S/390 企业级服务器下的用户管理策略分析

余祥宣　龙涛　彭娅婷　（华中理工大学计算机学院 IBM 技术中心　430074）

摘要：本文对 IBM 公司的企业级服务器——S/390 大型机系统环境下的资源访问控制器 RACF 作了简单介绍。详细分析了对大型机上的用户及组的 RACF 描述文件结构和定义过程，并对该系统下用户及组的管理策略提出了自己的构想。

关键词：用户管理　RACF　UP　GP

一、引言

S/390 是 IBM 大型机的新一代产品，运行 OS/390 操作系统。在安全管理方面与前代系统相比，OS/390 采用了新的控制部件 RACF(Resource Access Control Facility)专门担负安全管理任务，包括用户、组、数据集和通用资源(如磁盘、磁带、终端、交易程序等)。通过 RACF，可以实现对系统和用户资源灵活而严格的保护，防止对被保护对象的非法访问和攻击。本文将着重介绍 RACF 对用户和组的管理方式和过程，并试图探讨一种有效的管理策略。

二、用户和组的结构关系

S/390 下的用户和组的组织有其特殊的地方。用户既是系统的保护对象，又是系统安全的防范目标。一般来说，用户都应定义在 RACF 下。通过 RACF 定义用户有利于用户的管理，减少用户非法访问系统资源的风险。由于用户使用系统的方式有很多，如直接登录活提交批作业等，因此在定义用户时应该根据实际情况，既要让用户有足够的权限完成自己的任务，又不能给用户不必要的权限。

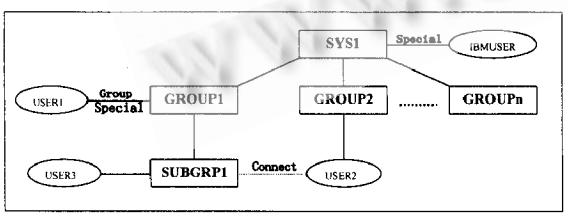

图 1　系统用户及组结构示意图

组的作用是为了便于管理具有共性的用户。实际的应用中组的定义常常对应于企业的部门或职能结构，如企业的各机关、各项目小组等等。和其他系统如 UNIX 不同，S/390 系统下的组有严格的树状层次结构，位于根节点的组名为 SYS1，这是系统安装初始组，以后定义的组都在 SYS1 之下。在定义组的时候，必须指明该组的上级组(或称父组)。定义用户时，每个用户都必须指明其缺省组。系统的用户和组的结构可以简单表示如图 1(方框表示组，椭圆表示用户)：

在上结构中，组 SYS1 为系统组结构的根节点，其中有一个名为 IBMUSER 的用户，该用户具有系统 SPECIAL 权限(IBMUSER 是系统安装时的初始用户)。SYS1 下有 GROUP1、GROUP2 等子组，GROUP1 下又有 SUBGRP1 子组。用户 USER1 属于组 GROUP1，该用户具有 GROUP－SPECIAL 权限，他将负责对整个组及其子组的管理工作。用户 USER2 属于组 GROUP2，但同时又通过 CONNECT 方式关联到组 USBGRP1，从而能享用两个组下定义的资源。关于用户和组的关系，本文将在后面详细说明。

三、UP 和 GP 的结构及其定义

RACF 是通过描述文件(Profile)来管理用户和组的。描述文件位于 RACF 数据库中，只有一定权限的用户通过专门的系统工具或 RACF 命令才能访问。

1. UP 的结构

一个用户描述文件(User Profile，以后简称为 UP)的主要内容可表示为如下形式：

UP 名	所有者	口令字(密文)	系统级属性	安全级	缺省组	组级属性	组级权限	其他信息

(1)UP 名：用户描述文件名，一般即为用户标识名。

(2)所有者：确定谁拥有此 UP，所有者可以是一个存在的用户或组，如果是用户，则该用户可以删除或修改此 UP；如果是组，则该组中具有 GROUP－SPECIAL 权限的用户可以删除或修改此 UP。

(3)口令字：用户的登录口令字，为密文形式。

(4)系统级属性：用户的系统级属性(主要相对于组

级属性而言)主要有以下几种:

①SPECIAL 具有系统级 SPECIAL 属性的用户可以使用 RACF 的所有命令,这意味着该用户能完全控制 RACF 的数据库,是最高权限者。因此应当严格控制这类用户的个数。

②AUDITOR 具有系统级 AUDITOR 属性的用户可以检查所有 RACF 描述文件的设置情况、按条件查询 RACF 的对象、设置系统日志纪录参数(即设置在何种情况下纪录日志)。以及使用系统审计工具等。

③OPERATIONS 具有系统级 OPERATIONS 属性的用户负责系统的数据维护工作,如备份、恢复、压缩文件、重组目录等工作,他们能全权访问 RACF 保护下的数据集、磁盘、磁带等资源。

(5)安全级:对用户做安全标记,用于实现强制访问控制(可以使系统达到 B1 级安全标准)。访问有安全标记的资源时,用户必须提供自己的安全标记(由管理员分配),如用户标记小于资源安全标记则无法访问该资源;

(6)缺省组:每个用户都必须有一个缺省组。该组决定了用户的基本职责和权限。

(7)组级权限:定义用户和组的关系,确定用户在组中的作用。常用的组权限有:

①USE 这是用户最基本的组级权限,表示用户可以访问组内资源。

②CREATE 这是具有一定管理权力的组级权限,具有 CREATE 权限的用户可定义该组下的数据集的 RACF 描述文件,并能创建组数据集。

③CONNECT 具有 CONNECT 权限的用户可以将其他组外用户关联到该组,使这些用户能访问该组资源。

④JOIN 具有 JOIN 权限的用户能在该组下定义子组。

以上各种属性是逐级递增的,具有 JOIN 属性的用户亦具有 CONNECT 用户的权限,具有 CONNECT 属性的用户亦有 CREATE 用户的权限,以次类推。

(8)组级属性:定义了用户在组中的特殊职责。常用的组属性有 GROUP_SPECIAL、GROUP_AUDITOR 和 GROUP_OPERATIONS。组级权限和相应的系统权限类似,只是各种操作权限仅限于该组范围内。

(9)其他信息:其他信息包括 TSO(Time Share Options,主机提供的交互式操作环境)、OMVS(Open MVS,一种主机系统下的 UNIX 环境)等有关的安全信息,以及用户登录时间、用户有效期、用户说明等等。

2. GP 的结构

一个组描述文件(Group Profile,以后简称为 GP)的内容相对较为简单,可表示为如下形式:

GP 名	所有者	上级组	其他信息

(1)GP 名:组描述文件名,一般即为组名。

(2)所有者:确定谁拥有此 GP,所有者可以是一个存在的用户或组,如果是一个用户,则该用户可以删除或修改此 GP;如果是一个组,此组必须为上级组,上级组中具有 GROUP－SPECIAL 权限的用户可以删除或修改此 GP。

(3)上级组:除了 SYS1 组外,每个组都必须定义其上级组,从而形成树状结构,这种结构是对应于企业的部门组织结构的。

(4)其他信息包括终端访问属性、OMVS 段、DFP 段,以及组的说明等,本文亦不作详细讨论。

3. 组和用户的定义和关联

定义用户和组。可以在命令行下使用 RACF 命令来定义他们。如:

ADDGROUP GROUP1 OWNER(SYS1) SUPGROUP(SYS1)

该命令定义了一个名为 GROUP1 的组。该组的所有者为 SYS1,上级组为 SYS1。命令名也可以简写为 AG。

ADDUSER USER1 OWNER(GROUP1) DFLTGRP(GROUP1) AUDITOR SECLEVEL(3)+

AUTHORITY(CONNECT) PASSWORD(USER1)

该命令定义了一个名为 USER1 的用户。该用户的所有者为 GROUP1,亦即其缺省组。用户具有系统级的 AUDITOR 权限和组级 CONNECT 权限。用户的安全级为 3,初始口令字与用户名相同(用户第一次登录时必须修改其口令字)。该命令也可以简写为 AU。

CONNECT USER1 GROUP(GROUP2) SPECIAL REVOKE(12/31/1999)

该命令将用户 USER1 关联到组 GROUP2 中,并赋予其组级 SPECIAL 权限。参数 REVOKE 在这里指明这个关联将在 1999 年 12 月 31 日失效。

以上命令也可以用系统提供的 TSO 环境下提示模板实现,这样更直观方便。但如果要编写批次处理的程序(如 CLIST),掌握 RACF 命令还是必要的。

四、用户和组的管理策略

制订完备的用户和组的管理策略,不但能减轻系统管理员的负担、便于日常维护,还可以最大程度地降低安全风险。这种管理策略越早制订越有效。通常系统中的用户和组的定义和企业组织结构密切相关,但还应从系统功能的角度对用户和组进行划分。

1. 组的规划

在定义组之前,应该仔细考虑定义该组的目的。从这个角度上考虑,系统中的组可按以下几类进行组织:

(1)管理员组。具有管理员权限的用户的集合,还可以分为系统管理员组和组管理员组。对组管理员,其职

能相当于部门或项目负责人。将这类用户归为一类主要是为了管理上的方便。

(2)数据控制组。某些系统数据集如 SYS1.RSRMLIB 等存放了系统初始化参数和系统工具程序集等关键信息。对这类数据集的保护显得尤为重要。定义数据控制组可以将这种管理职责交给组内用户专门负责,在撤销某些用户的这类职责时只需取消用户和该组的关联即可。

(3)功能组。这是最常见的组的划分办法。即从用户功能的角度将具有共性的用户归为一组。这种功能的划分往往是根据企业的实际情况进行的。如负责财会的用户往往需要访问特定的资源,使用特定的程序。将这类权限分配给专门的组,和该组关联的用户就可以完成关于财会方面的任务。

(4)用户组。即普通用户组,这也只是为了便于管理。比如公司职员、客户等。除了系统公用程序和工具,用户组中的成员基本无共同访问的特殊资源。

(5)限制组。限制组在系统中具有最低的权限,几乎不出现在任何一个访问控制表中。推荐系统中定义这样的组是从安全角度考虑的。将所有的新用户定义在该组下(以该组作为主组),然后将用户关联到各自的不同目的的组,能防止新用户得到不必要的权限。

2.权限的下放

从前面的介绍可以看出,具有系统级 SPECIAL 权限的用户是最高级别的管理员。这类用户应该尽可能的少(系统安装后,第一个具有该权限的用户为 IBMUSER。系统投入使用后,应该定义自己的 SPECIAL 用户,然后将 IBMUSER 的权限收回,或使该用户失效,以防敌手登录猜测其密码)。但对于一个大的企业来说,所有的用户和组的管理工作都交给有限的 SPECIAL 用户显然是不现实的。可以用定义组级 SPECIAL 用户的办法将下级组和用户的管理责任下放到其他用户。如图 1 所示,用户 USER1 承担了组 GROUP1 及其下级组和用户的管理工作(下级组和用户的所有者应设为 GROUP1)。同样,其他组如 GROUP2 等也应根据实际情况考虑设置他们的组级 SEPCIAL 用户,以分担系统级 SPECIAL 用户的工作。

值得一提的是,应将系统组和用户的结构按图 1 的形式画出,并标以详细说明,放置于安全隐秘的位置。

3.其他安全方面的考虑

为了减少系统被攻击的风险,管理员可以考虑设置用户的登录属性和 RACF 的口令字限制参数。常用的用户的登录属性有:

(1)有效期限:指明用户可以在何段时间内使用系统,通过 REVOKE 和 RESUME 参数指定。

(2)登录日:指明用户可以在每周的那些天访问系统,通过 WHEN 参数的 DAYS 子参数指定。

(3)登录时间:指明用户可以在每日的那个时间段内访问系统,通过 WHEN 参数的 TIME 子参数指定。

例如使用如下命令:

ALTUSER USER1 RESUME(1/1/1999) REVOKE(12/31/2000) +

WHEN(DAYS(WEEKDAYS) TIME(0900:1700))

将使用户 USER1 只能在工作日(周一至周五)的上午 9:00 至下午 5:00 时间内访问系统。并且该用户使用系统的有效日期为 1999 年 1 月 1 日至 2000 年 12 月 31 日。

常用的 RACF 口令辽限制参数有:

(1) INTERVAL 该参数值为 1 至 254 范围内的整数,指明用户的口令字有效天数。如果用户在该天数内未修改其口令字,系统将强制用户修改之。

(2)HISTORY 该参数值为 1 至 32 范围内的整数,指明系统将保存的用户口令字历史纪录数,用户在修改口令字时,不能和历史纪录的口令字相同。

(3)RULEn 该参数指明用户在设置其口令字时必须遵守的法则。另有子参数 LENGTH、NUMERIC 等进行该法则的定义。

(4)REVOKE 该参数值为 1 至 254 范围内的整数,指明系统允许用户尝试其口令的次数。如果用户连接输入错误的口令次数超过该值,用户帐号将暂时失效,直至管理员将该用户恢复。

例如使用如下命令:

SETROPTS PASSWORD(INTERVAL(15),HISTORY(1),REVOKE(3),+

RULE1LENGTH(5:8),NUMERIC(5)))

该命令说明用户的口令字有效期为 15 日;用户修改口令字时不能与原口令字相同;用户有三次尝试其口令字的机会;口令字的最小长度为 5 个字符,最大长度为 8 个字符,且第五个字符必须为数字。

显然,用上述方法可以大大提高系统的安全性,防止敌手用口令字典试探用户口令字,或进行午夜攻击等。以上命令和管理方式在华中理工大学 IBM 技术中心 S/390 大型机上成功通过和实现

参考文献

[1] OS/390 RACF V2R1 General Information,First Edition, 1996 年 9 月,IBM 手册文档

[2] OS/390 RACF V2R1 General User's, Guide, First EDition, 1996 年 9 月,IBM 手册文档

[3] OS/390 RACF V2R1 Security Administrator's Guide,First Edition, 1996 年 9 月,IBM 手册文档

(来稿时间:1999 年 9 月)