安全管理实验
实验指导书

同济大学 高珍 编写

实验 1.3 分散式 RACF 安全管理实验

实验目的： 实现 RACF 中的管理权限下放(Delegation)

实验设备： IBM 大型主机 z900

实验结果： 实验后，学生应该掌握

- 不同安全管理员（Group Special 用户、Connect 用户、Create 用户等）的权限差异

实验介绍： 该实验将新建管理员用户，包括负责组安全管理的管理员，仅负责将用户连接到功能组的管理元，控制对组数据集资源访问的管理员

实验要求： 完成实验报告

步骤 1 确定前面实验中所建立的 USERxx 用户的 OWNER 是 DIVxx，以下是其中几个用户身份的定位：

- 身份 1: USERxx(Janet Smith)：该管理员仅可以将其他用户关联到 DIVxx 组中，以帮助新用户通过组来继承权限。
- 身份 1: USERxx(Janet Smith)：该管理员可以为 DIVxx 组数据集创建数据集 PROFILE，以控制用户对 DIVxx 组数据集的访问。
- 身份 2: USERxx(Janet Smith)：该管理员是组管理员，将对 DIVxx 组的资源进行全方位的安全管理。

(1) 请依次以不同身份完成如下实验，通过 CONNECT 命令给 USERxx 赋予身份。

HINT ： CONNECT

(2) 使用‘LU’RACF 命令或者 RACF 控制面板查看 USERxx 的属性，请回答以下问题

► 该用户关联到哪些组?

► 该用户有哪些用户特权?

► 该用户是否有类权限（class authorization）?

► 该用户关联到组 DIVxx 上时是否有什么特权（connect attributes）?

步骤 2 测试步骤 1 的功能是否实现

(1) 以 USERxx 身份登陆 TSO，尝试修改用户密码等

HINT ： ALU

(2) 以 USERxx 身份登陆 TSO，将 ST0xx 用户关联到 DIVxx 组下

```
CONNECT ST0xx GROUP(DIVxx)
```

(3) 以 USERxx 身份登陆 TSO，将 ST0xx 从 DIVxx 组中移走

HINT ： REMOVE

```
REMOVE ST0xx GROUP(DIVxx)
```

(4) 以 USERxx 身份登陆 TSO，对 DIVxx 组文件进行保护：通用权限使用 NONE，授权 DIVxx 组对 DIVxx.**数据集有 ALTER 的权限。

HINT：命令 1：ADDSD … ；命令 2：PE…

(5) 分别以 USERxx 和 ST0xx 身份登陆 TSO，对 DIVxx 的组数据集保护进行验证。
USERxx 新建数据集 DIVxx.DATA 并编辑内容，是否成功？_____
如果失败了，思考如何为 USERxx 进行正确赋权？_____
ST0xx 新建数据集 DIVxx.DATA 并编辑内容，是否成功？_____
如果失败了，思考如何为 ST0xx 进行正确赋权？_____

步骤 3 请使用 RACF 命令 LU 查看用户 USERxx，将查看到的内容截屏，然后将截屏图像作为实验报告内容 1 提交；体会上述实验，总结 group special、connect、create 权限的差异，将总结作为实验报告内容 2 提交。

步骤 4 将 USERxx 身份按照步骤 1 要求修改，然后再重复步骤 1 到步骤 3。