安全管理实验
实验指导书

同济大学 高珍 编写

实验 1.5 保护 TSO 资源

实验目的： 授权用户登陆 TSO

实验设备： IBM 大型主机 z900

实验结果： 实验后，学生应该掌握

- RACF 如何控制用户对 TSO 的访问
- 如何利用 RACF 通用资源 PROFILE 保护 TSO 的登陆过程(TSOPROC)和用户帐号(ACCTNUM)
- 如何定义用户 PROFILE 的 TSO 段

实验介绍： 该实验将首先为 AP(application programmer)和 SP(system programmer)用户建立组结构，然后为 TSO 的登陆过程(TSOPROC)和用户帐号(ACCTNUM)建立一些通用资源 PROFILE 进行保护，接着新增 AP/SP 用户 PROFILE，对 TSO 段进行赋值，并对他们授权访问 TSO

需要用到的一些通用资源 RPOFILE 结构如下图，可以根据需要逐渐补充完整：

TSOPROC	OWNER	UACC	Access List

ACCTNUM	OWNER	UACC	Access List

步骤 1 以 yourid 登陆 TSO，该用户是 RACFLAB 的 Group Special 用户，应该已经赋予了充分的权限新建和管理该组的用户，请使用‘LU’命令查询 yourid 的权限回答以下问题。（可选）

(1) What give you the capability to define the new user profiles to RACF?

---

(2) You have been given UPDATE access in a profile name USER.TSO.* in the Field general resource class. Will this be sufficient to allow you to define TSO segments when you define new users?

---

(3) What give you the capability to define profiles to control access to TSO logon procedures?

---

(4) What give you the capability to define profiles to control access to account

numbers?

步骤 2 新增 AP 和 SP 用户，这些用户需要访问 TSO

(1) 对 USERxx 的 TSO 字段做如下修改：

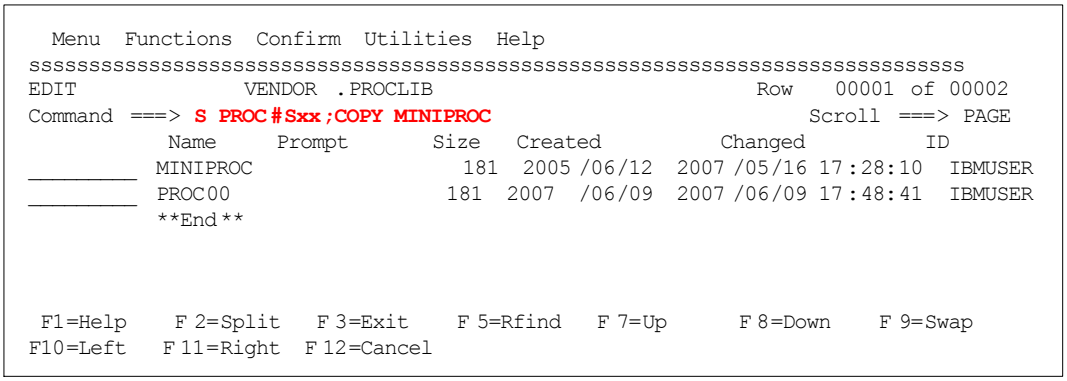
(1) 账户使用 ACCTxx

(2) 登陆过程使用 PROCxx

(3) Region 大小为 4096

HINT: ALU

步骤 3 为 TSO 用户创建一个新的登陆过程 PROCxx (下图中的 IKJ#ST 是已建好的登陆过程的模版，请注意，把图中的 PROC#Sxx 相应改为 PROCxx)，该登陆过程必须存放在 VENDOR.PROCLIB 库中，注意要把成员中的过程名和作业步的名字也相应改为 PROCxx



步骤 4 测试 USERxx 登录 TSO，成功吗？出现什么信息？

步骤 5 保护 PROCxx 登陆过程 (TSOPROC 类)：创建一个通用资源 RPOFILE

(1) 创建通用资源 TSOPROC 的 RPOFILE，保护 TSO 登陆过程

授权规则：PROCxx 只有 DIVxx 用户组才能使用(READ 权限)，其他人不可以使用；

思考：资源 Profile 的 Owner 如何指定？

HINT: RDEFINE... ； PE...

(2) 浏览 PROCxx PROFILE 内容，确认保护策略是否正确，并截屏提交。

HINT: RLIST

步骤 6 刷新 TSOPROC 类在内存中的 Profile

HINT: SETROPTS RACLIST() REFRESH

步骤 7 保护 ACCTNUM

创建 TSO 账户(ACCTNUM)，并创建一个通用资源 RPOFILE 保护该 ACCTNUM

(1) 创建 RPOFILE：ACCTxx 该 ACCTNUM 为 DIVxx 用户提供 TSO 登陆服务

授权规则：ACCTxx 只有 DIVxx 组才能使用(READ 权限)，其他人不可以使用；

思考：资源 Profile 的 Owner 如何指定?

HINT: RDEFINE... ； PE...

(2) 浏览 ACCTxx PROFILE 内容，确认保护策略是否正确，并截屏提交。

HINT: RLIST

步骤 8 保护 TSOAUTH（可选)

TSOAUTH 通用资源类提供保护 TSO 权限的功能，TSO 权限主要包括：ACCT，JCL，MOUNT，OPER，RECOVER 等。系统已经定义了一个 JCL PROFILE 用于保护 TSO 的 JCL 权限，该权限是允许通过 TSO 向 JES 提交 JCL 批量作业

(1) 查看 USERxx 用户/DIVxx 组的用户是否拥有提交 JCL 作业的权利。

HINT: RLIST TSOAUTH JCL

步骤 9 检测 TSO 用户的设置是否有效

(1) 以 USERxx 登陆 TSO，测试是否成功

---

(2) 在登陆过程中，可以尝试做下面的测试

- 删除 TSOPROC 和 ACCTNUM，看系统怎么反应?

- 键入不存在的 TSOPROC 和 ACCTNUM，看系统怎么反应?

---

(3) 以 yourid 登陆 TSO，删除 USERxx 用户 RPOFILE 的 TSO 段，然后再尝试以 USERxx 登陆，看系统怎么反应?

HINT:请查阅《Security Server RACF Command Language Reference》(SA22-7687-09) 参考书的 123 页

(4) 为 USERxx 重新赋值 TSO 段，使 USERxx 能够成功登陆 TSO

步骤 10 思考：如果想为 TSO 资源的保护指定一个管理员，如何操作比较简单高效?

步骤 11 包括三部分内容，分别如下：

（1）完成步骤 5（2）的截屏提交；

（2）完成步骤 7（2）的截屏提交；

（3）完成 USERxx 用户在步骤 9（1）成功登陆系统后的 ISPF 界面（类似下面截图，必须有用户 ID 信息）截屏提交。