RACF: z/OS V1R10 Functions Password Reset Granularity

Laurie Ward
Email Address: LWard@us.ibm.com
External Phone: (845) 435-8028

© 2008 IBM Corporation

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Session Objectives

- Things you will learn:
  - Why use Password Reset Granularity?
  - How to use IRR.PWRESET profiles
  - How to use IRR.LU profiles
  - Reference materials

© 2008 IBM Corporation

Overview

- **Problem Statement / Need Addressed:**
  - Current Support is 'all or nothing'
    - ALTUSER: Access to resource IRR.PASSWORD.RESET in the FACILITY class gives you the authority to reset passwords and resume user IDs **for all users**
    - LISTUSER: Access to resource IRR.LISTUSER in the FACILITY class gives you the authority to list information in the base segment of USER profiles **for all users**
  - Limitation: Cannot limit the users over which you have these authorities

© 2008 IBM Corporation

Overview…

- **Solution:**
  - Now you can specify the users over which you have password reset authority
  - ALTUSER: Grant authority to reset passwords and resume user IDs
    - BY OWNER: User IDs owned by a group or user
    - BY TREE: User IDs in the scope of a group tree (User IDs owned by a group and users owned by groups that are owned by that group)
  - LISTUSER: Grant authority to list information in the base segment of USER profiles
    - BY OWNER: User IDs owned by a group or user
    - BY TREE: User IDs in the scope of a group tree (User IDs owned by a group and users owned by groups that are owned by that group)
- **Benefit:**
  - Allows further granularity of IRR.PASSWORD.RESET authorities
  - Allows further granularity of IRR.LISTUSER authorities

© 2008 IBM Corporation

Overview…

- **Customer requirements answered:**
  - MR00042369 - RACF - Group Member with Password and not Dataset Authority
  - MR0128042219 - Provide Granularity in Authority Defined by FACILITY Resource IRR.PASSWORD.RESET
  - MR020402160 - ENHANCE IRR.PASSWORD.RESET TO PROVIDE MORE GRANULARITY.
  - MR0420058019 - RACF/IRR.PASSWORD.RESET Define a Group Which Can Manage Passwords for Other Groups of Users
  - MR0918023413 - ENHANCE IRR.PASSWORD.RESET TO PROVIDE MORE GRANULARITY.
  - MR0129017129 – Data Security Administrator
  - MR0201017335 – Data Security Administrator (Beyond Group Level)

© 2008 IBM Corporation

Usage & Invocation

- Overview of ALTUSER changes
- Overview of LISTUSER changes
- Sample Group/User Structure illustrations
- How to use the ALTUSER support
- How to use the LISTUSER support

© 2008 IBM Corporation

Overview of ALTUSER Changes

- ALTUSER: Grant authority to reset passwords and resume user IDs
  - BY OWNER: User IDs owned by a group or user
    - Access to resource IRR.PWRESET.OWNER.*owner-of-user-profile*
  - BY TREE: User IDs in the scope of a group tree (User IDs owned by a group and users owned by groups that are owned by that group)
    - Access to resource IRR.PWRESET.TREE.*owner-of-tree*
  - Set excluded users with resource IRR.PWRESET.EXCLUDE.*excluded-user*

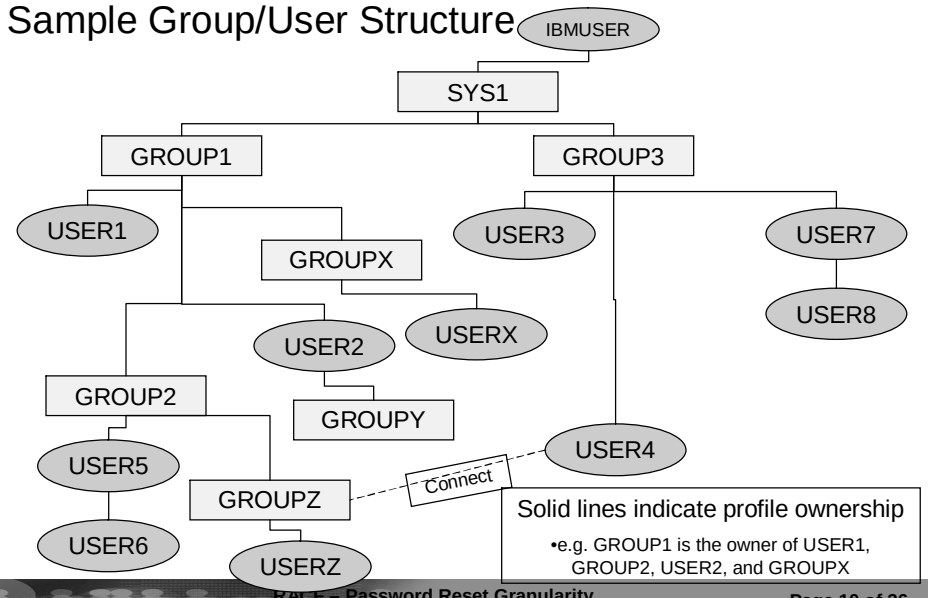
© 2008 IBM Corporation

Overview of LISTUSER Changes

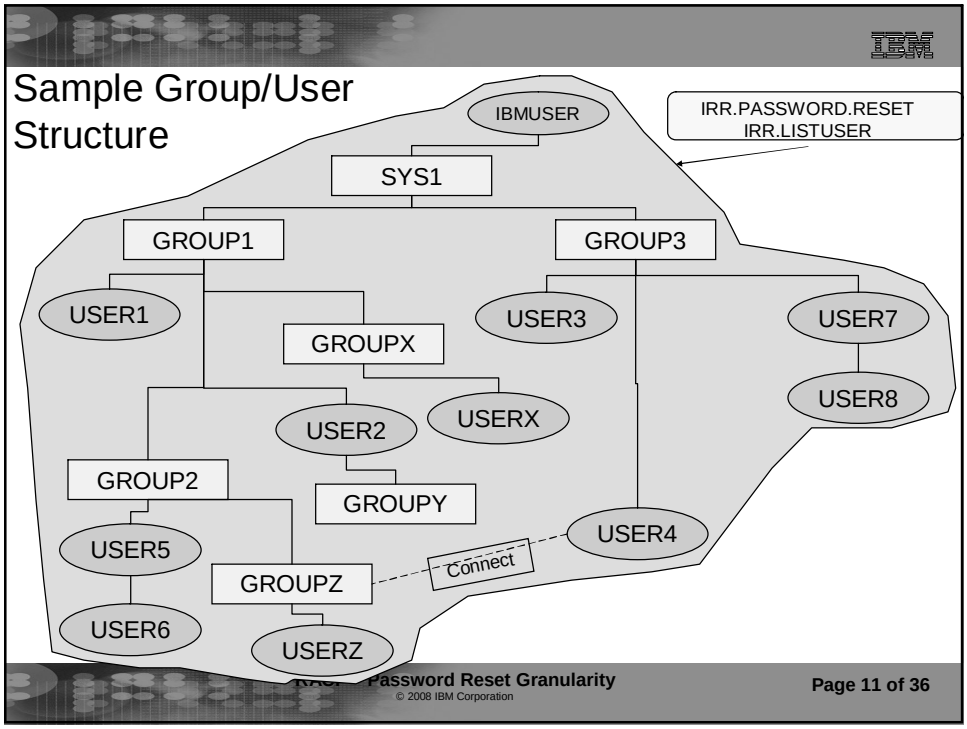
- LISTUSER: Grant authority to list information in the base segment of USER profiles
  - BY OWNER: User IDs owned by a group or user
    - Access to resource IRR.LU.OWNER.*owner-of-user-profile*
  - BY TREE: User IDs in the scope of a group tree (User IDs owned by a group and users owned by groups that are owned by that group)
    - Access to resource IRR.LU.TREE.*owner-of-tree*
  - Set excluded users with resource IRR.LU.EXCLUDE.*excluded-user*

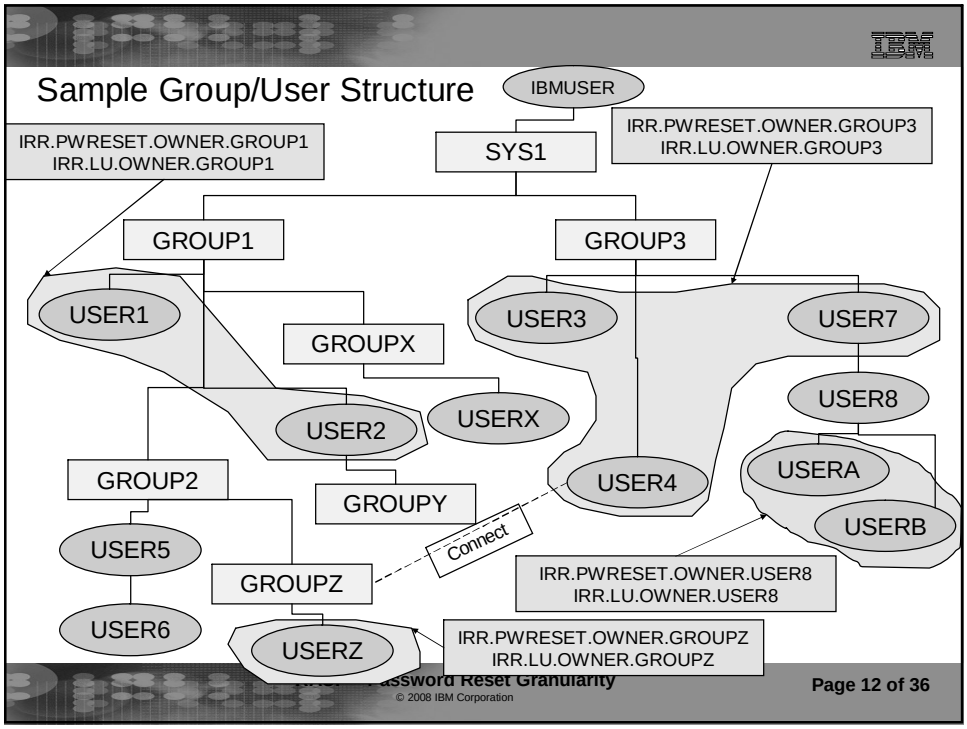
© 2008 IBM Corporation

Sample Group/User Structure

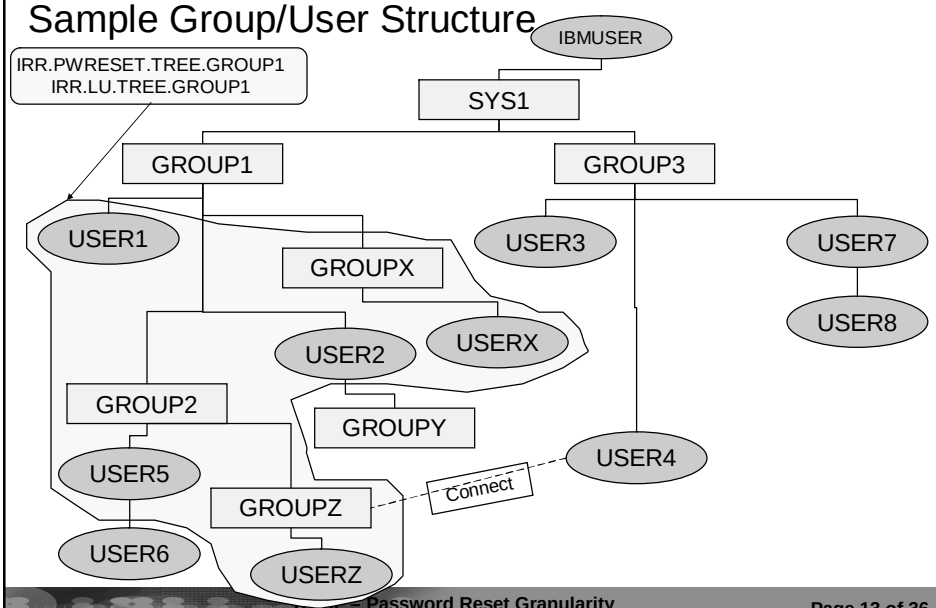


© 2008 IBM Corporation


Sample Group/User Structure
IBMUSER
IRR.PASSWORD.RESET
IRR.LISTUSER
SYS1
GROUP1
GROUP3
USER1
USER3
USER7
GROUPX
USER8
USERX
USER2
GROUP2
GROUPY
USER4
USER5
Connect
GROUPZ
USER6
USERZ
Password Reset Granularity
© 2008 IBM Corporation
Page 11 of 36

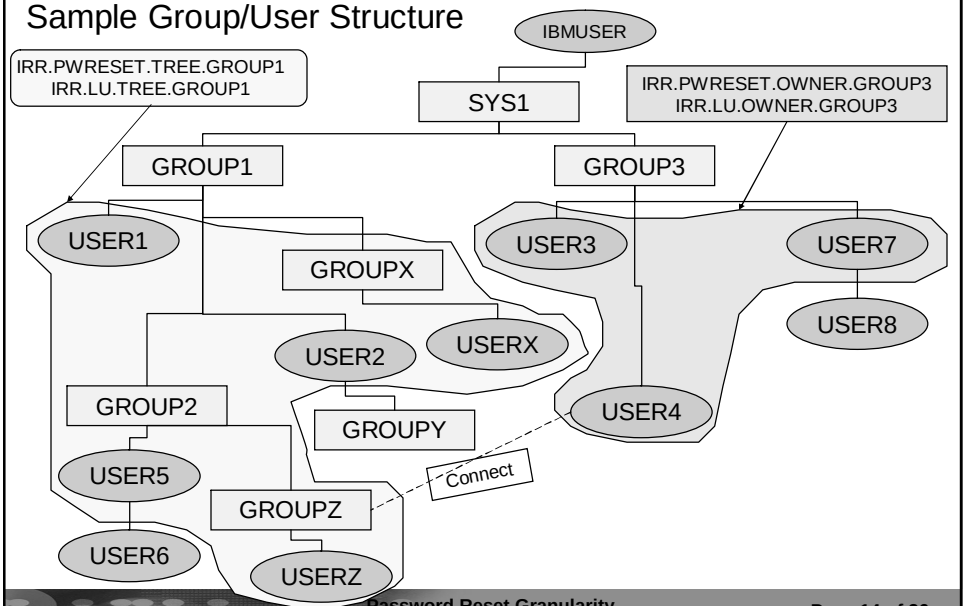

Sample Group/User Structure
IBMUSER
IRR.PWRESET.OWNER.GROUP1
IRR.LU.OWNER.GROUP1
SYS1
IRR.PWRESET.OWNER.GROUP3
IRR.LU.OWNER.GROUP3
GROUP1
GROUP3
USER1
USER3
USER7
GROUPX
USER8
USERX
USER2
GROUP2
USERA
USER4
GROUPY
USERB
USER5
Connect
GROUPZ
IRR.PWRESET.OWNER.USER8
IRR.LU.OWNER.USER8
USER6
USERZ
IRR.PWRESET.OWNER.GROUPZ
IRR.LU.OWNER.GROUPZ
Password Reset Granularity
© 2008 IBM Corporation
Page 12 of 36

Sample Group/User Structure



© 2008 IBM Corporation

Sample Group/User Structure



© 2008 IBM Corporation

Before you Start

- Create some profiles before you start to prevent interaction from other FACILITY class profiles:
  - –RDEFINE FACILITY IRR.PWRESET.** UACC(NONE)
  - –RDEFINE FACILITY IRR.PWRESET.EXCLUDE.** UACC(READ)
  - –RDEFINE FACILITY IRR.LU.** UACC(NONE)
  - –RDEFINE FACILITY IRR.LU.EXCLUDE.** UACC(READ)
- Some users are always excluded from this support
  - –System SPECIAL, OPERATIONS, AUDITOR users are automatically excluded
    - Authority to reset a password for a SPECIAL, OPERATIONS, AUDITOR, or **PROTECTED** user follows normal ALTUSER authority rules only (no IRR.PASSWORD.RESET, no IRR.PWRESET)
    - Authority to list a USER profile for a SPECIAL, OPERATIONS, or AUDITOR user follows normal LISTUSER authority rules only (no IRR.LISTUSER, no IRR.LU)

© 2008 IBM Corporation

ALTUSER – Allow by Owner

- Step 1 - Define which users have the authority to reset passwords and resume user IDs for user IDs owned by a user or group
  - –Resource IRR.PWRESET.OWNER.*owner-of-user-profile* in FACILITY class
    - •*Owner-of-user-profile* can be a user ID or a group name
    - •Auditing is performed based on auditing options set in the profile
      - –Suggested profile audit settings: FAILURES(NONE) SUCCESSES(READ)
      - –No ICH408I messages will be issued
      - –LOGOPTIONS in FACILITY class will not be honored
    - •Failed attempts are logged as ALTUSER command violations
  - –READ, UPDATE, CONTROL access to this resource is similar to access to IRR.PASSWORD.RESET – access determines type of password reset/resume which can be performed (details later)
  - –List of groups has no effect on this function (SETROPTS GRPLIST)
    - •See “allow by tree” option

© 2008 IBM Corporation

ALTUSER – Allow by Owner…

- Step 2 (Optional) – Create a profile for each "excluded" user who should not be subject to a password reset (for example, a group-special user)
  - –Format of the FACILITY resource to exclude a user from being subject to a password reset
    - •IRR.PWRESET.EXCLUDE.*excluded-user*
    - •*excluded-user* is the user ID whose password is being reset
    - •If command issuer has NO authority to resource, then user is excluded and authority fails
    - •NOTE: This same resource applies to password reset authority by owner and by tree
  - – Define the profile to exclude the user
    - •RDEFINE FACILITY IRR.PWRESET.EXCLUDE.*excluded-user* UACC(NONE)
    - •Using UACC(NONE) will prevent everyone from resetting password of *excluded-user*
- Step 3 – If you have FACILITY class RACLISTed
  - •SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

ALTUSER – Allow by Owner…

- Example
  - –Allow user ANDREW to reset passwords and resume user IDs for users that are owned by TEAMLDR
    - •RDEFINE FACILITY IRR.PWRESET.OWNER.TEAMLDR UACC(NONE)
    - •PERMIT IRR.PWRESET.OWNER.TEAMLDR CLASS(FACILITY) ACCESS(READ) ID(ANDREW)
  - –Allow users connected to group HLPDESK8 to reset passwords and resume user IDs for users that are owned by group AREA8. Do not allow the password of Help Desk Admin ID called HELPADM to be reset.
    - •RDEFINE FACILITY IRR.PWRESET.OWNER.AREA8 UACC(NONE)
    - •PERMIT IRR.PWRESET.OWNER.AREA8 CLASS(FACILITY) ACCESS(READ) ID(HLPDESK8)
    - •RDEFINE FACILITY IRR.PWRESET.EXCLUDE.HELPADM UACC(NONE)
  - –If you have FACILITY class RACLISTed:
    - • SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

ALTUSER – Allow by Tree

- Step 1 - Define which users have the authority to reset passwords and resume user IDs for user IDs in the scope of a group
  - –Resource IRR.PWRESET.TREE.*owner-of-tree* in FACILITY class
    - •*Owner-of-tree* should be the group name at the 'top' of a group tree
    - •Auditing is performed based on auditing options set in the profile
      - –Suggested profile audit settings: FAILURES(NONE) SUCCESSES(READ)
      - –No ICH408I messages will be issued
      - –LOGOPTIONS in FACILITY class will not be honored
    - •Failed attempts are logged as ALTUSER command violations
  - –READ, UPDATE, CONTROL access to this resource is similar to access to IRR.PASSWORD.RESET – access determines type of password reset/resume which can be performed (details later)
  - –List of groups must be in effect for this function for work properly (SETROPTS GRPLIST)

© 2008 IBM Corporation

ALTUSER – Allow by Tree…

- Step 2 (Optional) – Create a profile for each "excluded" user who should not be subject to a password reset (for example, a group-special user)
  - –Format of the FACILITY resource to exclude a user from being subject to a password reset
    - •IRR.PWRESET.EXCLUDE.*excluded-user*
    - •*excluded-user* is the user ID whose password is being reset
    - •If command issuer has NO authority to resource, then user is excluded and authority fails
    - •NOTE: This same resource applies to password reset authority by owner and by tree
  - – Define the profile to exclude the user
    - •RDEFINE FACILITY IRR.PWRESET.EXCLUDE.*excluded-user* UACC(NONE)
    - •Using UACC(NONE) will prevent everyone from resetting password of *excluded-user*
- Step 3 – If you have FACILITY class RACLISTed, update FACILITY class profiles in storage
  - –SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

ALTUSER – Allow by Tree…

- Example
  - –Allow user USERH to reset passwords and resume user IDs for users that are in the scope of group GROUP1
    - •RDEFINE FACILITY IRR.PWRESET.TREE.GROUP1 UACC(NONE)
    - •PERMIT IRR.PWRESET.TREE.GROUP1 CLASS(FACILITY) ACCESS(READ) ID(USERH)
  - –Allow users connected to group HLPDESK8 to reset passwords and resume user IDs for users that are owned by group GROUP1. Do not allow the password of group-special user USER1 to be reset.
    - •RDEFINE FACILITY IRR.PWRESET.TREE.GROUP1 UACC(NONE)
    - •PERMIT IRR.PWRESET.TREE.GROUP1 CLASS(FACILITY) ACCESS(READ) ID(HLPDESK8)
    - •RDEFINE FACILITY IRR.PWRESET.EXCLUDE.USER1 UACC(NONE)
  - –If you have the FACILITY class RACLISTed:
    - •SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

Summary of Access Level Authorities

- RACF access level the user has for each IRR.PWRESET.xx.xx resource determines the specific ALTUSER operations the user can perform.
  - – Same as existing RACF access level meanings for IRR.PASSWORD.RESET

Resource authority to IRR.PWRESET.xx.xx	What it allows you to do	Restrictions
READ	•Use the PASSWORD operand. •Use the RESUME operand, without specifying a date	• User being altered does not have the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute. • User is not excluded with a IRR.PWRESET.EXCLUDE profile
UPDATE	•All authorities of READ access. •Use the NOEXPIRED operand (in conjunction with the PASSWORD operand).	
CONTROL	•All authorities of UPDATE access. •Reset a user's password within the minimum password interval for that user.	

© 2008 IBM Corporation

LISTUSER – Allow by Owner

- Step 1 - Define which users have the authority to LIST user profiles owned by a user or group
  - –Resource IRR.LU.OWNER.*owner-of-user-profile* in FACILITY class
    - •*Owner-of-user-profile* can be a user ID or a group name
    - •Auditing is performed based on auditing options set in the profile
      - –Suggested profile audit settings: FAILURES(NONE) SUCCESSES(READ)
      - –No ICH408I messages will be issued
      - –LOGOPTIONS in FACILITY class will not be honored
    - •Failed attempts are not logged
  - –READ access to this resource is sufficient
  - –List of groups has no effect on this function (SETROPTS GRPLIST)
    - •See “allow by tree” option

© 2008 IBM Corporation

LISTUSER – Allow by Owner…

- Step 2 (Optional) – Create a profile for each “excluded” user who should not be subject of a LISTUSER command (for example, a group-special user)
  - –Format of the FACILITY resource to exclude a user from being subject to a password reset
    - •IRR.LU.EXCLUDE.*excluded-user*
    - •*excluded-user* is the user ID whose USER profile is being listed
    - •If command issuer has NO authority to resource, then user is excluded and authority fails
    - •NOTE: This same resource applies to LISTUSER authority by owner and by tree
  - – Define the profile to exclude the user
    - •RDEFINE FACILITY IRR.LU.EXCLUDE.*excluded-user* UACC(NONE)
    - •Using UACC(NONE) will prevent everyone from listing the USER profile of *excluded-user*
- Step 3 – If you have FACILITY class RACLISTed, update FACILITY class profiles in storage
  - –SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

LISTUSER – Allow by Owner…

- Example
  - –Allow user ANDREW to list USER profiles that are owned by TEAMLDR
    - •RDEFINE FACILITY IRR.LU.OWNER.TEAMLDR UACC(NONE)
    - •PERMIT IRR.LU.OWNER.TEAMLDR CLASS(FACILITY) ACCESS(READ) ID(ANDREW)
  - –Allow users connected to group HLPDESK8 to list USER profiles that are owned by group AREA8. Do not allow the listing of Help Desk Admin ID called HELPADM.
    - •RDEFINE FACILITY IRR.LU.OWNER.AREA8 UACC(NONE)
    - •PERMIT IRR.LU.OWNER.AREA8 CLASS(FACILITY) ACCESS(READ) ID(HLPDESK8)
    - •RDEFINE FACILITY IRR.LU.EXCLUDE.HELPADM UACC(NONE)
  - –If you have FACILITY class RACLISTed:
    - • SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

LISTUSER – Allow by Tree

- Step 1 - Define which users have the authority to list USER profiles in the scope of a group
  - –Resource IRR.LU.TREE.*owner-of-tree* in FACILITY class
    - •*Owner-of-tree* should be the group name at the 'top' of a group tree
    - •Auditing is performed based on auditing options set in the profile
      - –Suggested profile audit settings: FAILURES(NONE) SUCCESSES(READ)
      - –No ICH408I messages will be issued
      - –LOGOPTIONS in FACILITY class will not be honored
    - •Failed attempts are not logged for LISTUSER
  - –READ access to this resource is sufficient
  - –List of groups must be in effect for this function for work properly (SETROPTS GRPLIST)

© 2008 IBM Corporation

LISTUSER – Allow by Tree…

- Step 2 (Optional) – Create a profile for each "excluded" user who should not have their USER profile listed (for example, a group-special user)
  - –Format of the FACILITY resource to exclude a user from being subject to LISTUSER
    - •IRR.LU.EXCLUDE.*excluded-user*
    - •*excluded-user* is the user ID whose USER profile is being listed
    - •If command issuer has NO authority to resource, then user is excluded and authority fails
    - •NOTE: This same resource applies to LISTUSER authority by owner and by tree
  - – Define the profile to exclude the user
    - •RDEFINE FACILITY IRR.LU.EXCLUDE.*excluded-user* UACC(NONE)
    - •Using UACC(NONE) will prevent everyone from listing the USER profile of *excluded-user*
- Step 3 – If you have FACILITY class RACLISTed, update FACILITY class profiles in storage
  - –SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

LISTUSER – Allow by Tree…

- Example
  - –Allow user USERH to list USER profiles that are in the scope of group GROUP1
    - •RDEFINE FACILITY IRR.LU.TREE.GROUP1 UACC(NONE)
    - •PERMIT IRR.LU.TREE.GROUP1 CLASS(FACILITY) ACCESS(READ) ID(USERH)
  - –Allow users connected to group HLPDESK8 to list USER profiles that are owned by group GROUP1. Do not allow the USER profile of group-special user USER1 to be listed.
    - •RDEFINE FACILITY IRR.LU.TREE.GROUP1 UACC(NONE)
    - •PERMIT IRR.LU.TREE.GROUP1 CLASS(FACILITY) ACCESS(READ) ID(HLPDESK8)
    - •RDEFINE FACILITY IRR.LU.EXCLUDE.USER1 UACC(NONE)
  - –If you have the FACILITY class RACLISTed:
    - •SETROPTS RACLIST(FACILITY) REFRESH

© 2008 IBM Corporation

Session Summary

- Using Password Reset Granularity, the customer can:
  Limit the users for which a local administrator (or help desk personnel) :
  - Can reset passwords for
    - IRR.PWRESET profiles
  - Can list the USER profiles for
    - IRR.LU profiles
- Any Questions?

© 2008 IBM Corporation

Appendix

- Publications

ƒ SA22-7683 *Security Server RACF Security Administrator's Guide*
  ƒ Chapter on "Authorizing help desk functions"

ƒ SA22-7687 *Security Server RACF Command Language Reference*
  ƒ ALTUSER, LISTUSER, SETROPTS commands – mention authorities related to the IRR.PWRESET and IRR.LU profiles

z/OS V1R10 Publications available online:
http://www-03.ibm.com/systems/z/os/zos/bkserv/r10pdf/

© 2008 IBM Corporation

Password Reset Authority Scoped by Owner/Tree

- Allow the password reset function for a set of users based on desired criteria
  - –Can also exclude specific users
    - •Users with SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute are automatically excluded

Limit users by	**FACILITY Resource**	**Access level of command issuer**	**Privilege allowed**
Owner of user profile	IRR.PWRESET.OWNER *.owner-of-profile*	READ, UPDATE, or CONTROL	Can reset passwords for all users owned by *owner-of-profile*
Tree Owner of user profile	IRR.PWRESET.TREE *.owner-of-tree*	READ, UPDATE, or CONTROL	Can reset passwords for all users owned by *owner-of-tree* and users owned by groups that are owned by *owner-of-tree*

- Can use combination of these criteria within an installation

© 2008 IBM Corporation

Summary of Profiles for Password Reset Authority Scoped by Owner/Tree

- Allow the password reset function for a group of users based on desired criteria
  - –Users with SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute are automatically excluded

Limit users by	**FACILITY Resource**	**Access level of command issuer**	**Resource to exclude users from being subject to a password reset**
Owner of user profile	IRR.PWRESET. OWNER *.owner-of-profile*	READ, UPDATE, or CONTROL	IRR.PWRESET.EXCLUDE.*excluded-user* With NO access to command issuer
Tree Owner of user profile	IRR.PWRESET. TREE *.owner-of-tree*	READ, UPDATE, or CONTROL	IRR.PWRESET.EXCLUDE.*excluded-user* With NO access to command issuer

- Can use combination of these criteria within an installation

© 2008 IBM Corporation

LISTUSER Authority Scoped by Owner/Tree

- Allow a user to list information in the base segment of the USER profiles for a set of users based on desired criteria

Limit users by	FACILITY Resource	Access level of command issuer	Privilege allowed
Owner of user profile	IRR.LU.OWNER *.owner-of-profile*	READ	Can list information in the base segment of the USER profiles for all users owned by *owner-of-profile*
Tree Owner of user profile	IRR.LU.TREE. *.owner-of-tree*	READ	Can list information in the base segment of the USER profiles for all users owned by *owner-of-tree* and users owned by groups that are owned by *owner-of-tree*

- Can use combination of these criteria within an installation

© 2008 IBM Corporation

Summary of Profiles for LISTUSER Authority Scoped by Owner/Tree

- Allow a user to list information in the base segment of the USER profiles for a group of users based on desired criteria
  - –Users with SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute are automatically excluded

Limit users by	FACILITY Resource	Access level of command issuer	Resource to exclude users from having their USER profile listed
Owner of user profile	IRR.LU.OWNER *.owner-of-profile*	READ	IRR.LU.EXCLUDE.*excluded-user* With NO access to command issuer
Tree Owner of user profile	IRR.LU.TREE *.owner-of-tree*	READ	IRR.LU.EXCLUDE.*excluded-user* With NO access to command issuer

- Can use combination of these criteria within an installation

© 2008 IBM Corporation