第 6 章　访问控制

Windows 2000 的安全特性通过身份验证和授权这两种相互联系的机制，来控制对系统和网络资源的访问和使用。访问控制则是实现第二阶段的功能，即确定一个已通过验证的用户是否具有访问资源的正确权限。

6.1　访问控制概述

访问控制的目的是为了限制访问主体用户进程服务等对访问客体（文件、系统等）的访问权限，从而使计算机系统在合法范围内使用。决定用户能做什么，也决定代表一定用户利益的程序能做什么。访问控制的作用是对需要访问系统及其数据的用户进行鉴别，并验证其合法身份，这也是进行安全审核等的前提。

与 Windows NT 4.0 相同，Windows 2000 使用访问控制技术来保证已被授权的主体对客体的使用。在 Windows 2000 系统中，安全主体（Security Principal）不仅仅包括用户，还包括组和服务等主动的实体；而客体则包括文件、文件夹、打印机、注册表、活动目录项以及其他对象。访问控制技术即决定安全主体能够在对象上执行何种类型的操作，如某个用户是否能够读取、写入还是执行某个文件。

6.2　访问控制机制

首先，从访问控制的主体角度出发，Windows 2000 系统在用户登录（无论是本地登录还是远程登录）的时候，都会为该用户创建一个访问令牌（Access Token）。该访问令牌含有该用户的 SID，用户所属组的 SID 和用户的特权。此令牌为用户在该计算机上的任何操作提供了安全环境。

而当用户每启动一个应用程序时，所执行的每一个线程都会得到一份该访问令牌的复本。作为用户的代理，每当线程请求对某个受到权限控制保护的对象进行任何级别的访问时，该线程都要把此访问令牌提交给操作系统。然后操作系统就使用该令牌针对对象的安全信息来执行访问检查。这种检查可以确保主体是在经过授权之后才进行访问的。

另一方面，从访问控制的客体角度出发，安全描述（Security Discriptor）定义了客体（被访问的对象）的安全信息。安全描述中除了对象所有者自身的 SID 之外，主要说明了哪些用户和组是被允许还是被拒绝访问。这通过一个由访问控制项（Access Control Entries, ACE）组成的自由访问控制列表（DACL）来实现。Window 2000 系统通过寻找 ACL 中的项（即 ACE）来匹配访问令牌中的用户 SID 和组 SID，以此 ACE 来确定用户是否有权限进行所请求的访问。图 6-1 描述了访问令牌与安全描述之间的关系。

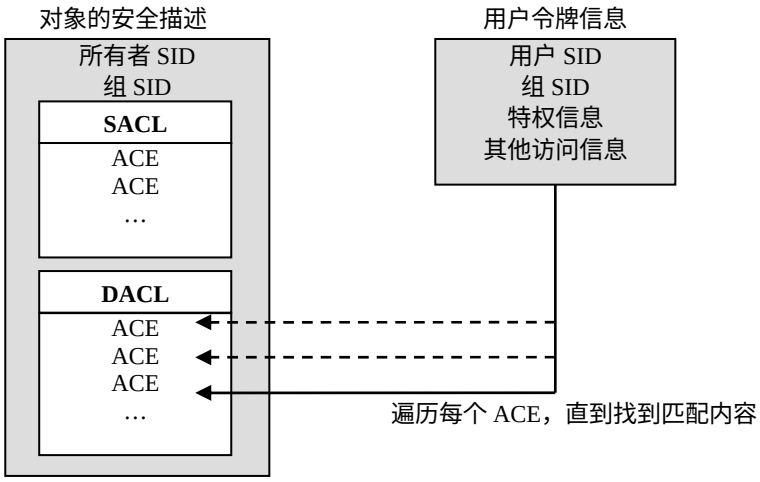

图 6-1　安全描述与访问令牌

对于配置了安全审核（后续章节中将详细叙述）的对象来说，安全描述中另外还包含了一个系统访问控制列表（SACL），用来通知安全子系统如何对访问对象的行为尝试进行审核和记录。

6.2.1 安全标识符

Windows 2000 使用安全标识符（SID）来标识安全主体和安全组。SID 是在主体账户或安全组创建时生成的。SID 的创建者和作用范围依赖于账户类型。对于用户账户，就由本地安全授权机构（LSA）生成在该系统内惟一的 SID。而对于域账户则是由域安全授权机构来产生 SID。活动目录把域账户 SID 当作该 SID 所标识的用户或组的一个对象属性来存储，而域账户 SID 在域内是惟一的。

SID 出现在下列一些访问控制结构中：

- 访问令牌包括一个用户的 SID 和用户所属组的 SID
- 安全描述包含与安全描述相关联对象所有者的 SID
- 安全描述中的每个 ACE 把 SID 与相应的访问权限关联起来

SID 的值是分层的，并且长度可变。像 Administrators 组、Everyone 组所用的 SID 都较为简洁，例如 Administrators 组的 SID 值固定为 S-1-5-32-544，Everyone 组的 SID 值固定为 S-1-1-0，而其他的 SID 则更长并且更为详细。SID 值的一般格式为：S-R-X-Y^1-Y^2…Y^{n-1}-Y^n。其中各部分的含义如下。

- S：表示该字符串是一个 SID
- R：表示 SID 结构的版本号。在 Windows 2000 系统中，这个值为 1。
- X：表示标识符颁发机构（Identifier Authority）。对于 Administrators 组或其他任何特定的 Windows 2000 用户和组，这个标识符颁发机构是 NT Authority（标识符颁发机构 5）；而对于 Everyone 等一般用户和组，则由 World Authority（标识符颁发机构 1）来颁发 SID。
- Y^1~Y^{n-1}：表示子级颁发机构。这些元素能够用来区分不同域中的 SID。如 Administrators 组的域标识符为 Builtin（32），而 Everyone 组没有域标识符。
- Y^n：相对标识符。它用来标识域内特定的账户和组。如 Administrators 组的相对标识符是 Administrators（544），而 Everyone 组的相对标识符为空。

6.2.2　访问令牌

访问令牌是一个受保护的对象，其中包含与用户账号有关的标识和特权信息。当用户交

互地或通过网络连接登录到一台运行 Windows 2000 的计算机上时，登录进程会对用户的登录资格进行认证。若认证成功，登录进程会返回该用户的 SID 和该用户的安全组的 SID 列表。计算机上的本地安全授权机构（LSA）根据这个返回信息创建一个访问令牌，里面包含登录进程返回的 SID 和由本地安全策略分配给用户和用户的安全组的特权列表。代表用户执行的所有进程和线程都有访问令牌的一个复本。只要某个线程与安全对象发生作用或试图执行一个需要特权的系统任务，操作系统就检查与该线程相关的访问令牌来确定它的授权级别。

1. 访问令牌的内容

访问令牌包含进程或线程的安全上下文的完整描述，其中含有如下信息。

- 用户（User）。用户账号的 SID。若用户登录到本地计算机上的一个账号，则他的 SID 来自于本地 SAM 维护的账号数据库；若用户登录到一个域账号，则他的 SID 来自于活动目录里用户对象的 Object-SID 属性。
- 组（Groups）。包含该用户的安全组的 SID 列表，表中也包含代表活动目录里用户账号的用户对象的 SID-History 属性里的 SID。
- 特权（Privileges）。用户和用户的安全组在本地计算机上拥有的特权列表。
- 所有者（Owner）。特定用户或安全组的 SID，这些用户或安全组默认成为用户所创建或拥有的任何对象的所有者。
- 主组（Primary Group）。用户的主安全组的 SID。这个信息只由 POSIX 子系统使用，Windows 2000 的其他部分对其忽略。
- 默认任意访问控制表（Default Discretionary Access Control List, DACL）。一组内置许可权。在没有其他访问控制信息存在时操作系统将其作用于用户所创建的对象。默认 DACL 向创建所有者和系统赋予完全控制（Full Control）权限。
- 源（Source）。导致访问令牌被创建的进程，例如会话管理器、LAN 管理器或远程过程调用（RPC）服务器。
- 类型（Type）。指示访问令牌是主（primary）令牌还是模拟（impersonation）令牌。主令牌代表一个进程的安全上下文；模拟令牌是服务进程里的一个线程，用来临时接受一个不同的安全上下文（如服务的一个客户的安全上下文）的令牌。
- 模拟级别（Impersonation Level）。指示服务对该访问令牌所代表的客户的安全上下文的接受程度。
- 统计信息（Statistics）。关于访问令牌本身的信息。操作系统在内部使用这个信息。
- 限制 SID（Restricting SID）。由一个被授权创建受限令牌的进程添加到访问令牌里的可选的 SID 列表。限制 SID 可以将线程的访问限制到低于用户被允许的级别。
- 会话 ID（Session ID）。指示访问令牌是否与终端服务（Terminal Services）客户会话相关。

2. 模拟

线程能够在与拥有它的进程的上下文不同的安全上下文里执行，这种能力称为模拟，它是为了满足客户/服务器应用的安全需求而设计的。当在一个客户的安全上下文里运行时，服务在某种程度上“是”客户。服务的一个线程使用代表客户资格的访问令牌来访问该客户有权访问的对象。

模拟的主要原因是根据客户的标识执行访问检查。使用客户标识进行访问检查可以根据该客户拥有的许可权来限制或扩展访问。例如，假设一个文件服务器上有包含秘密信息的文件，这些文件都由一个 DACL 保护。为了防止客户未经授权就可访问这些文件中的信息，

服务可以在访问文件之前模拟客户。

每个进程都有一个主令牌（primary token）来描述与该进程相关的用户账号的安全上下文。与普通的应用进程相关的用户是启动该应用的人为用户，但对一个服务进程却非如此：服务在自己的账号下运行，在自己的权限内充当用户。与操作系统一起安装的系统服务在本地系统账号下运行，其他的服务可以配置为在这个账号下运行，也可以给予在本地系统上或活动目录里的单独账号。一个服务的主令牌与该服务进程里的控制线程和代表该服务运行的所有其他线程相关。它标识该服务的账号、该账号的组和特权。当服务请求访问完成工作所需的对象时，在访问检查时使用该信息。

当服务接受一个客户时，它创建一个线程来完成这项工作并将客户的访问令牌与工作线程相关联。客户的访问令牌是一个模拟令牌，它标识客户、客户的组和特权。当线程代表客户请求访问资源时，在访问检查过程中使用该信息。在模拟结束后，线程重新使用主令牌并返回到服务自己的安全上下文里操作，而不是客户的上下文。

3. 模拟级别

模拟成功意味着客户在某种程度上同意服务器“ 成为 ”客户。客户进程通过在连接到服务时选择一个模拟级别可以控制服务在何种程度上充当客户。通过选择模拟级别，客户告知服务它能够如何模拟自己。

模拟级别不能由用户选择，它作为服务安全质量（SQoS）信息在客户/服务器应用的代码里加以说明。模拟有四种级别：匿名（anonymous）、标识（identify）、模拟（impersonate）和委托（delegate）。匿名从来都不被支持。在 Windows 2000 之前的系统只支持标识和模拟，Windows 2000 增加了对委托的支持。下面是各个级别的简要描述。

- 匿名：客户对于服务是匿名的。服务可以模拟客户，但模拟令牌不含有客户的任何信息。
- 标识：服务可以获得客户的标识并在自己的安全机制里使用该信息，但它不能模拟客户。
- 模拟：服务可以模拟客户。若服务与客户进程在同一台计算机上，则它可以作为客户来访问网络资源；若服务在一台远端计算机上，它只能在访问服务所在的计算机上的资源时模拟客户。
- 委托：服务不仅在访问自己所在的计算机上的资源时可以模拟客户，也可在访问其他计算机上的资源时进行模拟。

6.2.3 安全描述

1. 安全描述的结构

正如访问令牌把用户权限和特权通知安全子系统一样，包含在对象安全描述中的信息也帮助安全子系统控制哪些用户可以访问对象以及如何访问。当在授权用户安全环境中执行的线程创建一个对象时，安全描述就会被填入访问控制信息。

虽然安全描述中的具体信息依赖于对象类型以及对象的创建方式，但是安全描述有一个已定义的结构，包括下列部分。

- 头部（Header）。除一个修订版本号之外，这部分还包括用于描述安全描述及其组件的一组控制标志。这些控制标志是一些说明布尔值的位，例如描述符中包含的是 DACL 还是 SACL。另外，Windows 2000 安全描述中的控制标志位还包含有关自动传播的信息，例如可继承权限是否能够修改安全描述中的 DACL 和 SACL。
- 所有者（Owner）。该字段包含对象所有者的 SID。

- 主组（Primary Group）。该字段包含所有者主要组的 SID。
- 自由访问控制列表（DACL）。在对象所有者的控制下，DACL 是包含零个或多个 ACE 的列表，用它来控制特定用户和组对对象的访问。每个 ACE 属于一个 SID，并且包含一些指定该项允许还是拒绝访问的信息以及与这些访问类型相关联的操作。
- 系统访问控制列表（SACL）。SACL 也是包含零个或多个 ACE 的列表，但是 SACL 用于审核而非控制对象访问。除用户或组的 SID 之外，SACL 中的 ACE 还包括所要审核的操作以及审核事件是由成功操作还是失败操作（或者两者一起）触发的。

2．默认安全描述

如前所述，活动目录对象的所有者可以在创建对象时指定一个安全描述。如果所有者没有指定安全描述，那么资源管理器就会提供操作系统应用于对象的默认安全信息。活动目录提供的默认安全描述的字段依赖于创建者的访问令牌和对象所属容器的可继承属性。安全描述的字段适用于下列规则：

- 如果访问令牌中没有包含一个默认所有者，那么 Owner 字段就被设置为创建者访问令牌中的 SID。否则，Owner 字段就被设置为创建者的默认所有者。但是，如果创建者属于 Domain Administrator 组，那么 Owner 字段就被设置为 Domain Administrator 组的 SID。
- 如果 Primary Group 字段存在的话，将被设置为创建者访问令牌中的默认主要组；否则，Primary Group 字段就被设置为一个空 SID。
- 如果提供了一个直接 DACL，那么该 DACL 就会同父容器 DACL 中的任何可继承 ACE 合并到一起，并被设置为新对象的 DACL。如果没有提供直接 DACL，但是活动目录架构提供了一个默认 DACL，那么该默认 DACL 就被设置为新对象的 DACL。如果默认 DACL 不是由活动目录而是由所有者的访问令牌所提供的，那么该默认 DACL 也会被设置为对象的 DACL。如果以上都不成立，那么新对象将没有任何 DACL，并且所有用户都可以无条件地访问该对象。
- 像 DACL 一样，SACL 被设置为所提供的直接 SACL，并且其尾部附有来自其父容器 SACL 中的所有可继承 ACE。如果没有提供直接 SACL，那么可以由活动目录架构提供一个默认的 SACL；如果活动目录架构也没有提供默认 SACL，那么新对象将没有任何 SACL。

6.2.4 访问控制列表和访问控制项

访问控制列表（ACL）定义了系统在对被访问的对象进行保护时所使用的标准。由于 Windows 2000 安全子系统考虑了多方位的基于对象的访问控制，如是针对对象本身的访问请求还是针对对象某一个属性的访问请求，是何种类型的请求（读取、写入还是执行），以及是允许还是拒绝该访问类型。所以，一个 ACL 中会存储大量的安全信息。

1. 访问控制列表

访问控制列表（ACL）是访问控制项（ACE）的有序列表，这组 ACE 定义了作用于对象和它的属性的保护措施。每个 ACE 都标识一个安全主体，并规定了一组对该安全主体的允许、禁止或审计的访问权限。ACL 的数据结构如图 6-2 所示。

ACL 大小	ACL 修改版本
ACE 数目	
[ACE 1]	
[ACE ...]	
[ACE n]	

图 6-2 ACL 的结构

ACL 的各组成部分如下。

- ACL 大小：分配给该 ACL 的内存字节数。ACL 的大小与它的 ACE 的数目和大小有关。
- ACL 修改版本：ACL 的修改版本号。所有 ACL 版本的结构都是相同的，但它的 ACE 结构可以不同。大多数对象的版本号是 2，活动目录对象的版本号是 4。
- ACE 数目：ACL 里包含的 ACE 数目。0 表示 ACL 中没有 ACE，即 ACL 为空，因此可以结束访问检查。
- ACE：含有 0 个或多个 ACE 的有序列表。访问检查时，ACE 按照排列顺序被处理。

ACL 包括 DACL 和 SACL 两种类型。其中 DACL（自由访问控制列表）规定了哪些安全主体可以访问对象以及能以何种类型的方式进行访问，而 SACL（系统访问控制列表）则规定了应该审核哪些安全主体发出的哪些访问请求。

这里需要注意的是，“ 空 DACL ” 与 “ 没有 DACL ” 是截然相反的。“ 没有 DACL ” 的意思指的是对于该对象没有任何保护，发出请求的任何用户都被允许访问该对象；而 “ 空 DACL ” 则恰恰相反，它表示在列表中没有任何 ACE 的存在，所以也就不允许任何用户进行访问。

2. 访问控制项

Windows 2000 支持在访问控制列表（ACL）中使用六种类型的访问控制项：三种一般的 ACE 类型，可以存在于所有安全对象的 ACE 里；另外三种 ACE 类型则是与对象有关的，只能出现在活动目录对象里。这六种类型的 ACE 分别是：

- 拒绝访问。该一般类型在 DACL 中拒绝访问。
- 允许访问。该一般类型在 DACL 中允许访问。
- 系统审核。该一般类型在 SACL 中记录访问尝试。
- 特殊对象的拒绝访问。该类型在 DACL 中拒绝对一个或一批属性的访问，并限制子对象的继承。
- 特殊对象的允许访问。该类型在 DACL 中允许对一个或一批属性的访问，并限制子对象的继承。
- 特殊对象的系统审核。该类型在 SACL 中记录对一个或一批属性的访问尝试，并限制子对象的继承。

其中的三种一般类型在任何可保护对象的 ACL 中都可以找到，而另外三种类型都称为特殊对象类型，它们只出现在活动目录对象的 ACL 中，是 Windows 2000 所新增的。特殊对象类型与一般类型 ACE 之间的基本区别在于，特殊对象类型 ACE 对可继承这些 ACE 的子对象类型提供了更好的控制粒度。

与对象有关的 ACE 对可以继承自己的子对象类型提供了更大的控制粒度。例如，一个 OU 对象的 ACL 可以有一个被标记为只由用户对象继承的与对象有关的 ACE。其他类型的对象，如计算机对象，不会继承该 ACE。它们的继承性可以限制到特定类型的子对象。

这两类 ACE 在控制对对象的访问方面也有类似的区别。一般 ACE 应用于整个对象。若

一个一般 ACE 给予某个用户读访问的权限，该用户就可以读与该对象相关的所有信息，包括数据和属性。对于大多数对象类型来说这不是一个严重的限制。例如，文件对象只有很少几个属性，都是用来描述对象的特征而不是存储信息，文件对象里的大多数信息作为对象数据而存储，所以没必要对文件的属性进行分开控制。而与对象有关的 ACE 可以作用于对象的一个或一组属性上，这些 ACE 类型只用于活动目录对象的 ACL 中。与其他对象类型不同，这些对象在属性中存储它们的大多数信息。通常会希望对一个活动目录对象的每个属性进行单独控制，与对象有关的 ACE 使得这种操作变为可能。

3. 一般 ACE 的结构

上面三种一般的 ACE 类型都有同样的数据结构，如图 6-3 所示。

图 6-3 一般 ACE 的结构

ACE 的各组成部分如下。

- ACE 大小：为该 ACE 分配的内存字节数。
- ACE 类型：规定该 ACE 是否允许、禁止或监视访问。
- 继承和审计标志：一组控制继承和审计的位标识。
- 访问屏蔽码：一共 32 位，每一位对应着该对象的访问权限。可设置为打开或关闭，但设置的含义与 ACE 类型有关。例如，若对应于读许可权限的一位被打开，ACE 类型为禁止，则该 ACE 禁止读对象的许可权限；若 ACE 类型为允许，则该 ACE 授予读对象的许可权限。
- SID 标识：其访问由该 ACE 控制或监视的一个用户或组。

4. 与对象有关 ACE 的结构

图 6-4 给出了与对象有关的 ACE 的结构。

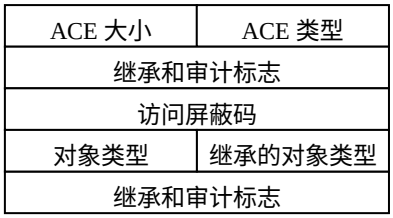

图 6-4 与对象有关的 ACE 的结构

其中 ACE 大小、ACE 类型、继承和审计标志、访问屏蔽码和 SID 的含义与一般 ACE 结构中对应的部分是相同的。一般 ACE 和与对象有关 ACE 的主要不同如下。

- 对象标志。对象标志指示对象类型或继承的对象类型是否存在。
- 对象类型。对象类型含有一个 GUID，标识以下内容之一：
  - 子对象类型。该 ACE 控制谁可以在一个容器中创建特定类型的子对象。ACE 的 SID 部分标识可以创建这种子对象类型的一个用户或组，ACE 的访问屏蔽码含有与对象有关的访问权限 ADS_RIGHT_DS_CREATE_CHILD。
  - 属性或属性集。该 ACE 控制读或写特定属性或属性集的能力。ACE 的 SID 部分标识可以读或写该属性或属性集的一个用户或组， ACE 的访问屏蔽码含有

ADS_RIGHT_DS_READ_PROP 或 ADS_RIGHT_DS_WRITE_PROP。

- 扩展权限。该 ACE 控制执行与该扩展权限有关的操作的权利。ACE 的 SID 部分标识拥有该扩展权限的一个用户或组，ACE 的访问屏蔽码含有 ADS_RIGHT_DS_CONTROL_ACCESS。

- 继承的对象类型。继承的对象类型含有一个 GUID，标识可以继承该 ACE 的子对象的类型。继承也由 ACE 的继承标志和在子对象的安全描述符控制标志里对子对象设置的任何继承保护来控制。

6.3 用户和组基础

用户账户可为用户提供登录到域以访问网络资源或登录到计算机以访问该机资源的能力。Windows 2000 提供两种类型的用户账户：本地用户账户和域用户账户。用户使用域用户账户（Domain User Account）可登录到域以获得对网络资源的访问，而使用本地用户账户（Local User Account）可登录到特定计算机以访问该机资源。用户在登录到 Windows 2000 计算机（非域控制器）的时候可以选择是登录到域还是本地计算机。

若要创建和管理域用户账户，可使用“ Active Directory 用户和计算机 ”控制台。可在该控制台中创建用户对象、删除或禁用用户对象，也可以管理用户对象的属性。

而组（Group）是用户或计算机账户的集合。组可以允许将权限分配给一组用户而不是单个用户账户，从而简化系统和网络管理。当将权限分配给组时，组的所有成员都将继承那些权限。除用户账户外，还可以将其他组、联系人和计算机添加到组中。将组添加到其他组可创建合并组并减少需要分配权限的次数。也可以将计算机添加到组中，从而简化从一台计算机上访问另外一台计算机上资源的任务。

Windows 2000 允许在独立的计算机和 Active Directory 服务中创建组。与使用用户账户一样，本地组是专门用来管理单个计算机的资源，而使用 Active Directory 组可允许用户访问网络资源。

6.3.1 组类型

组的使用有时是与安全性相关的，如分配访问控制的权限、进行审核等；而有的时候则用于非安全性用途，如发送电子消息。所以，Windows 2000 系统包括有两种类型的组：安全组（security）和分布组（distribution）。两种类型的组都存储在 Active Directory 服务的数据库中，该数据库使得网络上的任何位置都可以使用组，而组的类型决定该如何使用组。

- 安全组：Windows 2000 自身只使用安全组，安全组可用来分配访问资源的权限和执行任务的权利。专门使用 Active Directory 服务的程序也可将安全组用于非安全性的用途，如检索要在 Web 应用程序中使用的用户信息。安全组也可拥有分布组的所有功能。
- 分布组：应用程序可将分布组用于与安全性不相关的列表。当组的惟一功能与安全性（如同时向一组用户发送电子邮件）不相关时，就可以使用分布组。与安全组不同的是，分布组不能用来分配权限。

6.3.2 组作用域

组作用域（group scope）用来决定在网络的什么位置可以使用组，也可以决定能以不同的方式分配权限。在 Windows 2000 系统中有 3 个组作用域，它们分别是全局组、域本地组和通用组。当通过“ Active Directory 用户和计算机 ”控制台创建组的时候，就必须对组类型和组作用域进行选择，如图 6-5 所示。

图 6-5 指定组作用域和组类型

有通用作用域的组可将其成员作为来自域树或树林中任何 Windows 2000 域的组和账户，并且在域树或树林的任何域中都可获得权限。有通用作用域的组称为通用组。

有全局作用域的组可将其成员作为仅来自组所定义的域的组和账户，并且在树林的任何域中都可获得权限。有全局作用域的组称作全局组。

有本地作用域的组可将其成员作为来自 Windows 2000 或 Windows NT 域的组和账户，并且可用于仅在域中授予权限。具有本地作用域的组称作域本地组。

如果具有多个树林，仅在一个树林中定义的用户不能放入在另一个树林中定义的组，并且仅在一个树林中定义的组不能指派另一个树林中的权限。

它们之间的区别如表 6-1 所示。

表 6-1 不同类型组作用域之间的区别

	全局组	**域本地组**	**通用组**
可添加的成员来源	本地域	任何域	任何域
可访问的资源范围	任何域内	本地域内	任何域内
常见的应用环境	用来对具有类似网络访问要求的用户进行组织	用来给资源分配权限	用来给多个域内的相关资源分配权限

6.3.3 本地组

本地组（local group）是本地计算机上的用户账户的集合。可使用本地组给本地组所在计算机上的资源分配权限。Windows 2000 在本地安全性数据库（SAM）中创建本地组。注意将这个本地组同具有域本地作用域的 Active Directory 组区别开来。

使用本地组的原则如下，

- 只可在创建本地组的计算机上使用本地组。本地组权限只提供对本地组所在计算机上资源的访问。
- 可在运行 Windows 2000 的非域控制器的计算机上使用本地组，不能在域控制器上创建本地组。这是因为域控制器不能拥有与 Active Directory 服务中数据库独立的安全性数据库。
- 可使用本地组来限制本地用户和组访问网络资源的能力，而无须创建域组。

能够添加到本地组的用户必须满足如下条件。

- 本地组只包含来自本地组所在计算机上的本地用户账户。
- 本地组不能使其他任何组的成员。

6.4 内置本地组

Windows 2000 系统在初始安装的时候，只是一个成员服务器。活动目录需要在安装后创建，同时默认的安装配置也会有所改变。在安装时，Windows 2000 会自动创建以下的用户组，如表 6-2 所示：

表 6-2 Windows 2000 默认创建的用户组

成员服务器	
Administrators	管理员对计算机/域有不受限制的完全访问权
Backup Operators	备份操作员为了备份或还原文件可以替代安全限制
Guests	按默认值，来宾跟用户组的成员有同等访问权，但来宾账户的限制更多
Power Users	权限高的用户拥有最高的管理权限，但有限制。因此，权限高的用户可以运行经过证明的文件，也可以运行继承应用程序
Replicator	支持域中的文件复制
Users	用户无法进行有意或无意的改动。因此，用户可以运行经过证明的文件，但不能运行大多数继承应用程序
域控制器	
Account Operators	成员可以管理域用户和组账户
Print Operators	成员可以管理域打印机
Server Operators	成员可以管理域服务器

Windows 2000 系统安全的一个重要部分是由默认访问权限定义的。它提供了巨大的灵活性和基于标准的许多方法，与文件、打印以及网络服务一样，用户认证也达到了最高层次的安全保障。这些权限分三个组授予：Users 组、Power User 组和 Administrators 组。

6.4.1 Administrators 组

Administrators 组具有所有的权利。同时，Administrators 组可以执行任何和所有操作系统提供的功能。它也自动拥有对于磁盘上所有文件和文件夹的权限。如果缺省设置没有给 Administrators 组赋予一定的权利，它们自己可以授权给自己。

理想情况下，管理员只有在下列情况下才需要访问系统：

- 安装操作系统和组件（包括硬件驱动程序，系统服务及其他）。
- 安装 Service Pack 和 Hotfix 修补程序
- 安装 Windows Update
- 升级操作系统
- 修复操作系统
- 配置机器范围内的重要的操作系统参数（如密码策略、访问控制、审核策略、内核模式驱动程序配置等）
- 获取已经不能访问的文件的所有权
- 管理安全措施和审核日志
- 备份和还原系统

在实际操作中，管理员账户必须经常用来安装和运行基于 Windows 的旧版应用程序。综上所述，为了安全起见，推荐系统管理员和安全管理员只给自己普通用户的账号，只有在进行上述操作的时候，才使用 Administrators 的账号登录进行操作。

此外，Windows 2000 提供了一个新的功能：辅助登录服务（Secondary Logon Service, SLS），也称为 RunAs 服务。使得管理员可以使用标准的用户账户登录，并在必要的时候可以调用具有更高权限的管理员控制台来执行管理任务。可以通过两种方法访问 RunAs 服务。一种方法是通过在管理工具（Administrative Tool）应用组件上右击，然后从弹出的菜单中选择“运行为…”，就会出现如图 6-6 所示的对话框：

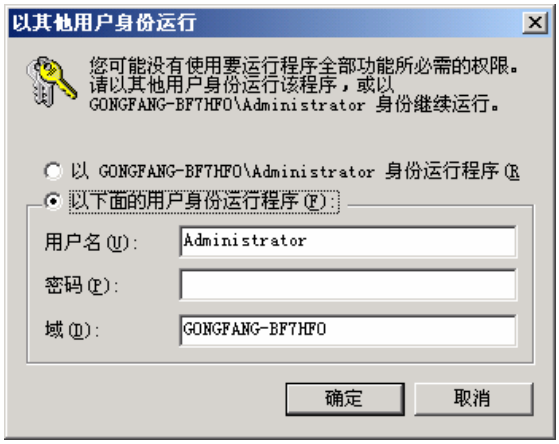

图 6-6　RunAs 对话框

还有一种方法就是在 DoS 命令符中输入“ runas ”，并按回车键来访问此服务。

6.4.2　Users 组

Users 组与 Administrators 组情况刚好相反。假设 Windows 2000 是完全安装到 NTFS 分区，默认设置不允许 Users 组破坏操作系统的完整性和安装的应用程序。Users 组不能修改底层的注册设置、操作系统文件或程序文件。用户不能安装可以被其他用户运行的应用程序（防止特洛伊木马）。用户不能访问其他用户的私有数据和桌面设置。

因此，以下两个方面对于保证基于 Windows 2000 系统的安全非常重要：

- 保证终端用户仅是用户组的成员。
- 部署普通用户可以顺利运行的应用程序。

理想情况下，用户应该能够运行由管理员、Power User 或自己事先安装的任何应用程序。用户应该不能运行由其他用户安装的应用程序。

实际操作中普通用户将不能运行绝大多数旧版应用程序，这是因为绝大多数旧版应用程序设计时没有考虑到操作系统的安全。而 Power User 组的成员应当可以运行这些应用程序。基本上 Microsoft 公司自己的软件和经过 Microsoft 认证过的软件，以及符合 Windows 2000 应用程序规范的应用程序可以在普通用户环境中顺利运行。例如 Microsoft Office 2000 / XP 等。

6.4.3　Power Users 组

Power User 在系统访问权限方面介于管理员和用户之间。Windows 2000 对 Power User 的默认安全设置与 Windows NT 4.0 系统中对用户的默认安全设置向后兼容。简而言之，Power User 事实上有一定权限。

理想情况下，Power User 应当能够执行除上述管理任务之外的任何任务。因此，Power User 应当能够：

- 在每一台机器上执行应用程序的安装和卸载，只要这些应用程序不需要安装系统服务即可。
- 自定义系统范围内的资源（如系统时间、显示设置、共享、电源管理、打印机及其他）。

但 Power User 无权访问其他用户存储在 NTFS 分区中的数据。实际情况下，Power User 不能安装许多旧版应用程序，因为这些应用程序在安装过程中试图替换操作系统的文件。

除了默认的 ACL 和用户权限允许的权限之外，Power User 还可以：

- 创建本地用户和组

- 修改其创建的用户和组
- 创建和删除非管理员文件共享
- 创建、管理、删除和共享本地打印机

管理员也可以执行所有这些操作。但是对于账户管理，管理员可以创建、删除或修改任何账户，而 Power User 只能修改或删除自己创建的账户。User 则不能执行这些额外的 Power User 操作。

默认情况下，Power User 还拥有：

- 对程序文件目录的修改访问权
- 对 HKEY_LOCAL_MACHINE \Software 注册表区内的修改访问权
- 对许多系统目录包括%windir%和%windir%\system32 的写入访问权

这些权限允许 Power User 在每一台机器上执行应用程序的安装，只要这些应用程序不需要修改系统服务即可。

但不幸的是，这些权限还允许 Power User 放置特洛伊木马，如果管理员或其他用户执行了特洛伊木马，将危及系统和数据的安全。做出系统范围内操作系统和应用程序更改，这些更改将影响系统的其他用户。

6.5 默认组成员

Windows NT 4.0 和 Windows 2000 默认安全设置之间的最大不同就是指派访问控制的方法。在 Windows NT 4.0 中，Everyone 组是用来包括文件系统 ACL、注册表 ACL 和用户权限的包罗万象的组。在某种意义上，Everyone 组不是一个传统意义上的组，因为管理员不能定义谁属于这个组，谁不属于这个组。相反，Windows NT 自动定义组成员身份，这样任何用户都是 Everyone 组的成员。如果管理员希望进行更细化的访问控制，必须对默认 ACL 进行修改以删除 Everyone 组并添加管理员能够控制的组。

Windows 2000 中使用不同的方式。那些像“任何人”和“经过身份验证的用户”组这样的其成员身份由操作系统自动配置的组不再用于分配权限。相反，只使用那些成员身份可以被管理员控制的组分配权限。在上一节中就讨论了这样的三个组：Users 组、Power Users 组和 Administrators 组。

表 6-3 列出了哪些用户是这些组的默认成员。如果用户是一个组的成员，那么该用户就自动拥有分配给该组的权限。

表 6-3 用户组的默认成员

本地组	默认工作站成员	默认服务器成员
Administrators	管理员	管理员
Power Users	交互式用户	
Users	经过身份验证的用户	经过身份验证的用户

默认情况下，在全新安装的 Windows 2000 Professional 和 Windows 2000 Server 上的用户组添加“经过身份验证的用户”组。只在 Windows 2000 Professional 上将“交互式用户 INTERACTIVE”组添加到 Power User 组。“经过身份验证的用户”和“交互式用户”组的成员身份由操作系统自动控制。除了没有匿名用户之外，“经过身份验证的用户”与“Everyone”组相同。因此，默认情况下，访问 Windows 2000 Server 的任何非管理员用户自动都是普通用户；访问网络上的基于 Windows 2000 Professional 的系统的任何非管理员用户都是普通用户；访问本地的基于 Windows 2000 Professional 系统的任何非管理员用户都是普通用户。

就访问控制设置而言，这种情形能保证 Windows 2000 Professional 计算机具有很好的向

后兼容性。因为 Windows 2000 的 Power User 具有与 Windows NT 4.0 用户相同的文件系统和注册表权限，Windows 2000 Professional 计算机上的交互式用户应当能够运行 Windows NT 4.0 用户能够运行的任何应用程序。但是，保证基于 Windows 2000 工作站的安全相对于 Windows NT 的前几个版本来说简单多了。可以不必修改大量的文件系统和注册表 ACL，只需从 Power User 组删除“交互式用户”即可。随后的（非管理员）登录将成为用户组的成员，自动服从理想的访问控制策略。因此，为了保证 Windows 2000 系统的安全，保证应用程序符合 Windows 2000 的应用程序规范非常重要。这些应用程序将可以顺利地在（非管理员、非 Power User）用户环境下运行。

默认情况下，如果是 Windows 2000 Server 的全新安装，没有人是 Power User 组的成员。因此，登录到 Windows 2000 Server 上的终端用户（或服务账户）自动在向普通用户（非管理员、非 Power User）开放的安全环境下运行。如果需要与 Windows NT 4.0 向后兼容，那么管理员必须进行一些具体操作，把这些账户放置在 Power User 组，但这样会降低安全性。

最后，当工作站或服务器加入到一个域时，原先添加到 Windows NT 4.0 本地组的域组被添加到 Windows 2000 本地组。具体来讲，加入域之后域管理员和域用户分别添加到本地管理员和本地用户组。

6.6 默认的访问控制设置

默认的访问控制设置针对 Windows 2000 系统中的大量组件，包括注册表和文件系统以及用户权限和组成员身份。

在工作站、服务器和域控制器上的默认安全设置分别位于系统上的下列文件中：

- %windir%\security\template\basicws.inf
- %windir%\security\template\basicsv.inf
- %windir%\security\template\basicdc.inf

安全模板可用记事本打开，查看其设置。当然，管理员应该通过集成在 Microsoft 管理控制台（Microsoft Manage Console, MMC）中的“安全模板”这一管理单元来进行设置，我们将在后续章节中进行阐述。

Windows 2000 在全新安装或从 Windows 9x 的升级期间，在图形安装模式开始时就应用默认的安全设置。由于在图形化模式安装时已经开始应用了安全设置，所以对于在图形化模式安装阶段可以选择的可选组件（如 IIS 或终端服务器）并没有定义明确的安全设置。如果可选组件的安全与默认继承的安全不同，可选组件应当自行设置自己的安全。而在 Windows NT 系统升级的情况下不会对原有的安全设置进行修改。

6.5.1 文件系统和注册表的默认设置

首先，文件系统的默认安全设置只能在 Windows 2000 初始安装在 NTFS 分区的情况下才适用。

管理员、系统和创建者（所有者）对图形化模式安装开始时存在的所有文件系统和注册表对象具有完全的控制权限。用户仅对表 6-4 中所列出位置具有明确的写权限。

表 6-4 系统中默认具有写入权限的文件系统和注册表位置

对象	权限	备注
HKEY_Current_User	完全控制	注册表的用户部分
%UserProfile%	完全控制	用户的配置文件目录
所有用户\文档	修改	共享的文档位置
所有用户\应用程序数据	修改	共享的应用程序数据位置

%Windir%\Temp	同步、遍历、添加文件和添加子目录	每一机器的临时目录。这是对基于服务的应用程序的一个让步，这样就无须加载配置文件来获得模拟用户的每用户临时目录。
\（根目录）	安装期间未配置	安装期间未配置是因为 Windows 2000 ACL 继承模式将影响所有子对象，包括那些安装范围外的对象。

而用户对系统的其他部分只具有只读（或更低）访问权。值得注意的是，安装期间不定义访问根目录的权限。因此，将保持原先存在的访问根目录的任何权限。默认情况下，“ Format ”命令赋予 EveryOne 完全控制的权限，因此管理员应当根据其安全需要和需要运行的应用程序的要求来配置根目录。

安装不会改变访问根目录的权限，因为 Windows 2000 文件和文件夹的继承模式将试图循环地配置根目录的所有子目录。这可能会导致安装分区上的非基于 Windows 2000 的目录发生不应有的变化。

对于一些系统文件，推荐进行如表 6-5 所示的访问控制设置。

表 6-5 重要系统文件的推荐设置

文件	**基准权限**
%SystemDrive%\Boot.ini	Administrators：完全控制 System：完全控制
%SystemDrive%\Ntdetect.com	Administrators：完全控制 System：完全控制
%SystemDrive%\Ntldr	Administrators：完全控制 System：完全控制
%SystemDrive%\Io.sys	Administrators：完全控制 System：完全控制
%SystemDrive%\Autoexec.bat	Administrators：完全控制 System：完全控制 Authenticated Users：读取和执行、列出文件夹内容、读取
%systemdir%\config	Administrators：完全控制 System：完全控制 Authenticated Users：读取和执行、列出文件夹内容、读取
%SystemRoot%\system32*.exe	Administrators：完全控制

如果需要的话还可以为 Windows 2000 的注册表子项配置安全权限，方法如下：

（1） 选择“ 开始→运行 ”命令，运行 regedt32.exe 命令。

（2） 选择需要编辑的子键。

（3） 选择菜单栏上的“ 安全 ”→“ 权限 ”命令。

（4） 在“ 安全 ”选项卡中编辑需要更改的组的权限设置。

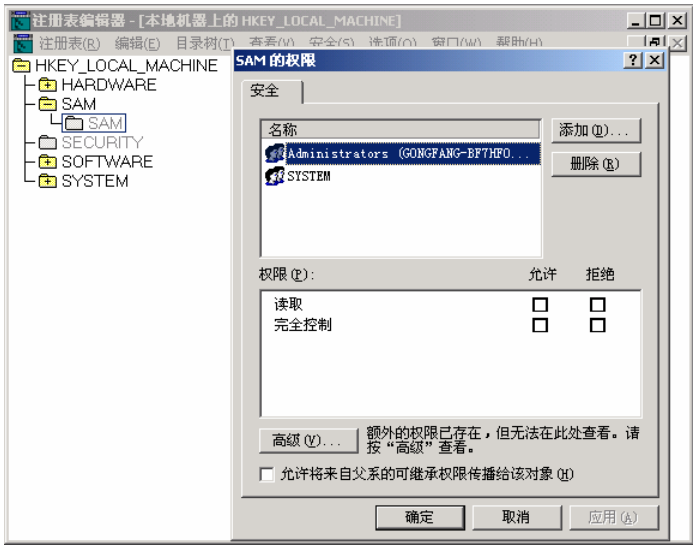

图 6-7 对注册表的访问控制进行设置

6.5.2 用户权利的默认指派

全新安装的工作站和成员服务器的默认用户权利指派如表 6-6 所示。它们仅在一个方面上有所不同，即“关闭系统”权限，在服务器上的用户默认情况下没有该权限。

表 6-6 默认的用户权利指派

用户权限	默认工作站	默认服务器
更换进程级令牌		
产生安全审核		
作为批量作业登录		
备份文件和目录	管理员、备份操作员	管理员、备份操作员
绕过遍历检查	管理员、备份操作员、Power User、用户和任何人	管理员、备份操作员、Power User、用户和任何人
创建页文件	管理员	管理员
创建永久共享对象		
创建令牌对象		
调试程序	管理员	管理员
提高日程安排优先级	管理员	管理员
增加配额	管理员	管理员
交互地登录	管理员、备份操作员、Power User、用户和来宾	管理员、备份操作员、Power User、用户和来宾
加载和卸载设备驱动程序	管理员	管理员
锁定内存内的页		
在域中添加工作站		
从网络访问这台计算机	管理员、备份操作员、Power User、用户和任何人	管理员、备份操作员、Power User、用户和任何人
描述单个进程	管理员和 Power User	管理员和 Power User
从远端系统的强制关机	管理员	管理员
还原文件和目录	管理员、备份操作员	管理员、备份操作员
管理审核和安全日志	管理员	管理员
作为一个服务登录		
关闭系统	管理员、备份操作员、Power User 和用户	管理员、备份操作员、Power User
修改固件环境变量	管理员	管理员
描述系统性能	管理员	管理员
更改系统时间	管理员和 Power User	管理员和 Power User
取得文件或其他对象的所有权	管理员	管理员
成为操作系统的一部分		

拒绝交互式登录		
拒绝成批登录		
拒绝服务登录		
拒绝网络登录		
从插接站移动计算机	用户、Power User 和管理员	用户、Power User 和管理员
将目录服务数据同步		
使计算机和用户账户接受委派		

在 Windows 2000 系统中，本地计算机可以根据自己的需要，通过“本地安全设置”中的“用户权利指派”管理单元来对用户权利进行设置，如图 6-8 所示。

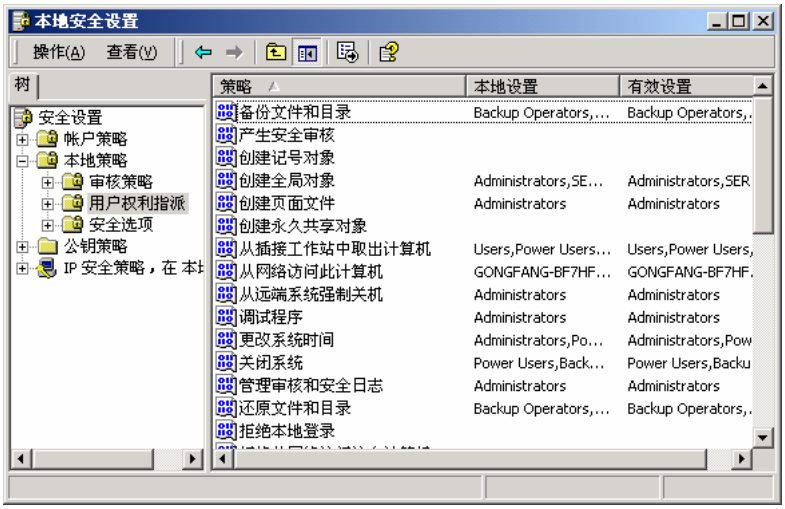

图 6-8 用户权利指派的设置