RSH CONSULTING

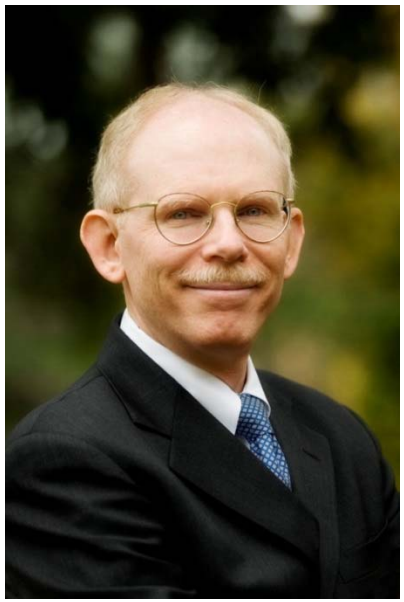
RACF
Administrative Authorities

KOIRUG - November 2015

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

Administrative Authorities

- System & Group Authorities
- Profile Ownership
- Group Connect Authorities
- Class Authorization (CLAUTH)
- FACILITY Class IRR Profiles
- FIELD Class Profiles
- Miscellaneous Authorities

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 DELETE

Highlights:

- Green - yes

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

System & Group Authorities

- System & Group Authorities
  - SPECIAL — Administer RACF profiles, view non-audit options, & set control options
  - AUDITOR — View RACF profiles, view all options, & set audit options
  - ROAUDIT — (z/OS 2.2) View RACF profiles & view all options - System level only
  - OPERATIONS — Access resources, create group datasets & define group dataset profiles

- 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

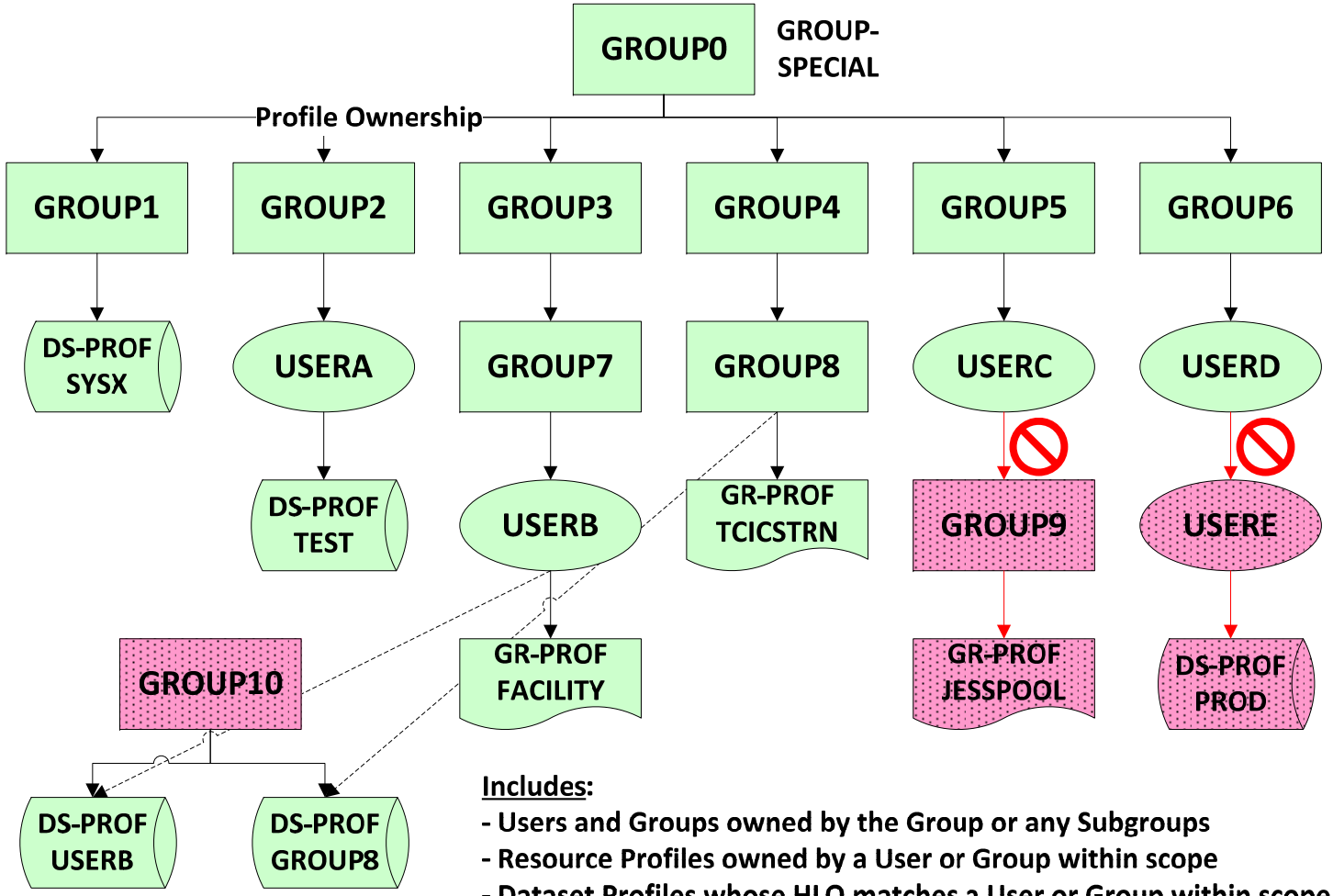
```
USER=RJONES    NAME=RODGER JONES         OWNER=USRGRP1    CREATED=09.012
…
 GROUP=DASDMGT    AUTH=USE     CONNECT-OWNER=RJONES2  CONNECT-DATE=09.181
  CONNECTS=     00  UACC=NONE        LAST-CONNECT=UNKNOWN
  CONNECT ATTRIBUTES=SPECIAL
```

  Authority limited by Scope-of-Groups - follows profile ownership, not group structure

  User ownership of a group or user profile breaks the scope

  Cannot administer or view profile segments

Scope-of-Groups



Includes:

- Users and Groups owned by the Group or any Subgroups
- Resource Profiles owned by a User or Group within scope
- Dataset Profiles whose HLQ matches a User or Group within scope

Excludes:

- User and Group Profiles owned by a User; and any profiles they in turn own (with the exception of dataset profiles with matching HLQs)

AUDITOR & ROAUDIT - System

SETROPTS	USER	GROUP	DATASET	GENRES	OTHER
LIST	LISTUSER	LISTGRP	LISTDSD	RLIST	DSMON(4)
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 DELETE

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

(2) UAUDIT only

(3) GLOBALAUDIT only

(4) RACF protecting program ICHDSM00 takes precedence; authority is ignored if program is protected

ROAUDIT - Can only do LIST commands

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 DELETE

(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 DELETE

(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 DELETE

(1) Excluding Audit Options
(2) Excluding Profile Segments
(3) Excluding GLOBALAUDIT
(4) Requires CLAUTH(USER)
(5) Excludes System-level attributes
(6) Can only assign authorities also held
(7) Excluding UAUDIT
(8) To change SUPGROUP, authority to group and both new and old SUPGROUP group
(9) Create profiles from group profile members
(10) ADDMEM resources from member profiles
(11) Excludes NOEXPIRE on password change
(12) If specify FROM, must have admin authority to FROM profile

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 DELETE

(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 OPERATIONS(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 DELETE

(1) Excluding segments & GLOBALAUDIT

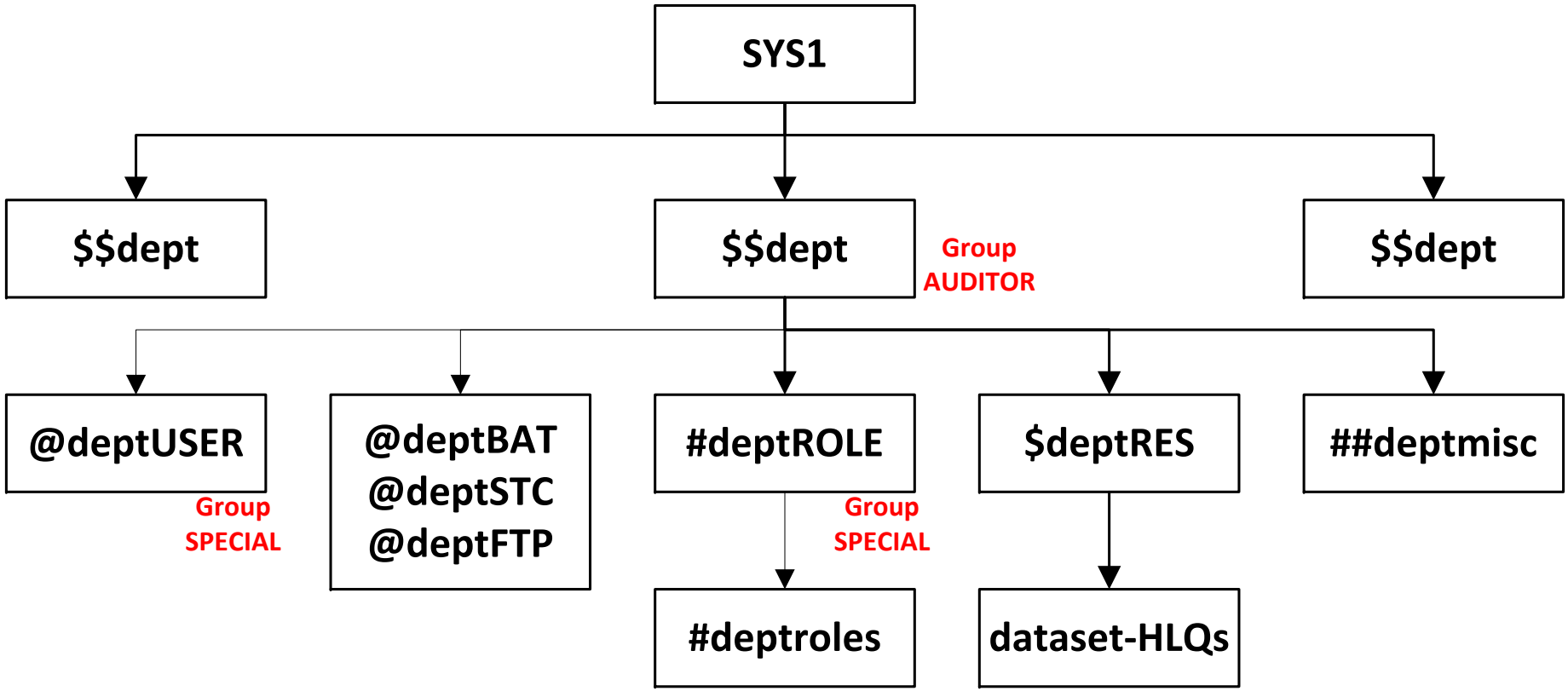
(2) Group datasets only

(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 OPERATIONS(YES)

Group Authority Example



$$ - Department/Organizational Component
@ - User Owner/Default Group
# - RBAC Access Granting Group
$ - Resource Owning Group
- Miscellaneous Group (used for documentation)

Profile Ownership

- Authority depends on type of profile owned (Recommended Owner)
  - User (Default Group)
  - Group (Superior Group)
  - Dataset (HLQ Group or User)
  - General Resource (Designated Owning Group)
- When owned by a Group, Group-SPECIAL allows administration
- 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
- Best Practices
  - Profiles should be owned by groups unless there is a specific reason for a user to own and administer a particular profile
  - TSO users typically own the profiles protecting their own datasets

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(1,2,3)	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 UAUDIT & system-level attributes

(4) Can only assign authorities owner also holds

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 - General 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 to a grouping profile if owner has admin authority over the resources to be added

Group Connect Authorities

- CONNECT AUTHORITY(*authority*)
  - USE — Use access granted to Group
  - CREATE — Create Group dataset profiles; Create Group datasets
  - CONNECT — Connect & Remove users for Group; Assign users same authorities as also held by connecting user
  - JOIN — Create users (with CLAUTH(USER)); Assign users same authorities as also held by joining user; Create Subgroups; Delete Subgroups
- Authorities are cumulative
- Scope-of-Groups does not extend authority

Class Authorization - CLAUTH

- Class Authorization - CLAUTH
  - Allows creation of profiles and grouping members for undefined resources in a specific resource class without System-SPECIAL authority
    - Cannot create a Discrete profile or member matching a Generic without authority over the latter
  - User profile attribute - ALTUSER *userid* CLAUTH(*class*)
    - CLAUTH authority extends to all classes with the same POSIT value even though the other classes may not appear in the LISTUSER display (POSIT values are assigned in the CDT)
    - Can be used for all classes except GROUP and DATASET
  - Does not allow creation of segments (this requires FIELD access)
- CLAUTH(USER) - to create a USER profile requires authority to default group
  - Group-SPECIAL
  - Group JOIN authority
  - Group profile owner
- Once a profile has been created, the creator's ability to administer the profile thereafter is determined by normal administrative authorities (e.g., profile ownership or Group-SPECIAL)
- Best Practice - Only assign CLAUTH to users who are responsible for resources in the related class when these users are better able manage the profiles than the RACF administration staff

Class Authorization - CLAUTH

- General Resource Profiles - CLAUTH(*class*)
  - Can execute SETROPTS REFRESH GENERIC() GLOBAL() RACLIST() and WHEN(PROGRAM) for assigned CLAUTH classes
  - With CLAUTH(GLOBAL) and Group-SPECIAL, can ADDMEM entries to the Global Access Table for group and user dataset HLQs within scope-of-groups
  - If a resource is already defined as a discrete profile or grouping class member, can define it as a discrete profile or member in another grouping profile if CLAUTH user has ALTER access, Group-SPECIAL, or ownership for the existing profile
  - CLAUTH for RACFVARS, NODES, or PROGRAM can ADDMEM members to profiles
- GENERICOWNER SETROPTS Option
  - Owner of a General Resource generic profile (e.g., A*) retains control over resources protected by the profile
  - Restricts ability of other users with CLAUTH to create undercutting member class profiles (e.g., cannot create AB* undercutting A*), but not grouping class members
  - Only the profile owner or users who have Group-SPECIAL where the profile is within their Scope-of-Groups can create undercutting profiles
  - Does not apply to PROGRAM class

FACILITY Class IRR Profiles

- List user profiles - LISTUSER
  - General Resource
    - Class - FACILITY
    - Profiles
      - IRR.LISTUSER - All users
      - IRR.LU.OWNER.*owner* - Users owned by user or group
      - IRR.LU.TREE.*group* - Users owned by groups in scope
      - IRR.LU.EXCLUDE.*userid* - Excludes users in OWNER or TREE - Blocks LISTUSER
    - Access Level - READ - list user profile
    - To list an ID protected by an EXCLUDE profile, user must be permitted READ access to the EXCLUDE profile (overrides the block)
  - Cannot list users with System-level SPECIAL, OPERATIONS, AUDITOR, or ROAUDIT
  - Can only list base profile, not segments
  - Violations are not logged; successes may be logged based on profile and user audit options
  - Best Practice - Limit access to those individuals with a need to list profiles of other users (e.g., Help Desk, Departmental User Administrators, Tech Support)

FACILITY Class IRR Profiles

- Reset user passwords - ALTUSER
  - General Resource
    - Class - FACILITY
    - Profiles
      - IRR.PASSWORD.RESET - All users
      - IRR.PWRESET.OWNER.*owner* - Users owned by user or group
      - IRR.PWRESET.TREE.*group* - Users owned by groups in scope
      - IRR.PWRESET.EXCLUDE.*userid* - Excludes users in OWNER or TREE - Blocks reset
    - Access Levels
      - READ - Resume user, reset password/phase to expired value (but not NOREVOKE)
      - UPDATE - Resume user, reset password/phase to non-expired value
      - CONTROL - Change password prior to MINCHANGE interval
    - To perform a resume/reset on an ID protected by an EXCLUDE profile, user must be permitted access to the EXCLUDE profile at the same level (e.g., UPDATE to use NOEXPIRE)
  - Cannot reset passwords for users with System-level SPECIAL, OPERATIONS, AUDITOR, or ROAUDIT, or PROTECTED
  - Best Practice - Limit access to those individuals and processes with a need to reset passwords for other users (e.g., Help Desk, Departmental User Administrators, automated password reset functions)

FACILITY Class IRR Profiles

- EXCLUDE
  - A generic profile such as IRR.** may inadvertantly result in USERIDs being covered by EXCLUDE and thereby block administrative access

    IRR.LU.EXCLUDE.*userid*

    IRR.PWRESET.EXCLUDE.*userid*
  - To avoid this problem, create generic profiles to cover all EXCLUDEs with a UACC sufficient to permit administration if other IRR.LU and .PWRESET profiles allow it

    RDEFINE FACILITY IRR.LU.EXCLUDE.** UACC(READ)

    RDEFINE FACILITY IRR.PWRESET.EXCLUDE.** UACC(CONTROL)
  - Define more specific EXCLUDE profiles just for USERIDs intended to be excluded

    RDEFINE FACILITY IRR.LU.EXCLUDE.PAYFTPID UACC(NONE)

- To prevent unintended delegation via profiles like IRR.**, define the following

  RDEFINE FACILITY IRR.LISTUSER UACC(NONE)

  RDEFINE FACILITY IRR.LU.** UACC(NONE)

  RDEFINE FACILITY IRR.PASSWORD.RESET UACC(NONE)

  RDEFINE FACILITY IRR.PWRESET.** UACC(NONE)

Blocking RESUME

- Situation: A REVOKED USERID is within the scope of a non-SPECIAL administrator , and you do not want the latter to RESUME the ID
- Block RESUMEs by users with Group-SPECIAL access
  - Change user profile owner to a user or group not within scope (e.g. DEADGRP)
- Block RESUMEs by users permitted FACILITY IRR.PASSWORD.RESET
  - REVOKE ID's Default Group Connect (e.g., CONNECT REVOKE) to inhibit logon
  - Make ID PROTECTED
  - Set REVOKE(*today's-date*) on the ID
- Block RESUMEs by users permitted FACILITY IRR.PWRESET.OWNER.*owner* or IRR.PWRESET.TREE.*group*
  - Change user profile owner to a user or group not within scope
  - REVOKE ID's Default Group Connect (e.g., CONNECT REVOKE) to inhibit logon
  - Make ID PROTECTED
  - Set REVOKE(*today's-date*) on the ID
  - Exclude user with FACILITY profile IRR.PWRESET.EXCLUDE.*userid*

FIELD Class Profiles

- Delegate maintenance of profile segments (e.g., TSO, OMVS, STDATA)
- General Resource
  - Class - FIELD
  - Profile - *profile-type.segment.field* (e.g., USER.TSO.ACCTNUM)
  - Access Levels
    - READ - examine
    - UPDATE - change
- Applies to <u>all</u> 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)
- UPDATE to resource <u>*profile-type.segment.*</u> (includes ending period) is required to create an empty segment or delete a segment

FIELD Class Profiles

```
RLIST FIELD USER.OMVS.UID AUTH
CLASS      NAME
-----      ----
FIELD      USER.OMVS.UID

LEVEL   OWNER      UNIVERSAL ACCESS   YOUR ACCESS  WARNING
-----   --------   ----------------   ---- ------  -------
 00     OS$RES          NONE               READ     NO

INSTALLATION DATA
-------------------------------------------------
UNIX USER IDENTIFIER FIELD

USER      ACCESS    ACCESS COUNT
----      ------    ------ -----
UNIXSPT   UPDATE
&RACUID    READ
INTAUDIT   READ
```

- Best Practices
  - Limit UPDATE access to those individuals responsible for management of the segment's related product (e.g., TSO) when these users are better able manage the segment than the RACF administration staff
  - Avoid generics in the first two qualifiers except to permit READ access
  - Implement UNIXPRIV SHARED.IDS if granting UPDATE to USER.OMVS.UID

FIELD Class Resources - Examples

USER.WORKATTR.		USER.TSO.	
USER.WORKATTR.WANAME	WANAME	USER.TSO.TACCNT	ACCTNUM
USER.WORKATTR.WABLDG	WABLDG	USER.TSO.TCOMMAND	COMMAND
USER.WORKATTR.WADEPT	WADEPT	USER.TSO.TDEST	DEST
USER.WORKATTR.WAROOM	WAROOM	USER.TSO.THCLASS	HOLDCLASS
USER.WORKATTR.WAADDR1	WAADDR1	USER.TSO.TJCLASS	JOBCLASS
USER.WORKATTR.WAADDR2	WAADDR2	USER.TSO.TLPROC	PROC
USER.WORKATTR.WAADDR3	WAADDR3	USER.TSO.TLSIZE	SIZE
USER.WORKATTR.WAADDR4	WAADDR4	USER.TSO.TMCLASS	MSGCLASS
USER.WORKATTR.WAACCNT	WAACCNT	USER.TSO.TMSIZE	MAXSIZE
		USER.TSO.TSCLASS	SYS
DATASET.DFP.		USER.TSO.TSOSLABL	SECLABEL
DATASET.DFP.RESOWNER	RESOWNER	USER.TSO.TUDATA	USERDATA
		USER.TSO.TUNIT	UNIT
STARTED.STDATA.			
STARTED.STDATA.FLAGPRIV	PRIVILEGED	GROUP.CSDATA.	
STARTED.STDATA.FLAGTRAC	TRACE	GROUP.CSDATA.*custom-field*	Custom field name
STARTED.STDATA.FLAGTRUS	TRUSTED		
STARTED.STDATA.STGROUP	GROUP	GROUP.OMVS.	
STARTED.STDATA.STUSER	USER	GROUP.OMVS.GID	GID

Access Enabled Authority

- READ or Greater - LISTDSD or RLIST
  - List base RACF segment information
    - Does not include access list or GLOBALAUDIT settings
    - Prohibited if user is connected to any Group in the access list with access of NONE
- ALTER in Discrete profile
  - List, change, and delete the profile
  - List access list and grant or remove access permissions
  - If permitted ALTER to a RACFVARS or NODES profile, can ADDMEM entries to it
  - Can add an entry for a general resource profile in the GLOBAL class profile
- Above applies to access permitted via USERID, Group, ID(*), or UACC

User Authority for Own ID and Datasets

- List own User profile, but not segments
- Change own User profile ...
  - Name
  - Default Group (if connected to the target group)
  - Model Dataset (if active)
  - Password (if within SETROPTS MINCHANGE interval)
  - Password-interval (to a number equal to or less than SETROPTS INTERVAL)
- Execute IRRUT100 Cross-Reference Utility on own ID
- Create, change, and delete dataset profiles where HLQ matches the user's ID, even if not the profile owner
- Create, change, and delete datasets where HLQ matches the user's ID, even if not permitted access

Miscellaneous Authorities

- When a resource profile is created, the UACC, if not specified, defaults to the value specified by DEFAULTUACC in the class' CDT entry
  - DEFAULTUACC(ALTER | CONTROL | UPDATE | READ | NONE | ACEE)
  - If set to ACEE, the UACC is taken from the UACC in the user's current connect group
  - Best Practice - Always set CONNECT UACC to NONE

```
USER=RSHT11  NAME=RSH TEST ID Z1.11     OWNER=TESTGRP   CREATED=11.262
...
  GROUP=TESTGRP   AUTH=USE       CONNECT-OWNER=TESTGRP   CONNECT-DATE=11.262
   CONNECTS=     10  UACC=NONE     LAST-CONNECT=15.120/19:50:35
```

- All users can execute RVARY command

- 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

```
SETR LIST
…
ADDCREATOR IS NOT IN EFFECT
```

Miscellaneous Authorities - GRPACC

- 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
  - Recommend GRPACC be avoided to prevent unintended access