第 14 章 Windows Server 2003 安全

现在大多数的企业单位已经通过将 Intranet、Extranet 和 Internet 站点的合成扩展了传统意义上的局域网（LAN）的涵义，因此扩大了的系统的安全问题显得比从前更为重要。为了提供一个安全的计算环境，被 Microsoft 宣称的“迄今为止微软最强大的 Windows 服务器操作系统”的 Windows Server 2003 提供了一些重要的新安全特性，以及在 Windows 2000 Server 原有安全特性的基础上作了一些改进。

14.1 NTFS 和共享权限

在 Windows 2000 系统及早期版本中，默认的 NTFS 访问权限将“完全控制”授予了 Everyone 组。所以对于本地访问来说，整个文件系统就根本没有安全性可言。

但从 Windows XP Pro 系统开始，包括 Windows Server 2003，授予 Everyone 组的根目录 NTFS 权限只有读取和运行，且这些权限只对根文件夹有效。这也就是说，对于任何根目录下创建的子文件夹，Everyone 组都不能继承这些权限。对于安全性要求更高的系统文件夹，例如 Program Files 和 Windows 文件夹，Everyone 组也已经从 ACL 中排除出去，如图 14-1 所示。

图 14-1 文件或文件夹的 NTFS 权限（Windows Server 2003）

而 Users 组除了读取和运行之外，还能够在子文件夹下创建文件夹（可继承）和文件（根驱动器除外）。授予 System 账户的权限和本地 Administrators 组成员的权限仍未改变，它们仍拥有对根文件夹及其子文件夹的完全控制权限。CREATOR OWNER 仍被授予子文件夹及其包含的文件的完全控制权限，也就是允许用户全面管理他们自己创建的子文件夹。

在 Windows Server 2003 系统，对于新创建的共享资源，Everyone 现在只有读取的权限。另外，Everyone 组现在不再包含匿名 SID（安全标识符），进一步减少了未经授权访问文件系统的可能性。

若要查看文件或文件夹的 NTFS 权限，可以右击文件或文件夹，在弹出的菜单中选择“安全”命令，单击“高级”按钮，然后查看“有效权限”选项卡即可，如图 14-2 所示。现在就不用再猜测或进行复杂的分析来了解继承的以及直接授予的 NTFS 权限。但是，这个功能还不能涵盖共享权限。

图 14-2 文件或文件夹的有效权限（Windows Server 2003）

14.2 文件和文件夹的所有权

在 Windows Server 2003 系统中，不仅可以拥有文件系统对象（文件或文件夹）的所有者权限，而且还可以通过该文件或文件夹“高级安全设置”对话框的“所有者”选项卡将权限授予任何人，如图 14-3 所示。

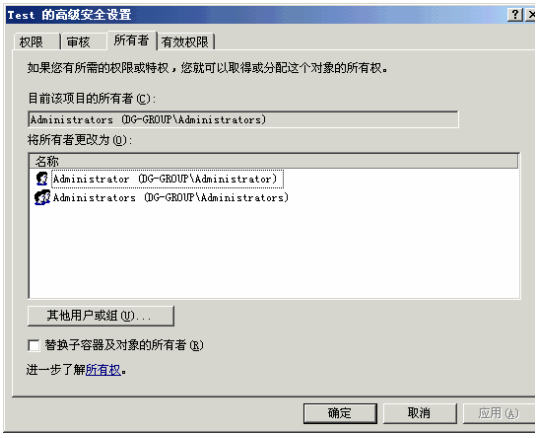

图 14-3 文件或文件夹的所有权（Windows Server 2003）

Windows 的磁盘配额是根据所有者属性计算的，授予其他人所有者权限的功能简化了磁盘配额的管理。例如，管理员应用户的要求创建了新的文件（例如复制一些文件，或安装新的软件），使得管理员成为新文件的所有者，即新文件占用的磁盘空间不计入用户的磁盘配额限制。以前，要解决这个问题必须经过繁琐的配置修改，或者必须使用第三方工具。现在 Windows Server 2003 直接在用户界面中提供了设置所有者的功能，这类有关磁盘配额的问题可以方便地解决了（对于使用 NTFS 文件系统的任何类型的操作系统都有效，包括 Windows NT 4.0、2000 和 XP Pro，只要修改是在 Windows Server 2003 上进行就可以了）。该功能（有效权限和授予所有者权限）对于从 Windows Server 2003 管理的活动目录对象也同样有效。

14.3 服务配置

在 Windows Server 2003 系统中，相对于 Windows 2000 在服务配置方面的安全性改进可分成两类。

- 启动类。几种最容易受到攻击的服务，比如 ClipBook（启用剪贴簿查看器储存信

息并与远程计算机共享）、Network DDE 和 Network DDE DSDM（前者的功能是为在同一台计算机或不同计算机上运行的程序提供动态数据交换的网络传输和安全；后者用于管理动态数据交换网络共享）、Telnet、WebClient（使基于 Windows 的程序能创建、访问和修改基于 Internet 的文件）等，默认情况下已经被禁止了。还有一些服务只有在必要时才启用，例如 Intersite Messaging（启用在运行 Windows Server 的站点间交换消息）只有在域控制器提升时才启用，Routing and Remote Access Service（为网络上的客户端和服务器启用多重协议——LAN 到 LAN、LAN 到 WAN、虚拟专用网络和网络地址转换路由服务）只有在配置 Windows Server 2003 作为路由器、按需拨号的服务器、远程访问服务器时才启用。

- 运行在 Local System 安全上下文之下的服务。Local System 具有不受限制的本地特权。现在，在许多情况下，Local System 被 Local Service 或 Network Service 账户取代，这两个账户都只有稍高于授权用户的特权。正如其名字所暗示的，Local Service 账户用于本地系统的服务，它类似于已验证的用户账户的特殊内置账户。Local Service 账户对于资源和对象的访问级别与 Users 组的成员相同。如果单个服务或进程受到危害，则通过上述受限制的访问将有助于保护系统。以 Local Service 账户运行的服务作为空会话，而且不使用任何凭据访问网络资源。相对地，Network Service 则被用于必须要有网络访问的服务，它对于资源和对象的访问级别也与 Users 组的成员相同，以 Network Service 账户来运行的服务将使用计算机账户的凭据来访问网络资源。

14.4 身份验证

Windows Server 2003 在身份验证方面的增强涵盖了基于本地系统的身份验证和基于活动目录域的身份验证。

在本地系统验证方面，默认的设置限制不带密码的本地账户只能用于控制台。这就是说，不带密码的账户将不能再用于远程系统的访问，例如驱动器映射和远程桌面/远程协助连接等。

活动目录验证的变化突出显示在跨越林的信任方面。跨越林的信任功能允许在林的根域之间创建基于 Kerberos 的信任关系（要求两个林都运行在 Windows Server 2003 功能级别上）。在 Windows Server 2003 林中，管理员可创建一个林，将单个林范围外的双向传递性扩展到另外一个 Windows Server 2003 林中。在 Windows Server 2003 林中，这种跨越将两个断开连接的 Windows Server 2003 林链接起来建立单向或双向可传递信任关系。双向林信任用于在两个林中的每个域之间建立可传递的信任关系。

林信任具有许多优点：

- 通过减少共享资源所需的外部信任数，使得跨越两个 Windows Server 2003 林的资源的管理得以简化。
- 每个林中每个域之间的完全的双向信任关系。
- 使用跨越两个林的用户主体名称（UPN）身份验证。
- 使用 Kerberos v5 和 NTLM 身份验证协议，提高了林之间传递的授权数据的可信度。
- 灵活的管理。每个林的管理任务可以是惟一的。

林信任只能在两个林之间创建，不能隐式扩展到第三个林。也就是说，如果在林 1 和林 2 之间创建了一个林信任，在林 2 和林 3 之间也创建了一个林信任，则林 1 和林 3 之间没有隐式信任关系。

需要注意的是：在 Windows 2000 林中，若要一个林中的用户可以访问另一个林中的资

源，管理员可在两个域之间创建外部信任关系。外部信任可以是单向或双向的非传递信任，因此限制了信任路径扩展到其他域的能力。但在 Windows Server 2003 活动目录中，默认情况下，新的外部信任和林信任强制 SID 筛选。SID 筛选用于防止可能试图将提升的用户权限授予其他用户账户的恶意用户的攻击。强制 SID 筛选不会阻止同一林中的域迁移使用 SID 历史记录，而且也不会影响全局组的访问控制策略。

在默认配置下，身份验证是在林的级别上进行的，来自其他林的责任人将被授予与本地用户和计算机同样的访问能力。但无论是谁，都受到设置在资源上的权限的约束。

如果上述默认配置不能满足要求，则可以配置选择性验证，不过这需要具有 Windows Server 2003 的林功能级别。在这种配置方式中，管理员可以指定哪些来自其他林的用户或组允许通过验证，以及选择本地林的哪些资源可用来执行验证。具体设置分两步进行。

第一步，授予来自其他林的责任人允许验证的权限。例如，假设有两个 Windows Server 2003 功能级别的林 Forest A 和 Forest B，两者之间有信任关系。Forest A 中 Domain A 域的 User A 用户需要访问 Forest B 中 Domain B 域 Server B 服务器的 Share B 共享资源。要达到这个目标，必须按如下方式操作。

（1）Domain A 的管理员在 Domain A 域中创建一个全局组（例如 Group A），其中包含成员 User A。虽然可以直接授予 User A 适当的权限（这种方式的优点之一是透明），但如果用户数量较多，直接配置各个用户的话效率就很低了。

（2）启动 Active Directory 用户和计算机管理器，找到 Domain B，再找到 Server B，双击 Server B 的图标，打开它的属性对话框。

（3）转到安全设置选项卡，将 Domain A Group A 加入到对话框上方的清单。在窗口下方，选中“允许验证”和“读取”权限的“允许”选项。第一步的设置到此为止，现在已经允许 Domain A Group A 的成员访问 Domain B Server B 时执行验证。

第二步，只要把 Server B 服务器 Share B 共享资源上适当的权限授予 Domain A Group A 全局组（或者，也可以将 Domain A Group A 全局组加入到 Domain B 域本地组，然后对本地组授权）。

14.5 IIS 6.0

Windows Server 2003 系统中的 IIS（Internet Information Server, Internet 信息服务器）的版本为 6.0。IIS 6.0 远比 Windows NT 中的 IIS 4.x 或 Windows 2000 中的 IIS 5.x 安全，它拥有很多新的功能特性，能够大大提高 Web 基础结构的安全性。此外，在默认状况下，IIS 6.0 即处于“锁定”状态，同时具有最为可靠的超时设置和内容限制。

- 锁定服务器：IIS 6.0 在安全性方面进行了很大的加强。为了减少系统向外界暴露的攻击表面积，IIS 6.0 默认情况下不会安装在 Windows Server 2003 之中，管理员必须明确地选择该组件并安装它。IIS 6.0 默认处于锁定状态下，并仅仅能够为用户提供静态内容。通过使用 Web 服务扩展节点，Web 站点的管理员可以根据组织的特殊需要，启用或禁用某些 IIS 功能。
- Web 服务扩展列表：默认情况下的 IIS 安装不会编译、执行或者提交任何动态页面。为了向用户提供这些文件，管理员必须在 Web 服务扩展列表中添加每个允许提交的文件扩展名。这种做法可以防止某些人调用一些不够安全的动态页面。
- 默认的低权限账户：所有 IIS 6.0 的工作进程默认情况下都使用“网络服务”用户账户运行，这个在 Windows Server 2003 中新增加的账户类型是一种拥有有限操作系统权限的内置账户。所有的 ASP 内置功能都使用低权限账户（匿名用户）在系统中运行。

- 授权：IIS 6.0 对 Windows Server 2003 内置的新的授权框架进行了进一步的扩展。此外，Web 应用程序可以使用 URL 授权，以及授权管理器（Authorization Manager）对用户的访问加以控制。现在，受约束的委派授权使得域管理员只能向特定的计算机和服务进行委派操作。