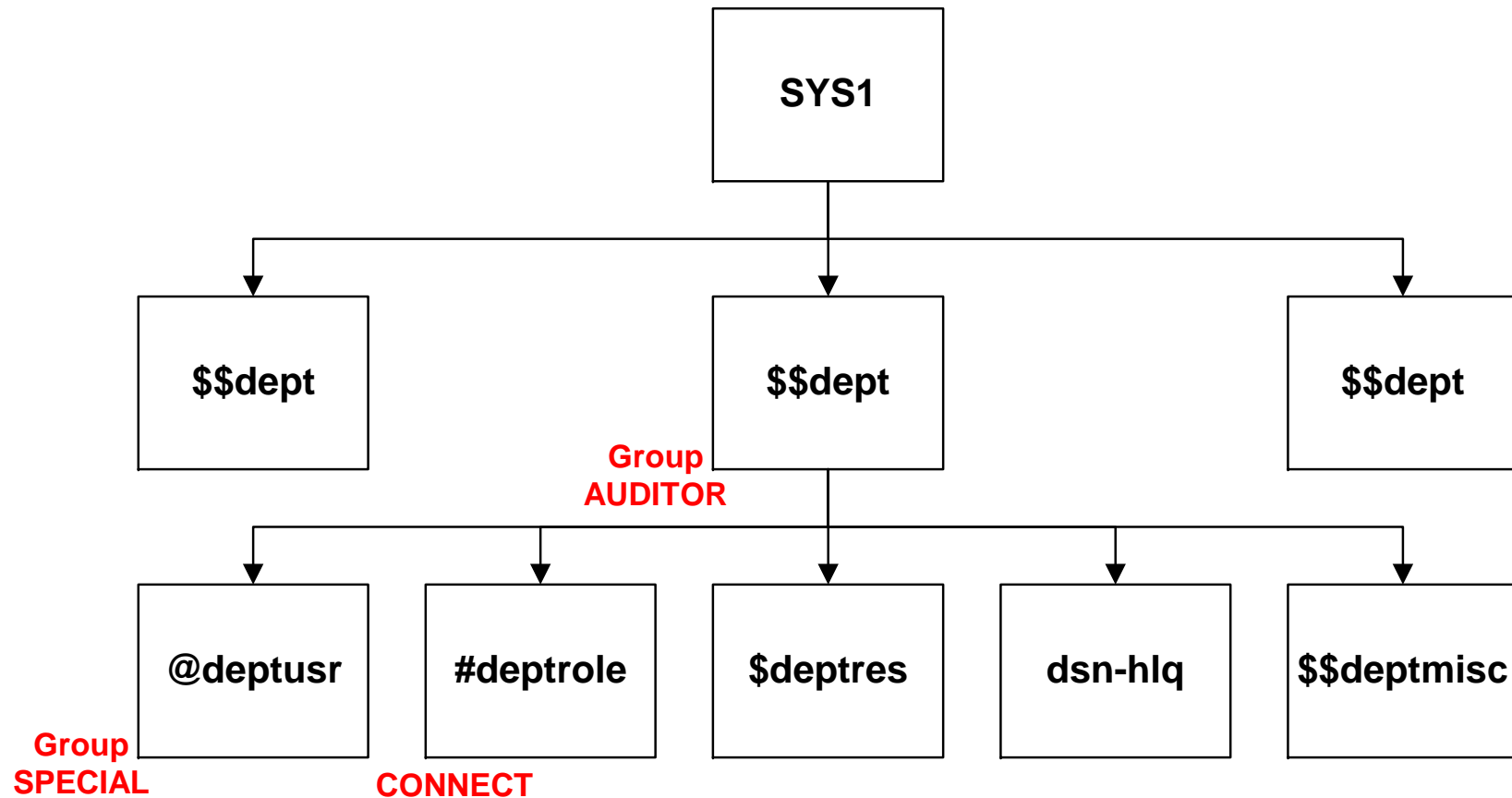
(2) Group datasets only

(3) If permitted accesses, access capped at the permitted level

(4) Create Group datasets unless connected to the Group with USE authority

(5) Classes defined with OPER=YES

GROUP AUTHORITY EXAMPLE



PROFILE OWNERSHIP

Authority depends on type of profile owned

- **User**
- **Group**
- **Dataset**
- **General Resource**

When owned by a Group, Group-level authority rules

When owned by a User, the User can administer the profile

The Profile Creator is made the Owner by default

Authority not extended by Scope-of-Groups

PROFILE OWNER - User Profile

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER ⁽¹⁾	LISTGRP	LISTDSD	RLIST	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100 ⁽²⁾
GLOBAL REFRESH	ALTUSER ⁽¹⁾	ALTGROUP	ALTDSD	RALTER	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Excluding segments, UAUDIT, & system-level attributes

(2) Only for User Profile owned

PROFILE OWNER - Group Profile

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP ⁽¹⁾	LISTDSD	RLIST	DSMON
Set Options	ADDUSER ^(2,3)	ADDGROUP ⁽¹⁾	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER	ALTGROUP ⁽¹⁾	ALTDSD	RALTER	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT ⁽⁴⁾	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

- (1) Excluding segments
- (2) Requires CLAUTH(USER)
- (3) Excluding segments, UAUDIT, & system-level attributes
- (4) Only assign held attributes

PROFILE OWNER - Dataset Profile

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD ⁽¹⁾	RLIST	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER	ALTGROUP	ALTDSD ⁽¹⁾	RALTER	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Excluding segments & GLOBALAUDIT

PROFILE OWNER - Gen. Resource Profile

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD	RLIST ⁽¹⁾	DSMON
Set Options	ADDUSER	ADDGROUP	ADDSD	RDEFINE	IRRUT100
GLOBAL REFRESH	ALTUSER	ALTGROUP	ALTDSD	RALTER ^(1,2)	RALTER GLOBAL ADDMEM
GENERIC REFRESH	DELUSER	DELGROUP	DELDSD	RDELETE	CATDSNS ACCESS
RACLIST REFRESH	PASSWORD	CONNECT	PERMIT	PERMIT	PROTECT- ALL ACCESS
		REMOVE	DATASET ACCESS	GENRES ACCESS	TEMPDSN ACCESS

(1) Excluding segments & GLOBALAUDIT

(2) ADDMEM resources owner has admin authority over

GROUP AUTHORITIES

USE	Use access granted to Group
CREATE	Create Group dataset profiles Create Group datasets
CONNECT	Connect & Remove users for Group Assign users up to same authority
JOIN	Create users (with CLAUTH(USER)) Assign users up to same authority Create Subgroups Delete Subgroups

**Authorities are cumulative
Scope-of-Groups does not extend authority**

CLASS AUTHORIZATION

Class Authorization - CLAUTH

- Allows creation of profiles and protection of undefined resources without System-SPECIAL
- User profile attribute - *ALU userid* CLAUTH(*class*)
- Can be used for all classes except GROUP and DATASET

User Profiles - CLAUTH(USER)

- Requires Group-SPECIAL, JOIN authority, or group owner

General Resource Profiles - CLAUTH(*class*)

- SETROPTS
 - Refresh GENERIC, GLOBAL, RACLIST for CLAUTH class
 - Refresh WHEN(PROGRAM) with PROGRAM class
- ADDMEM undefined resources to grouped profiles or Global Access Table

CLASS AUTHORIZATION

GENERICOWNER SETROPTS Option

- Owner of General Resource generic profile retains control over profile protected resources
- Restricts ability of other users with CLAUTH to create undercutting profiles (e.g., cannot create AB* undercutting A*)
- Only owner and users who also have Group-SPECIAL where profile is within Scope-of-Groups can create undercutting profiles
- Does not apply to PROGRAM class

CLAUTH authority extends to all resources classes with the same POSIT value even though they may not appear in the LISTUSER display

Once a profile has been created, creator's ability to administer the profile is determined by normal administrative authorities

FACILITY CLASS IRR PROFILES

User password reset authorization

- **Intended for Help Desk functions**
- **Reset any USERID's password, except those with System-level SPECIAL, OPERATIONS, or AUDITOR, or PROTECTED IDs**
- **General Resource**
 - **Class & Profile - FACILITY IRR.PASSWORD.RESET**
 - **Access Levels**
 - ◆ **READ - Resume user, reset password to expired value**
 - ◆ **UPDATE - Resume user, reset password to non-expired value**
 - ◆ **CONTROL - Change password prior to MINCHANGE interval (z1.7)**
- **Tip - to block reset, either:**
 - **Revoke user's default group connect (retains password)**
 - **Make PROTECTED (erases password)**

FACILITY CLASS IRR PROFILES

User profile list authorization

- **List any user profile, except those with System-level authorities**
- **General Resource**
 - **Class & Profile - FACILITY IRR.LISTUSER**
 - **Access Level - READ - list any user profile**
- **Can only list base profile, not segments**

FIELD CLASS PROFILES

Delegate maintenance of profile segments (e.g., TSO, OMVS)

General Resource

- Class - FIELD
- Profile - *profile-type.segment.field* (e.g., USER.TSO.ACCTNUM)
- Access Levels
 - READ - examine
 - UPDATE - change

Applies to all profiles, no Scope-of-Groups limitation

&RACUID can be used to permit users access to just their own USER segment(s) - usually to allow viewing (READ)

ACCESS ENABLED AUTHORITY

READ or Greater

- **List basic RACF segment information**
 - **Does not include access list or GLOBALAUDIT settings**
- **Prohibited if user connected to any Group with access of NONE**

ALTER in Discrete profile

- **Change, delete, and list access list of profile**
- **Permit access**
- **If permitted to a member-class profile (e.g., TCICSTRN), can ADDMEM the resource to any grouping-class profile (e.g., GCICSTRN)**
- **If permitted to a grouping-class profile (e.g., GCICSTRN), can create a member-class resource profile for grouping-class members**

USERID, Group, ID(*), and UACC granted access all apply

UNIVERSAL USER AUTHORITY

Any User

- **Change own User profile Name, Default Group, Model Dataset (if active)**
- **Change own User profile Password, Password-interval**
- **Change own User profile TSO logon defaults (e.g. Logon Proc)**
- **List own User profile**
- **Execute Cross-Reference Utility on own USERID**
- **Create, change, delete own user dataset profiles**
- **Add own user datasets to GLOBAL Access Table**
- **Issue RVAR Y command**

GRPACC AUTHORITY

GRPACC - Group Access

- **When a User creates a Group dataset profile, the Group itself is automatically granted UPDATE access**
 - User creates profile PAY.MAST.FILE
 - Group PAY is automatically added to access list with UPDATE access
- **System-level Attribute**
 - Applies to all Group dataset profiles created by the user
 - Supercedes Group-GRPACC
- **GROUP-level Attribute**
 - To enable its use, user must specifically log on to the Group where the user's group connect has this authority
 - Applies to any Group in the user's administrative scope, even those outside of the normal GRPACC Scope-of-Groups

MISCELLANEOUS AUTHORITY

Prevent automatic grant of ALTER access to creator's USERID during profile creation

- **RACF SETROPTS option**
- **ADDCREATOR** - add to access list (default)
- **NOADDCREATOR** - do not add to access list

UACC on Group Connect

- **Default UACC assigned upon profile creation**
- **Depends on Connect Group at time of profile creation**
- **Used when Default UACC in Class Descriptor Table specifies ACEE**
- **Defaults to NONE**

Automatic Dataset Protection (ADSP)

- **Activated in SETROPTS & assigned to user profile or group connect**
- **Automatically generates discrete profiles when creating datasets**

IMPLEMENTATION SUGGESTIONS

Ownership by Group only (except TSO users & their datasets)

Group Ownership follow Group Hierarchy

Avoid mixing Group Usage; Segregate Resource Owning Groups from Access Granting Groups

Limit assignment of SPECIAL, OPERATIONS, and CLAUTH

Restrict OPERATIONS access with Exclusion Group

Limit use of Discrete Dataset Profiles

Limit use of Discrete General Resource Profiles with ALTER access

Activate GENERICOWNER and NOADDCREATOR

Avoid ADSP, GRPACC, and Group UACC

Monitor all use of authorities - OPERAUDIT, SAUDIT, AUDIT(*)