What's Cool About the **CONNECT Command** in RACF

Stu Henderson
5702 Newington Road
Bethesda, MD 20816

stu@stuhenderson.com
www.stuhenderson.com
(301) 229-7187

AGENDA

1. We all know the
   CONNECT command

2. What is in **CONNECT INFO?**

3. Why use **CONNECT INFO?**

4. Summary and Call to Action

We all know the CONNECT command

The **CONNECT** command

CO USER02 GROUP(GROUPA)

is used to connect a
User to a *Group*

We all know the CONNECT command

The **REMOVE** command
(opposite of CONNECT)

RE USER02 GROUP(GROUPA)

is used to remove a
User from a *Group*

What is in CONNECT INFO?

❑ User profile has groups the user belongs to

❑ Group profile has users in the group

USER02 Profile
• …
• Member of: …

GROUPA Profile
• …
• User Members: …

What is in CONNECT INFO?

The CONNECT command puts
the group name in User Profile
and
the user name in Group Profile

CO USER02 GROUP(GROUPA)

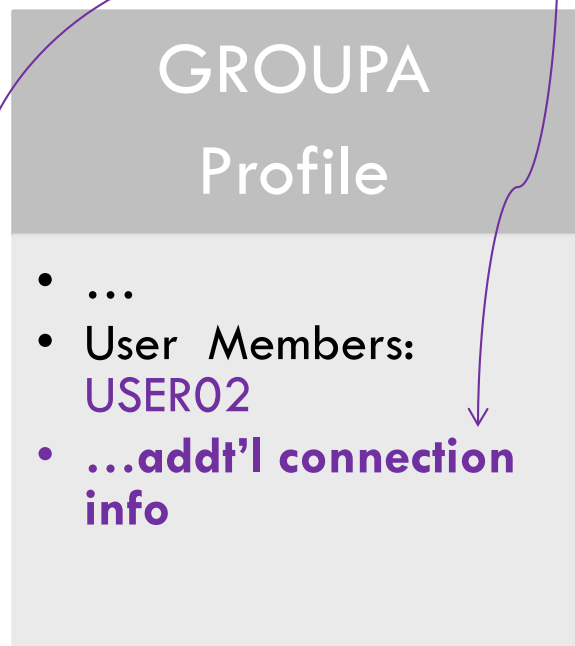| USER02 Profile	GROUPA Profile
• … • Member of: **GROUPA**	• … • User Members: **USER02**

What is in CONNECT INFO?

The CONNECT command may include additional connection information about how the User relates to the Group

CO USER02 GROUP(GROUPA) *…connection info*

USER02 Profile
- …
- Member of: GROUPA
- **…addt'l connection info**

GROUPA Profile
- …
- User Members: USER02
- **…addt'l connection info**

Stuart Henderson (c) 2015   www.stuhenderson.com   301-229-7187

What is in
CONNECT INFO?

✓ UserID and Group Name

✓ UACC

✓ AUTH

✓ Group Attributes, aka Connect Attributes

What is in CONNECT INFO?

UACC in CONNECT INFO

❑ Safely ignored

❑ Let it default to NONE

❑ Stored in ACEE

❑ Used only for certain resource classes when creating a new profile and you forget to specify the UACC (See DSMON Class Descriptor Table under UACC)

What is in CONNECT INFO?

AUTH in CONNECT INFO

❑ **JOIN** (can create new sub-groups under the group, and (with CLAUTH(USER) new userids in the group)

❑ **CONNECT** (can connect / remove others to the group)

❑ **CREATE** (can create dataset rule with groupname as HLQ)

❑ **USE** (just a member)

What is in CONNECT INFO?

Group Attributes in CONNECT INFO

❑ Any of: SPECIAL, OPERATIONS, AUDIT, REVOKE, GRPACC

❑ Gives the privilege in the group

❑ And all the groups it owns

❑ And all the groups they own…

What is in CONNECT INFO?

Group Attributes in CONNECT INFO

❑ So in DSMON, Selected User Attribute Report, you see that USER02 has Group-SPECIAL in GROUPA

❑ You LISTUSER USER02 to see which group(s)

❑ You find those groups in DSMON, Group Tree Report

What is in
CONNECT INFO?

❑ Find all the groups they own by following down the vertical lines in the Group Tree Report

❑ And the groups they own, and so on

What is in CONNECT INFO?

❑ Each group is owned by either a userid or a group. If a group, it must be the superior group, which is connected to it by a vertical line

❑ When a group has a name in parentheses to the right of the group name in the Group Tree Report, that's the name of the userid that owns the group

❑ When a group is owned by a userid, then the trickle-down stops with the group

What is in CONNECT INFO?

Two Phases:

1. List all the groups which the group owns, all the groups they own, on down the tree, as long as a group owns a group owns a group

2. List every profile owned by these groups, plus dataset profiles with these as HLQs

That's the scope of the group attribute

Why use CONNECT INFO?

- ☐ Delegation of Authority

- ☐ Famous Nome-Honolulu Principle

- ☐ AUTH gives authority just within the group

- ☐ Group-SPECIAL gives authority in the group, and all down the tree from there

Why use CONNECT INFO?

□ AUTH is great for RBAC (Role Base Access Control)

□ You permit the group where it needs and use AUTH(CONNECT) to let someone else just connect and remove for the group. He can't mess up your permit lists.

□ To learn AUTHs greater than USE,
//S1   EXEC RACFICE,REPORT=UADS

Stuart Henderson (c) 2015   www.stuhenderson.com   301-229-7187

Group-SPECIAL

- ☐ Is like having your userid be the owner of a profile: it lets you alter or delete it

- ☐ For the Help Desk, better to use FACILITY class rules named IRR.PASSWORD… to delegate the ability to administer passwords and revoke/resume

Summary / Call to Action

☐ Don't let your RACF implementation permit things you don't understand

☐ Map out your delegation of authority: who has AUTH above USE, who has group-attributes, who has CLAUTH, who has SPECIAL

☐ Then you know how to make it secure

☐ If not you, then who?

For More Information

RACF User News (back issues & subscribe)

http://www.stuhenderson.com/Newsletters-Archive.html

Articles on mainframe security and audit

http://www.stuhenderson.com/Articles-Archive.html

Thanks for Your Kind Attention.

Questions to Stu Henderson

(301) 229-7187

stu@stuhenderson.com

http://www.stuhenderson.com/