第 9 章　应用服务的安全

9.1　Internet 信息服务（IIS）

9.1.1　IIS 简介

IIS（Internet Information Server）5.0 是 Windows 2000 系统所带的 Internet 服务程序包，它包含了 Web、FTP、SMTP 以及 Index Server 等众多组件。无论是创建一个 Internet 外部站点，还是构造一个 Intranet 内部应用，使用 IIS 5.0 都是很好的选择。同时，如何保障 IIS 5.0 安全稳定运行、内容发布正确可靠，是系统管理员必须高度重视的问题。

IIS 中一个比较重要的组件就是 Web 服务器。Web 服务器的功能是接受 Web 浏览器请求并给它们提供内容服务。这些内容包括 HTML 页、图像、声音和可执行文件，以及要在 Web 浏览器上运行的活动内容（Active Content）等。Web 服务器还实现了 HTTP（超文本传输协议），因此又被称做 HTTP 服务器。IIS 5.0 还实现了对 HTTP 1.1 的 WebDAV（Web Distributed Versioning and Authoring, Web 分布式创作与版本控制）扩展，允许 Web 浏览器把 Web 资源当作文件系统来处理，来支持用户在 Web 服务器中修改、删除和上传文件。IIS 中还包括 FTP 服务器组件，但只是简单的允许 FTP 客户上传和下载静态文件。

9.1.2　IIS 的安全需求

1. 网络连接的安全需求

一般地，可以把下列网络连接的安全需求用于每个目录。

- 机密性 :保证服务器与其客户之间的部分或全部数据交换对于窃听者来说是不可访问的。
- 完整性：保证主动的网络攻击不能篡改数据。
- 授权访问：保证一些服务器内容只对已授权用户是可用的。

2. 服务器自身的安全需求

服务器安全需求与 Web 服务器以及为页面提供服务的所有其他文件服务器有关。

- 授权访问：保证对服务器的所有访问都是经过授权的。特别地，要保证运行 IIS 的服务器没有一个可使未经授权的访问进入 Windows 2000 主机的额外入口点。
- 机密性与完整性：保证一些 Web 内容、用户数据与配置信息是保密的和正确的。
- 有效性：保证灾难后服务的连续性，并确保恶意行为不会影响服务的有效性。也可以在其他地方解决可靠性和非恶意干扰等问题。

9.1.3　IIS 安全特性概述

为了提高安全性，IIS 5.0 改进了自身的安全验证方法，加强了安全通信功能，并与 Kerberos v5 验证协议完全集成。

- 在安全验证方面，IIS 5.0 用分级验证，能够安全、可靠地通过代理服务器和防火墙验证用户，此外使用 Anonymous 和 Windows 验证。
- 在安全通信方面，IIS 5.0 的安全套接层（SSL）3.0 和传输层安全（TLS）为客户和服务器之间的信息交换提供了安全的方式。此外，SSL 3.0 和 TLS 还为服务器提供了验证在用户登录到服务器之前的客户的方式。在 IIS 5.0 中，ISAPI 和 ASP 都得到客户证书，从而程序员可以通过他们的站点跟踪用户。同时， IIS 5.0 也可以将

客户证书映射到 Windows 用户账号，从而使管理员可以根据客户证书控制对系统资源的访问。服务器加密（SGC）是 SSL 的扩展，它允许长达 128 位的数据加密。不过，要使用 SGC 还需要特殊的 SGC 证书才行。

- IIS 与 Kerberos v5 验证协议完全集成，使已经连接并运行 Windows 的不同计算机之间能够传送证书。另外，Windows 证书管理器提供允许存储、备份和配置服务器证书的单入口点。

此外，Windows 2000 系统所提供的众多新安全特性也有利于 IIS 服务器的运行。

- 继承权限：针对目录或注册表键而指定的自由访问控制列表（DACL）可以被其内容所继承，因此在 Windows 2000 下使用 DACL 就更为容易而且更少出错。
- 安全模板：在 Windows 2000 系统中，包括用户权限、文件系统与注册表 DACL 和受限组成员身份在内的大量安全设置都已经收集到了安全模板文件中。可以利用这些模板来增强机器的本地安全策略，也可以测试计算机的当前配置与模板之间的一致性。
- 活动目录的目录服务：Windows 2000 域之间双向可传递的信任关系允许活动目录可以用作该组织机构的单一账户数据库。只有加入活动目录的域森林，运行 IIS 的服务器才可以使用该数据库自动对用户进行身份验证。
- 证书服务：Windows 2000 提供了复杂的公钥基础结构（PKI）。因此，域用户可以自动获取证书并用来访问运行于 IIS 服务器上的资源。活动目录会自动把证书映射到用户账户。
- Kerberos 身份验证：Windows 2000 中新出现的这个协议可用来提高运行 IIS 服务器的效率。与 NTLM 相反，Kerberos 对每个用户进行身份验证时不需要连接域控制器。Kerberos 还支持用户凭证的多重委派，让系统可以更加简单清晰地实现对后端数据库和其他资源的访问。
- IPSec：此协议提供了机密性、完整性以及 IP 层的主机间身份验证服务。可以在 Intranet 或 Internet 上实现 IPSec 以提供 VPN（虚拟专用网络）。在 VPN 上提供的 IIS 服务，无须进一步配置就可以透明地享受到那些安全服务所带来的好处。
- 高强度加密包。

9.1.4 IIS 的身份验证

IIS 身份验证机制（如图 9-1 所示）可以随意要求访问 Web 与 FTP 资源的用户验证他们自己的身份，并且始终将他们映射到 Windows 用户账户。然后，IIS 模拟成 Windows 用户访问它将服务的内容。Web 服务器访问权限、文件系统权限与客户主机的网络地址或主机名，都服务于更进一步的访问控制。访问控制机制与身份验证机制结合在一起，来决定哪个客户可以访问哪些文件。

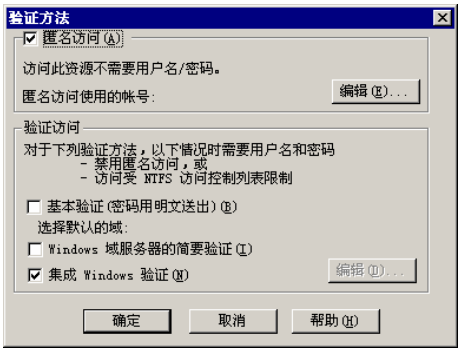

图 9-1 IIS 的身份验证机制

1. 匿名身份验证

匿名身份验证意味着根本就没有身份验证。在访问一个给匿名身份验证配置的资源时，IIS 就要把用户映射到本地账户，默认为 IUSR_Computername（其中，Computername 是运行 IIS 的计算机名称）。

IIS 默认配置为口令同步，也就是说 IIS 控制着账户口令。它在这种模式下执行网络登录来模拟账户，因此账户需要拥有“ 从网络访问计算机 ”的权限。如果关闭口令同步，IIS 就进行默认为交互式的明文登录，因而它需要拥有“ 本地登录 ”的权限。另外，也可以重新定义明文登录类型。

在创建 IUSR_Computername 时，就赋予了它上述权力并使它成为 Guests 组的成员，以限制它对文件系统的访问。如果使用其他账户进行匿名访问，就必须重复进行这些设置。

2. 基本身份验证

基本身份验证是收集用户名与口令信息的标准机制。Web 浏览器提示用户输入用户名和口令，并把它们传送到 IIS 进行加密。IIS 使用这些信息来模拟 Windows 2000 用户。如果服务器拒绝接受登录信息，浏览器就会反复提示用户直到用户关闭对话框为止。用户名可以选择在域\用户名（domain\username）格式中包括域名。

基本身份验证的优势在于它是 HTTP 标准的一部分，因而在大多数浏览器上已经实现。但是，它也有严重的不足之处，即把登录信息泄漏给了窃听者。如果需要非常严格的安全需求，就可能只在安全网络上才使用这种机制，或者使用 SSL/TLS 来保护网络连接。

基本身份验证也称作默认为交互式的明文登录，因为它需要拥有“ 本地登录 ”权限。

3. 域服务器的简要身份验证

简要身份验证（也成为摘要身份验证）是一种质询—应答（Challenge—Response）机制，它以非明文的传输形式提供关于用户口令的信息。可以在 IETF 的 RFC2069 文档中找到它的定义。

简要身份验证的工作过程如下：

（1）服务器向浏览器发送信息（质询）。

（2）浏览器提示用户输入与基本身份验证相关的用户名和口令。

（3）浏览器计算口令和质询信息的散列值，生成摘要，再把摘要与质询一起发送到服务器。

（4）服务器计算质询与用户口令的备份的散列值，然后把所得到的摘要与所接受到的摘要进行比较。

（5）如果两个摘要相同，则身份验证成功。

为了防止攻击者对应答信息进行重放，质询必须包括客户机的身份标识、域及时间。

简要身份验证是 HTTP 1.1 的一个新增特性，并不是所有的浏览器都支持这一特性。如果服务器要求简要身份验证而浏览器不支持它，那么身份验证就会失败，并且可能会反复提示用户输入用户名与口令。

简要身份验证要求用户在 Windows 2000 域中具有账户，而且还要求 Windows 2000 的域控制器以可逆加密的形式存储那些口令。这是因为在上述的散列值计算过程中，Web 浏览器采用了口令的纯文本形式，并且以计算过散列值的口令一般都不保存在域控制器里。因此，如果选择了摘要身份验证，就应该把严格的安全需求加入域控制器以保护可逆的加密口令。此外，还需要强制用户改变它们的口令，从而使可逆加密口令更有效。

IIS 使用简要身份验证机制来模拟通过网络进行登录的用户。因此，用户必须要拥有“ 从

网络访问计算机 ” 的权限。

该身份验证协议可以在代理服务器和防火墙中使用，并且对 WebDAV 也有效。

4. 集成 Windows 身份验证

集成 Windows 身份验证是由 Kerberos v5 与质询—应答身份验证协议组成的，这些机制一般用于 Windows 网络的身份验证，这里它们是在 HTTP 上实现的。与简要身份验证相似，该协议也以非明文的传输形式提供关于用户口令的信息，而且不用任何参数来对集成 Windows 身份验证进行配置。

集成 Windows 身份验证处理过程如下：

（1）如果用户已经登录到某个域上，Web 浏览器就会试图采用其中的用户凭证。

（2）如果由于用户没有登录或登录到的是另一个域，而使上一步失败的话，Web 浏览器就会提示输入用户名和口令，直到用户输入有效账户或关闭对话框为止。

尽管集成 Windows 身份验证是安全的，但它也具有下列局限性：

- 对 Web 浏览器的版本有限制。如只有 Internet Explorer 2 以上的版本才可用，Kerberos 协议只在 Internet Explorer 5.0 以上版本才可用。
- 不能在 HTTP 代理服务器上工作。
- 只有在已经加入到 Windows 2000 域的客户主机中，Kerberos 身份验证才是可用的。

因此，集成 Windows 身份验证最适合 Intranet 环境。

IIS 也使用该身份验证机制来模拟通过网络进行登录的用户，因此用户账户必须拥有“ 从网络访问计算机 ” 的权限。

5. 证书的使用

IIS 可以使用证书来验证用户的身份，并且可以选择把这些用户映射到 Windows 账户。

（1）证书身份验证

IIS 实现了 SSL/TLS 协议，这个协议向 Web 浏览器与 Web 服务器链接提供了机密性、完整性以及相互身份验证等服务。

最初，用户需要从 Web 服务器信任的证书颁发机构（CA）那里获取证书。然后，在 Web 服务器需要客户身份验证时，浏览器就提供证书并且使用质询—应答协议（SSL/TLS 协议的一部分）来证明它持有私钥。可以将每个证书映射到相互分离的账户，或者将其中的一部分映射到单一账户。这种账户映射不考虑其他 IIS 身份验证机制的映射，但可以与它们一起并行使用。

（2）证书映射

在身份验证之后，就可以采用很多方法将证书映射到 Windows 账户，如图 9-2 所示。

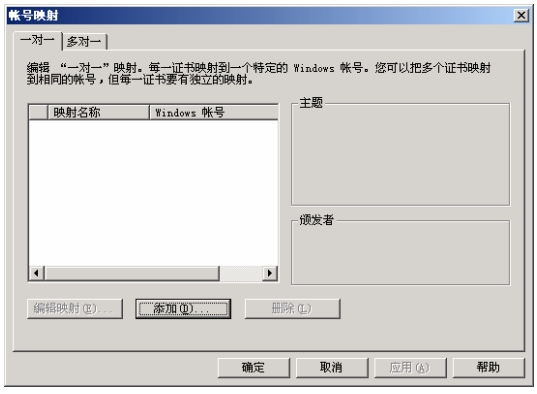

图 9-2　IIS 中的客户证书映射

在 IIS 中可以定义下列证书映射。

- 一对一映射：证书一个对一个地映射到账户。可以手工输入证书文件和与其相关的由用户名与口令组成的 Windows 账户。Web 浏览器提供的证书要与保存在 IIS 并将它映射到账户的证书进行一位一位（bit-for-bit）的比较。此过程优先下面的多对一映射。
- 多对一映射：也叫做通配符匹配。根据一定规则将证书映射到静态账户中。这些规则将简单地匹配 Web 用户证书中的字段，如拥有者名称、拥有者组织或发行者名称等，然后将它映射到预定义好的那个账户。

（3）身份验证与映射方案

- 证书身份验证、证书账户映射、SSL 及常规的 IIS 身份验证机制可以结合起来向管理员提供很多身份验证选项。下面就是一些常用的组合方式：
- 请求证书身份验证并启用映射：如果启用其他机制，它们也必须要让用户成功地通过身份验证。但是这种方案却会因为证书映射而忽略了它们的账户映射。
- 启用证书身份验证并启用映射：除了常规的身份验证机制把没有证书的用户映射到 Windows 账户外，这种方案的工作原理与上一种方案相类似。
- 启用证书身份验证但禁用映射：证书身份验证将会保证可信授权机构已经向用户发行了证书，而常规机制还要将此用户映射到 Windows 账户。

6. FTP 的身份验证

FTP 协议总是要提示输入用户名和口令。身份验证设置决定了可以接受什么样的用户名，但是不能对目录和文件进行身份验证，如图 9-3 所示。

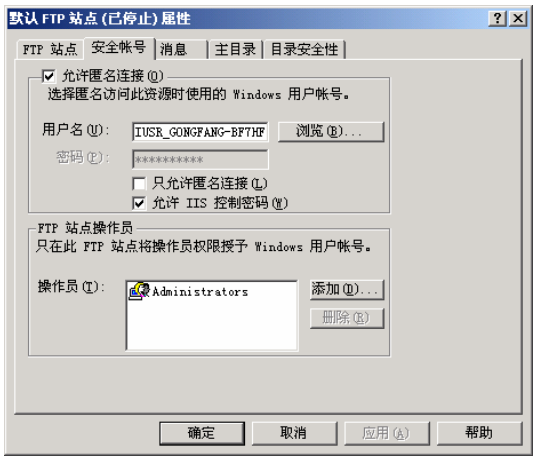

图 9-3　FTP 的身份验证

- 匿名 FTP 身份验证与 Web 的匿名身份验证相类似。用户可以匿名登录或通过某个口令来使用 FTP 服务。出于统计的目的，在实际情况中常常使用电子邮件地址作为 FTP 登录的口令。
- 基本 FTP 身份验证与 Web 的基本身份验证也是类似的。在提示登录时，用户可以输入用户名或者域\用户名。如果 IIS 在域控制器上运行，那么这两种格式的用户名是等效的。在独立服务器或成员服务器上，第一种格式的名称与本地账户相对应。

FTP 在网络上传输的数据都是以明文形式存在的，包括登录用户名和口令。而且，IIS 5.0 和常用的 FTP 客户程序都没有为 FTP 服务而支持 SSL/TLS 协议。所以，如果要求安全性，应该考虑使用 Web 服务来提供经过验证的资源访问。

9.1.5　IIS 的访问控制

IIS 的访问控制机制根据身份验证过程中的输入来确定，哪个客户能够访问什么文件。访问控制的过滤器可以是 Web 服务器的权限、文件系统（NTFS）的权限和客户端的 IP 地址或域名。

1. 访问控制流程

IIS 的访问控制与身份验证按照下面的方式结合在一起，如图 9-4 所示。

（1）客户从 IIS 请求 Web 或者 FTP 资源。

（2）IIS 根据身份验证的配置来要求还是不要求客户验证自己的身份。

（3）IIS 检查客户端主机的 IP 地址和 DNS 名称（仅对 Web 而言）。失败的 Web 请求会返回“访问被禁止”（403 Access Forbidden）的消息。

（4）IIS 检查在身份验证处理过程中规定的用户账户是否有效，口令是否正确。如果结果为否，则在 Web 请求的情况下返回“访问被禁止”的消息。

（5）IIS 检查 Web 或者 FTP 访问权限与客户请求的访问类型（读、写或其他访问）是否兼容。如果结果为否，则在 Web 请求的情况下返回“访问被禁止”的消息。

（6）IIS 调用由管理员指定的任何第三方安全模块。

（7）IIS 检查资源的 NTFS 权限是否与请求的访问类型是否兼容。如果结果为否，则在 Web 请求的情况下返回“访问被拒绝”（401 Access Denied）的消息。

（8）若上述检查全部都成功了，IIS 则开始执行客户请求。

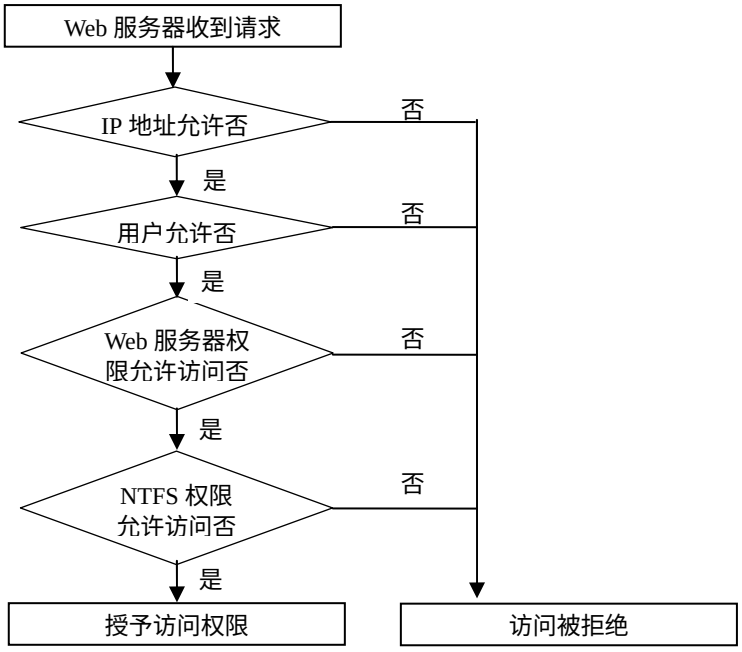

图 9-4　IIS 的访问控制流程

2. 网络地址的访问控制

管理员可以配置 IIS 的“IP 地址及域名限制”，使得特定的 IP 地址、处于某个范围内的 IP 地址或者用 FQDN（完全合格域名）描述的主机及 DNS 子域授权还是拒绝访问 IIS 服务，如图 9-5 所示。

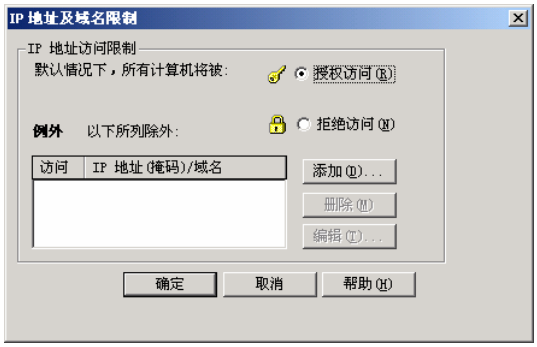

图 9-5 IIS 的 IP 地址及域名限制

有两种方式来使用 IP 地址和域名限制来控制对站点的访问：

- 拒绝对所有地址及域名的访问，除了那些被显式授权访问权限的某些地址。这种方式提供了更好的安全性，但是需要更多的维护工作。
- 允许对所有地址及域名的访问，除了那些被显式拒绝访问的某些地址。这种方式更适合对安全性要求较低但更易管理的情况。

3. IIS 服务器权限

Web 服务器与 FTP 服务器的权限定义了对每个资源允许执行的操作，并且被应用于所有的客户，而与文件系统基本的 NTFS 权限无关。如果这两种权限不一致，就采用最严格的限制。

对于大多数情况，Web 是只读的介质，但还可以使用 IIS 权限来指定是否允许用户在站点上执行脚本或程序，以及在某些特殊情况下，用户是否可以向 Web 服务器写入数据，如图 9-6 所示。FTP 站点通常都支持读取和写入两种访问方式，但是可以使用 IIS 权限将 FTP 限制为只读访问。

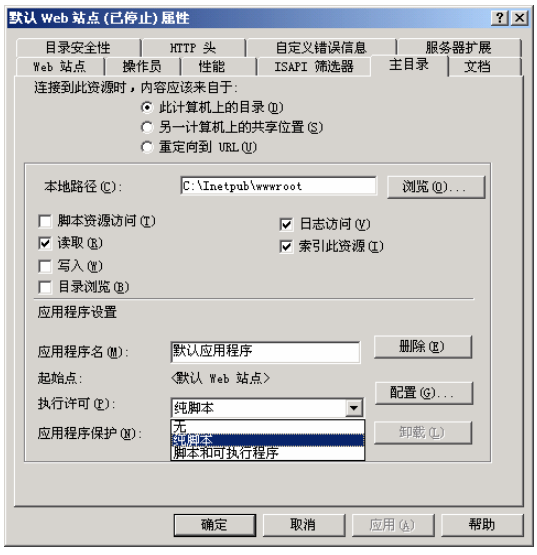

图 9-6 IIS 服务器的权限

与 NTFS 相似，可以在 IIS 站点层次结构的任何级别设置权限：站点级、虚拟目录级或是目录级。同样与 NTFS 类似，在特定级别设置的权限会被其下面的子对象所继承。

表 9-1 列出了 IIS 服务器的基本权限。

表 9-1 IIS 服务器基本权限

权限	说明

脚本资源访问	当设置了读取或写入权限时，是用户可以访问脚本的源代码
读取	使用户可以读取或下载文件或子目录以及与它们关联的属性
写入	使用户可以上载文件及与文件关联的属性，或更改启用了写入的文件的内容
目录浏览	使用户可以查看文件及目录的超文本形式的列表，但不包括虚拟目录

除上述这些权限之外，在应用程序的“执行许可”中还可设置：只允许用户执行脚本、允许用户执行脚本及可执行程序，还是两者都不允许。

4. 权限向导（Permission Wizard）

权限向导允许将对身份验证、Web/FTP 访问权限、网络地址访问控制以及 NTFS 文件系统权限预先定义的模板，应用于任何 Web 站点、FTP 站点或目录。管理员也可以使用此向导来完成从父容器（主要的服务、站点或目录）到子容器（站点或目录）的属性继承，如图 9-7 所示。

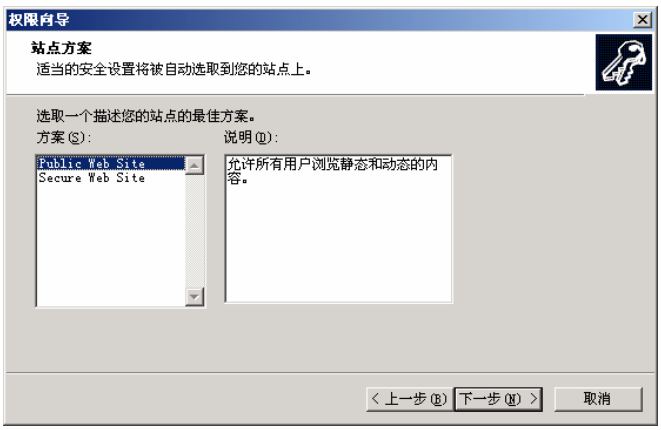

图 9-7　预定义的站点安全设置模板

预定义的 Web/FTP 站点模板如下。

- Public Web Site（公开 Web 站点）：这个模板适用于在 Intranet 或 Internet 上的公开访问。它将身份验证设置为匿名身份验证，Web 权限设置为读取和脚本资源访问，NTFS 权限设置为对 Administrators 组是完全访问以及对 Everyone 组是读取、读取且执行和显示文件夹内容。
- Secure Web Site（安全 Web 站点）：这个模板适用于在 Intranet 或 Internet 上的保密访问。它将身份验证设置为基本身份验证、简要身份验证和集成 Windows 身份验证。其他的设置与“公开 Web 站点”相同。
- Public FTP Site（公开 FTP 站点）：它将身份验证仅设置为匿名身份验证，FTP 权限设置为读取，NTFS 权限设置为对 Administrators 组是完全访问以及对 Everyone 组是读取。

9.1.6　IIS 的应用程序保护和应用程序权限

1. 应用程序保护

IIS 提供了将应用程序划分为不同进程的能力，这被称之为应用程序保护。IIS 提供了如下三种应用程序保护模式：

- 低（IIS 进程）。应用程序的进程与 IIS 进程相同，称之为进程内扩展。
- 中（公用的）。应用程序的进程与 IIS 进程合并，但与之分开，称之为进程外扩展。
- 高（独立的）。应用程序独立于 IIS 进程，完全与之分开，称之为进程外扩展。

这些不同的选项提供了一种防止应用程序彼此干扰或导致 IIS 服务器崩溃的方法，默认的保护级别是“中（公用的）”。

在系统安装 IIS 服务的时候，将创建两个账号：IUSR_ComputerName 和 IWAM_ComputerName，其中 ComputerName 是安装 IIS 的计算机名称。在使用低级应用程序保护能力的时候，IIS 将使用 IUSR_ComputerName 账号来响应匿名请求。通常，IIS 在与 IIS 服务器相同的进程空间内运行 Web 应用程序，这被称为进程内扩展。这意味着性能糟糕的应用程序可能导致 IIS 服务器或 Web 服务崩溃，甚至可能被恶意用户成功缓冲区溢出攻击之后获取系统（SYSTEM）权限，从而完全控制整个系统。

IIS 还为中级和高级应用程序保护能力的进程外扩展提供了支持，它们在 IWAM_Computer 账号的环境下运行。进程外扩展在 Microsoft 事务服务器（Microsoft Transaction Server, MTS）创建的进程中运行。因此，性能糟糕的进程外扩展无法使 IIS 服务器或 Web 服务崩溃，而只能使 MTX.exe 进程崩溃。不过，这两种扩展类型的成功缓冲区溢出攻击也存在相同的潜在安全风险，这是因为 IIS 服务进程和 MTX 进程都使用 LocalSystem 账号运行，并且通过完成模拟工作分别获得与 IUSR_ComputerName 和 IWAM_ComputerName 有关的权限。

2. 应用程序权限

IIS 还提供了限制应用程序在目录中所拥有的权限的能力，这些权限被称为执行权限。在 IIS 中有以下三种类型的应用程序权限。

- 无。不允许运行任何脚本和应用程序。
- 纯脚本。允许运行能够映射到一个脚本引擎的应用程序（如 Web 主目录及其所有子目录中的 asp 脚本、Perl 脚本或 JavaScript）。
- 脚本和可执行程序。允许运行任何应用程序。

“纯脚本”比“脚本和可执行程序”的限制更多，因此也更安全。

9.1.7 IIS 的安全配置

1. 安全配置 Windows 2000

（1）安装最新的补丁包

Windows 2000 Service Pack 提供了对 Windows 2000 系统的最新升级。这些升级汇集了对以下领域的修补：应用程序兼容性、操作系统可靠性、安全性和安装过程。每一个 Service Pack 包含以前版本的所有升级。

在 Windows 2000 的 SP3 中已经包括了 Automatic Updates（自动升级）服务，该服务能够在重要的 Windows 2000 修补程序发布之时向用户发出通知。Automatic Updates 是一种有预见性的下载服务，可以自动下载和安装 Windows 升级补丁，例如重要的操作系统修补和 Windows 安全性升级补丁。

针对最新的安全漏洞需要安装 HotFixes（热补丁）。需要注意的是，建议在系统需要的时候才安装相应的 HotFix。因为，并不是每个服务器都需要所有的 HotFix，其中有一些 Hotfix 修复的漏洞只存在于某些特定配置中。如果情况不是非常严重，可以等到新的 Service Pack 整个推出之后再安装。

可以使用 HFNetChk 这个命令行工具来帮助管理员从一个中心位置来检查网络中所有机器的补丁状态。（除了 Windows 系统，该工具还可以检测 Microsoft 其他产品的补丁状态，如 SQL Server 2000、Internet Explorer 等）。

此外，还可以使用 Microsoft Baseline Security Analyzer（MBSA）来监测系统的安全性。

Microsoft 基线安全分析器（MBSA）是一个由 Microsoft 开发的图形和命令行接口，它能从本地或远程执行系统扫描，评估特定 Microsoft 产品中任何遗漏的修补程序和弱点。

（2）安装微软高级加密包

Windows 2000 高度加密包是一个可以从美国出口到世界各地的软件（美国禁运的地方除外）。一些国家对进出口或加密产品的使用有部分的限制。对于中国用户来说，可以使用和下载该加密包。

安装微软高级加密包（Microsoft High Encryption Pack），可以将服务器达到最高水平的加密（128 位）。默认状态下，服务器软件的加密状态处于较低级别，必须手工将其配置为 128 位加密。而且，这项工作应该在创建账号和组之前进行，来保证在服务器上创建的所有项目都是 128 位加密级别的。

（3）对系统服务的启动方式重新进行规划

默认状态下，许多服务都随系统的启动而启动。但由于有些服务因为启动账号身份的权限过大，有可能埋下安全隐患，还有某些不必要的服务可能造成系统的漏洞，例如 FTP，SMTP 等，因此必须对所有服务的启动方式进行重新规划。

规划的原则应该是：除非绝对必要，就关闭该服务。

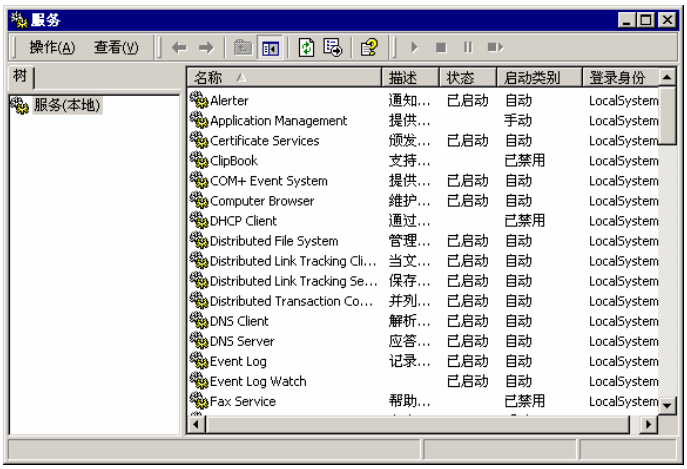

图 9-8 规划系统服务

可根据表 9-2 的建议来对系统的服务进行设置（没有在该表中列举的则表示保持默认的设置）。

表 9-2 系统服务的建议设置

名称	默认启动类别	建议启动类别
Alerter	自动	已禁用或手动
ClipBook	手动	已禁用
DHCP Client	自动	已禁用
Distributed File System	自动	手动
Distributed Link Tracking Client	自动	手动
Distributed Transaction Coordinator	自动	手动
Fax Service	手动	已禁用
Indexing Service	手动	已禁用
Internet Connection Sharing	手动	已禁用
Messenger	自动	手动或已禁用
Net Logon	手动	手动或已禁用
NetMeeting Remote Desktop Sharing	手动	已禁用

Network DDE	手动	已禁用
Network DDE DSDM	手动	已禁用
Remote Registry Service	自动	手动
Smart Card Helper	手动	已禁用
Telephony	手动	手动或已禁用
Uninterruptible Power Supply	手动	已禁用

（4）强化对 SAM 数据库的保护

SAM 数据库就是系统账户数据库，默认状态下，SAM 是用本地存储的启动关键字来加密的，这个关键字中包含一个杂乱信息代码，它在启动过程中被处理进而将账户数据库解密并存储在内存中，从而被系统访问。加密关键字的默认存储地点可以用 Windows 2000 命令行工具 syskey.exe 来修改，其运行时的界面如图 9-9 所示。

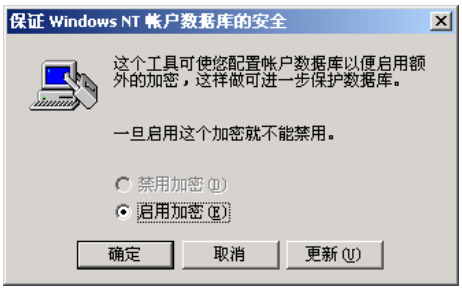

图 9-9 使用 syskey 强化 SAM 数据库的保护

使用 syskey 加密系统账户数据库时可以选择的密钥选项如表 9-3 所示。

表 9-3 Syskey 系统密钥选项

模式	系统密钥选项	安全等级	描述
模式 1	系统生成密码，本地存储启动密钥	安全	使用计算机生成的随机密钥作为系统密钥，并且将该密钥的加密版本存储到本地计算机中。该选项提供了对注册表中密码信息的强大加密，并且使得用户无须输入管理员密码或者插入软盘就能够重新启动计算机。
模式 2	管理员创建密码。使用密码启动	更安全	使用计算机生成的随机密钥作为系统密钥，并且将该密钥的加密版本存储到本地计算机中。该密钥还受到由管理员所选择的一个密码的保护。当计算机处于最初启动时，会提示用户输入系统密钥。该系统密钥密码不存储在计算机的任何位置。
模式 3	系统生成密码，在软盘上存储启动密码	最安全	使用计算机生成的一个随机密钥，并且存储到软盘中。系统启动时，需要包含存储该随机密钥的软盘，并且应当根据启动提示插入到软驱中。该系统密钥不存储在计算机的任何位置。

为了保护 SAM 数据库的安全，管理员可以使用这个工具将杂乱信息代码转移到软盘上，并注意为这个软盘制作多个备份，放置到一个非常安全的地方。如果这个软盘丢失或损坏，就无法重新启动服务器了，因为再没有其他办法可以对用户账户和口令数据库进行解密。

（5）去除对其他操作系统的支持

Windows 2000 可以很好地支持其他类型的操作系统，允许例如 OS/2 和 POSIX 的应用程序向服务器发送请求以执行代码。这种功能通常叫做 Windows 2000 子系统。

Windows 2000 的子系统一般情况下不会用到，而且容易产生安全隐患，应该采取措施进行防御。最简单的方法就是去掉该子系统，这并不会给 Windows 2000 服务器或 IIS 带来任何问题，因为它们是在 Win32 子系统中运行的。

禁止 OS/2 和 POSIX 要通过删除相关文件和改写相关注册表键值来完成，步骤如下：

①删除“ \%systemroot%\system32\os2 ”文件夹及其中所有内容。

②删除“ \HKLM\Software\Microsoft\OS/2 Subsystem for NT ”下面所有的子键。

③删除“ \HKLM\System\CurrentControlSet\Control\Session Manager\Environment ”中的值 Os2LibPath。

④清除“ \HKLM\System\CurrentControlSet\Control\Session Manager\Subsystems ”中 Optional 的内容，但保留值 Optional 的名字。

⑤删除“ \HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems ”中的值 Os/2 和 Posix。

⑥重新启动系统。

（6）合理调整页面文件的设置

页面文件（page file）在系统上的存放位置也需要进行处理。当应用程序或系统程序需要访问物理 RAM 时，Windows 2000 使用页面文件作为应用程序代码的临时保存区。因此，硬盘驱动器上必须有足够的空间供页面文件使用，否则就会导致系统崩溃。避免出现这种情况的方法有：

- 在系统上尽可能多安装 RAM。可用的物理 RAM 越多，系统运行的效率越高。
- 将所有的操作系统文件放置在自己的分区。这个分区中应该只包含操作系统文件和一个至少相当于物理 RAM 大小的页面文件。当系统遭遇一个 STOP 错误时，这个页面文件允许系统创建一个 crashdump 文件。
- 至少在另外一个分区上创建一个页面文件，其大小大约为物理 RAM 容量加上 11 MB。如果可能的话，将这个页面文件放置在一个单独的物理驱动器上，这样系统执行 I/O 操作就更加有效。
- 配置系统服务和生成日志文件及扩展数据的应用程序，使它们写入的文件不在操作系统所在的驱动器上。

（7）对重要系统文件的策略

操作系统中有许多非常重要的文件，如 cmd.exe 等。它们既可以让管理员方便地执行维护工作，又可能被攻击者利用来进行破坏活动。因此，有必要对这些文件进行删除、重命名或者为其设置严格的 NTFS 权限，目的就是使攻击者无法轻易的对其进行利用。

这些重要的文件如图 9-11 所示。

XCOPY.EXE	EDLIN.EXE	NET.EXE
AT.EXE	RSH.EXE	TRACERT.EXE
REGEDIT.EXE	FINGER.EXE	NETSH.EXE
CACLS.EXE	RUNAS.EXE	TSKILL.EXE
REGEDT32.EXE	FTP.EXE	POLEDIT.EXE
CMD.EXE	RUNONCE.EXE	WSCRIPT.EXE
REGINI.EXE	ISSYNC.EXE	RCP.EXE
CSCRIPT.EXE	TELNET.EXE	DEBUG.EXE
REGSRV32.EXE	NBTSTAT.EXE	REXEC.EXE
TFTP.EXE		

图 9-10 重要的系统文件

（8）更改网络连接属性

对于 IIS 服务器来说，在配置网络协议时务必关闭 NetBIOS 协议。在“ 本地连接属性 ”对话框中，只选中“ Microsoft 网络客户端 ”和“ Internet 协议（TCP/IP）”两项，如图 9-11 所示。

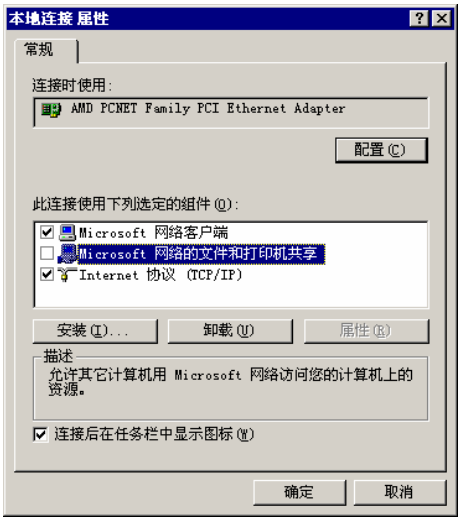

图 9-11 网络连接属性

选中“ Microsoft 网络客户端 ”的原因在于 NTLM 安全支持供应（Security Support Provider）组件是嵌入在操作系统中的，如果没有这个组件，IIS 将无法运行。

如果要在该服务器上使用其他功能，则可以为服务器安装两个网卡：第一个用于 Internet 连接，其上只绑定这两个服务协议；第二个用于从本地网络访问服务器，根据需要添加其他的服务协议，例如“ Microsoft 网络的文件和打印机共享 ”等。

除此之外，在 TCP/IP 协议的属性设置界面中，单击“ 高级 ”按钮进入“ WINS ”选项卡设置“ 禁用 TCP/IP 上的 NetBIOS ”，以阻止网卡向 Internet 发送和接收 NetBIOS 信息，如图 9-12 所示。

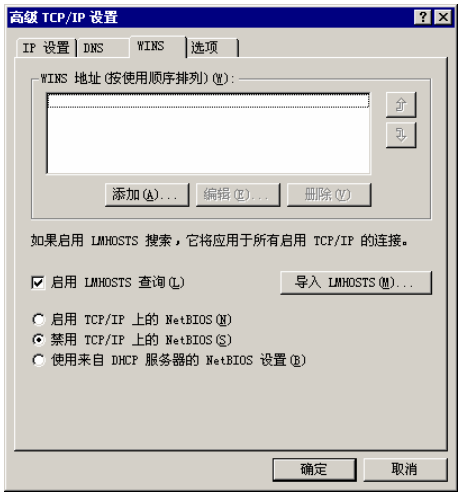

图 9-12 禁用 TCP/IP 上的 NetBIOS

（9）消除空连接安全漏洞

在 Windows 2000 系统中，攻击者可以使用一个空账号登录到系统来建立一个空对话，从而获取服务器上用户和组账号情况列表以及服务器上的所有共享资源列表。在很多网络攻击工具中均有利用此漏洞的工具。在本书的“ 文件系统安全 ”一章中，已经有过关于该问题的阐述，请参见相关内容。

(10) 改写注册表以降低被攻击的风险

在网络上，攻击者常常利用 DDoS 攻击，使用巨量非正常的 TCP SYN 以及 ICMP 数据包向服务器发出请求，最终导致服务器不能正常工作。改写注册表信息虽然不能完全制止这类攻击，但可以降低其风险。可以根据表 9-4 来对注册表进行设置，来降低网络攻击的风险。

表 9-4 针对网络攻击的注册表建议设置

键名	设置	说明
SynAttackProtect **项**：Tcpip\Parameters	**有效范围**：0, 1, 2 **默认值**：0（没有保护） **建议值**：2	与减少 SYN-ACKS 重新传输的数量有关，它会缩短资源保留分配的时间。在建立了连接之后才分配路由路径缓存项目的资源。如果设置为 2，则在三方连通后，连接才会指到 AFD。需注意的是，若 TcpMaxHalfOpen 和 TcpMaxHalfOpenRetried 的设置值超出了范围，保护机制才会执行操作
TcpMaxHalfOpen **项**：Tcpip\Parameters	**有效范围**：100~0xFFFF **默认值**：100 (Professional, Server)，500 (advanced server) **建议值**：默认值	在 SYN-ATTACK 保护开始操作之前，用该参数来控制 SYN-RCVD 状态中所允许的连接数。如果 SynAttackProtect 设置为 1，确定在所要保护的端口上，该值小于 AFD 监听的 backlog
TcpMaxHalfOpenRetried **项**：Tcpip\Parameters	**有效范围**：80~0xFFFF **默认值**：80 (Professional, Server)，400 (Advanced Server) **建议值**：默认值	在 SYN-ATTACK 保护开始操作之前，该参数控制 SYN-RCVD 状态（至少发送了一个 SYN 的重新传输）所允许的连接数
EnablePMTUDiscovery **项**：Tcpip\Parameters	**有效范围**：0, 1 **默认值**：1 （True） **建议值**：0（False）	当此参数设置为 1 时，TCP 试图从连到远程主机的路径中查找最大传输单位。通过找到路径 MTU 和将 TCP 段限制为该大小，TCP 可在路由器中沿着连接具有不同 MTU 的网络的路径消除碎片。碎片对 TCP 吞吐量和网络拥塞有不利的影响。将该参数设为 0 会导致 576 字节的 MTU 用于所有的连接中，而不只是用于本地子网上的主机而已
NoNameReleaseOnDemand **项**：Netbt\Parameters	**有效范围**：0, 1 **默认值**：0（False） **建议值**：1（True）	这个参数决定在计算机收到一个来自网络的名称释放请求时是否释放它的 NetBIOS 名称。 添加它的目的在于允许管理员保护机器不受恶意的名称释放所攻击
EnableDeadGWDetect **项**：Tcpip\Parameters	**有效范围**：0, 1 **默认值**：0（False） **建议值**：1（True）	当参数设为 1 时，则允许 TCP 检测失效的网关。 在激活这项功能后，如果许多连接都遇到困难，则 TCP 可能会要求 IP 更换到备用网关
KeepAliveTime **项**：Tcpip\Parameters	**有效范围**：1~0xFFFFFFFF **默认值**：7,200,000（两个小时） **建议值**：300,000（5 分钟）	该参数通过发送一个“保持活动”数据包来控制 TCP 试图多久验证一次闲置连接仍旧完好。 如果远程系统仍旧是可到达的且运行正常，它则确认该“保持活动”传输
PerformRouterDiscovery **项**：Tcpip\Parameters\Interfaces	**有效范围**：0，1，2 **默认值**：2（只有当 DHCP 发送路由器发现选项时才启用） **建议值**：0（禁用）	该参数控制 Windows 2000 是否根据 RFC 1256 在每一个接口上试图执行路由器发现
EnableICMPRedirects **项**：Tcpip\Parameters	**有效范围**：0, 1 **默认值**：1 （True） **建议值**：0（False）	该参数控制 Windows 2000 是否因 ICMP 重定向网络设备（如路由器）发送到它的消息而更改它的路由表

2. 安全配置 IIS

（1）TCP/IP 筛选配置

Windows 2000 的 TCP/IP 安全配置与 Windows NT 4.0 中的执行方式完全相同。在网卡的“TCP/IP 协议”属性的“高级”选项里，选择“TCP/IP 筛选”，单击“属性”按钮，打开如图 9-13 所示的对话框。

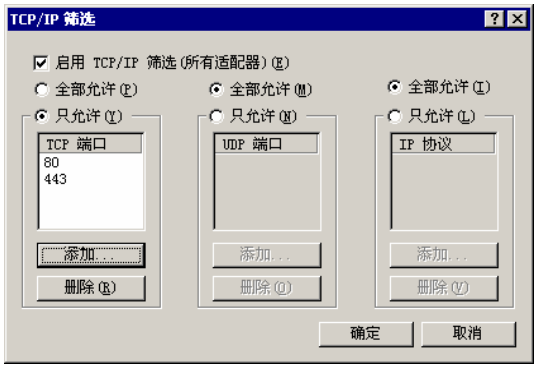

图 9-13 “TCP/IP 筛选”对话框

其中：“全部允许”表示允许来自所有端口的通信数据；“只允许”表示除了特别列举端口外的通信数据都将拒绝。一般来说，IIS Web 服务器通常使用的端口就是 HTTP 80 和 HTTPS 443。

（2）IP 安全设置

关于 IPSec 策略，请参看本书的“网络传输安全”一章中的相关内容。除了在“本地安全设置”中对用于本机的 IPSec 策略进行设置之外，也可以通过网卡的“TCP/IP 协议”属性“高级”选项里的“IP 安全设置”来进行，如图 9-14 所示。

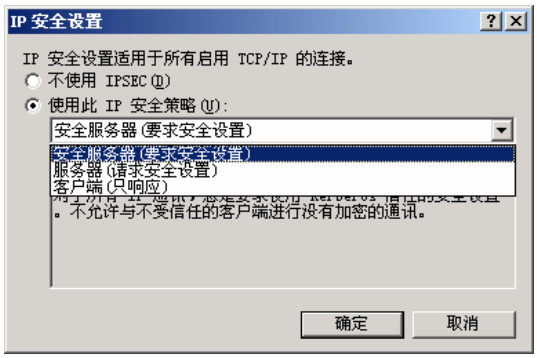

图 9-14　IP 安全设置

（3）单独设置 IIS 服务器

在可能的情况下，IIS 应该安装在一个单独的服务器上。换言之，该服务器不是任何域中的成员，不必与域控制器建立 Netlogon 信道，从而降低通过服务器之间连接而建立起来的空用户连接所带来的安全风险。而且，由于系统之间不传递认证通信信息，也就降低了登录口令被截获的可能性。

（4）合理设置根目录

应将 Web 根目录定位在操作系统分区以外的地方，甚至是其他的物理磁盘驱动器上。而且，当设置 Web 站点的虚拟目录或重定向目录时，也要保证这些目录不会被重定向到操作系统的启动分区，因为有些攻击能够危及访问目录所在分区上的其他目录。

另外的一种安全处理方式就是把 Web 根目录设置到另一个服务器上，使 IIS 服务器成为一个只缓冲请求、应答请求的系统。而且经过这样处理后，整个服务器基本上是一个通用型的，上面没有任何存储内容，即使站点遭到攻击而瘫痪也可以从磁带或其他备份中快速简单地恢复服务器。

此外，C:\inetpub\ftproot（FTP 服务所在目录）和 C:\inetpub\mailroot（SMTP 服务所在目录）的访问权限是 Everyone 完全控制，每个用户都具有向其中添加数据的权限。这样就有可能造成目录所在磁盘的空间耗尽。所以，应将这 2 个目录放置到另外的磁盘卷中，与其他的 IIS 服务程序分开，并使用 Windows 2000 磁盘配额功能来限制添加到这 2 个目录的数据量。

（5）删除危险的 IIS 组件

- 禁止或者删除所有的示例程序 :默认安装选项中，示例程序不会被安装到计算机中。对于一个正式应用的 IIS 服务器来说，不应该在其中安装任何示例程序。若已经安装了某些示例程序，应该将它们完整删除掉。表 9-5 列举的是示例程序的默认安装路径。

表 9-5　IIS 服务器示例程序的默认安装路径

示例程序类别	所在虚拟目录	默认安装路径
IIS 例子程序	\IISSamples	c:\inetpub\iissamples
IIS 文档	\IISHelp	c:\winnt\help\iishelp
Data Access	\MSADC	c:\program files\common files\system\msadc

- 删除虚拟目录 IISADMPWD：该虚拟目录的作用是允许用户重新设置他们在 Windows NT 或者 Windows 2000 操作系统上的账号口令，应用环境主要针对企业内部网 Intranet。IIS 5.0 的安装中没有包含这一项，但如果是从 IIS 4.0 升级到 IIS 5.0，

那么就会存在该虚拟目录。如果非 Intranet 环境，就将其删除。

- 删除不使用的应用程序映射关联：IIS 默认情况下可以解释如.asp、.htr、.shtm 等应用程序文件，当这些文件被 IIS 接收后，将交由一个 DLL 文件处理。这种应用程序的映射关联如图 9-15 所示。

图 9-15　应用程序映射

这些 DLL 文件常常因为自身的缺陷而给系统带来非常严重的危害。如果不使用其中的某类文件，那么就应该在 IIS Web 服务器属性的“应用程序映射”中删除该文件类型。在 IIS 中的映射关系可以参照表 9-6 删除相关的类别(如果不需要该类型)。

表 9-6　删除应用程序映射的参照表

应用	映射类型
基于 Web 的口令修改	.htr
Internet 数据库连接器	.idc
服务器端包含文件（Server-side Includes）	.stm, .shtm, and .shtml
Internet 打印	.printer
索引服务（Index Server）	.htw, .ida and .idq

（6）为 IIS 服务器的文件分类设置权限

- 为虚拟目录设置适当的访问权限：正确设置虚拟目录的访问权限，将会在很大程度上影响其中文件的安全可靠性。建议根据表 9-7 考虑设置的原则。

表 9-7　IIS 虚拟目录的访问控制设置

文件类型	建议的访问权限
CGI 程序(.exe, .dll, .cmd, .pl)	Everyone (X) Administrators (Full Control) System (Full Control)
脚本文件(.asp)	Everyone (X) Administrators (Full Control) System (Full Control)
包含文件(.inc, .shtm, .shtml)	Everyone (X) Administrators (Full Control) System (Full Control)
静态文件 (.txt, .gif, .jpg, .html)	Everyone (R) Administrators (Full Control) System (Full Control)

- 为不同类型的文件创建不同的目录：如果一个虚拟目录下面有多种类型的文件，按

照上面的原则为每一种文件设置访问权限，无疑是非常烦琐的事情。因此，可以采取为不同类型文件创建不同目录的方式，然后再按照上面的原则为每一个目录设置相应的访问权限。比如，可以创建如下的目录结构。

- C:\inetpub\wwwroot\myserver\static 存放静态文本文件（.htm, .html）
- C:\inetpub\wwwroot\myserver\include 存放包含文件（.inc）
- C:\inetpub\wwwroot\myserver\scripts 存放脚本文件（.asp）
- C:\inetpub\wwwroot\myserver\executable 存放可执行文件（.exe,.dll, .cmd, .pl）
- C:\inetpub\wwwroot\myserver\images 存放图形文件（.gif,.jpeg）

除了在操作系统级别上为 IIS 服务器上的文件设置必要的权限外，还要在 IIS 管理器中为它们设置权限。一般而言，对一个目录永远也不应同时设置写和执行权限，以防止攻击者向站点上传并执行恶意代码。此外，目录浏览功能也应该禁止，预防攻击者浏览站点上的目录发现有缺陷的文件或代码。一个较好的设置策略是：为 Web 站点上不同类型的文件建立不同的目录，然后给它们分配适当权限。

- Scripts 目录 包含站点的脚本文件，为该目录设置“ 纯脚本 ”执行许可权限。
- BIN 目录 包含站点上的二进制执行文件，为该目录设置“ 脚本和可执行程序 ”执行许可权限。
- Static 目录 包括所有静态文件，为该目录设置“ 读权限 ”

（7）保护 IIS Metabase

IIS Metabase 保存着包括口令在内的几乎 IIS 配置各个方面的内容，而且这些信息都以明文形式存储，因此保护它至关重要。建议采取如下措施。

- 把 HTTP 和 FTP 根文件夹从%systemroot%下移走
- 慎重考虑重新命名 Metabase 和移动 Metabase 位置
- 安全设置确定 Metabase 位置的注册表关键字
- 审核所有试图访问并编辑 Metabase 的失败日志
- 删除文件%systemroot%\system32\inetserv\Iissync.exe
- 为 Metabase 文件设置以下权限：Administrators 组完全控制，System 完全控制

完成配置后备份 Metabase，这时会创建目录%systemroot%\system32\inetserv\MetaBack，该目录用来存储备份文件。对于该目录，需要采取如下措施进行保护：

- 审核对 MetaBack 目录的所有失败访问尝试
- 为 MetaBack 目录设置如下权限：Administrators 组完全控制，System 完全控制

最后，还需要保护能够编辑 Metabase 的工具，可以参考以下内容。

- 转移包含 IIS 所有管理脚本的目录\Inetpub\Adminscripts。IIS 的管理脚本路径如图 9-16 所示。

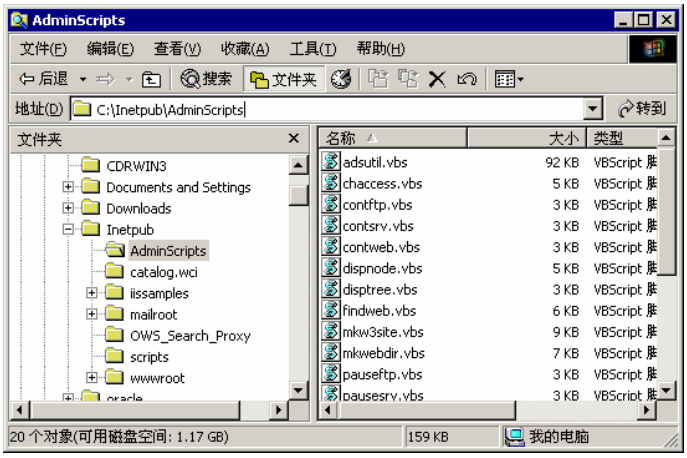

图 9-16 IIS 的管理脚本路径

- 将系统“ Program files ”下的 Metaedit.exe 和 Metautil.dll 这两个文件转移至%systemroot%\system32\Inetserv 目录下，并调整相应的开始菜单快捷方式。
- 审核对 Adminscripts 目录的所有失败访问尝试。
- 对执行.VBS 文件的%systemroot%\system32\csript.exe 设置权限为“ Administrators 组完全控制 ”。
- 对 Adminscripts 目录权限设置为“ Administrators 组完全控制 ”。

（8）使用 IP 地址和域名限制访问

如果 Web 站点只对特殊 IP 地址的客户服务，则对 Web 站点执行 IP 地址和域名限制的设置。如果设置的是 DNS 域名信息，则会导致 IIS 执行 DNS 搜索工作，耗费一定的时间，一般不建议采用。

（9）IIS 的日志审核

IIS 日志文件记录了所有访问 IIS 服务程序的信息，对于管理员检测故障、查找攻击者非常重要。一般来说，攻击者为了销毁他们的侵入痕迹总是要设法伪造或者删除日志文件。因此，应该对 IIS 的日志文件进行重点保护。

IIS 的日志文件默认位于%systemroot%\system32\LogFiles，应对其设置如下的访问权限。

- Administrators：完全控制
- System：完全控制
- Everyone：读取、写入和更改

3. 使用 IIS Lockdown 和 URLScan

（1）简介

Microsoft 发布的 IIS Lockdown Wizard（IIS 锁定向导）可用来帮助设置 IIS 服务器上的安全性。它通过关闭 IIS 服务器上的某些不必要的特性来工作，从而减少了攻击者能够利用和攻击范围。

URLScan 则是一个强大的 IIS 安全工具，它与 IIS 锁定向导协同工作，赋予了 IIS Web 站点管理员限制某些服务器处理某些特定 HTTP 请求的能力，并且因此阻止了潜在的有害请求到达并破坏服务器。为了提供深层次的锁定，或者说在多个层面抵挡攻击，URLScan 和面向每个受支持服务器角色的定制模板都已经被集成到了 IIS Lockdown Wizard 之中。

IIS Lockdown Wizard 最基本的功能就是帮助管理员设置 IIS 安全性。即使系统没有及时安装所有补丁，也能有效防止利用 IIS 的已知漏洞。它还可以帮助管理员去掉对 IIS 服务器上不必要的一些服务，使 IIS 在满足服务器需求的情况下运行最少的服务。

IIS Lockdown Wizard 在原有的版本上作了一些改进，主要体现在以下几个方面。

- 服务器角色：为与 IIS 相关的大多数 Microsoft 产品提供一些模板，这些产品包括 Microsoft Exchange 5.5、2000、Commerce Server、BizTalk, Small Business Server 4.5 和 2000、SharePoint Portal Server、FrontPage Server Extensions 和 SharePoint Team Server。
- URLScan 集成为每个受支持的服务器角色定制的模板。这种集成允许 Lockdown Wizard 通过应用 URLScan 而提供附加的安全性，无须管理员为特殊的服务器配置和应用设计定制的 URLScan 过滤器。
- 删除或禁用 IIS 服务的能力，例如 HTTP、FTP、SMTP 和 NNTP 服务。
- 升级向导可以读取应答文件，从而为脚本安装或者无人值守安装提供了支持。
- 基于用户反馈对用户重新进行了设计，并修正了一些程序错误。

（2）使用 IIS Lockdown

在运行 Lockdown Wizard 程序时，首先会看到微软的标准许可信息，然后将询问有关服务器模板的信息。此时，需要选择在整体结构中最适合服务器扮演的角色，例如 Dynamic Web server（ASP Enabled）服务器，如图 9-17 所示。这里的选择将决定 Lockdown Wizard 对 IIS 服务器开启何种类型的访问权限。

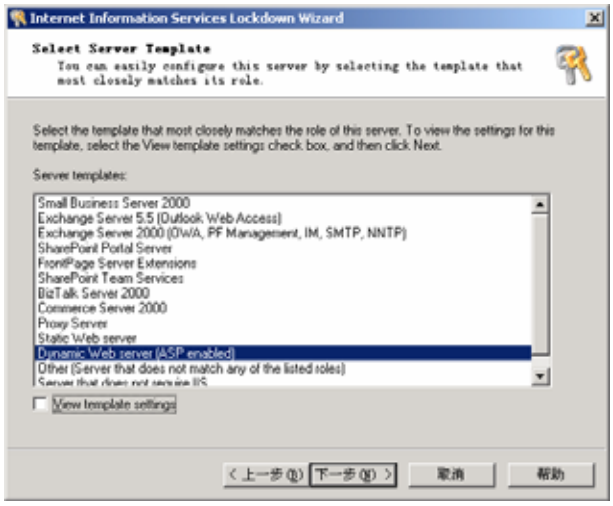

图 9-17　IIS Lockdown Wizard 的模板选择

可以通过选中对话框底部的“ View template settings ”（查看模板设置）复选框来在下几步对该模板进行详细的定制，使之更符合自身的需求。

最后允许选择是否安装 URLScan 如图 9-18 所示。这可以被用来筛选进入的 URL 请求，并根据一个可以修改和制定的规则集来拒绝某类特定的请求。

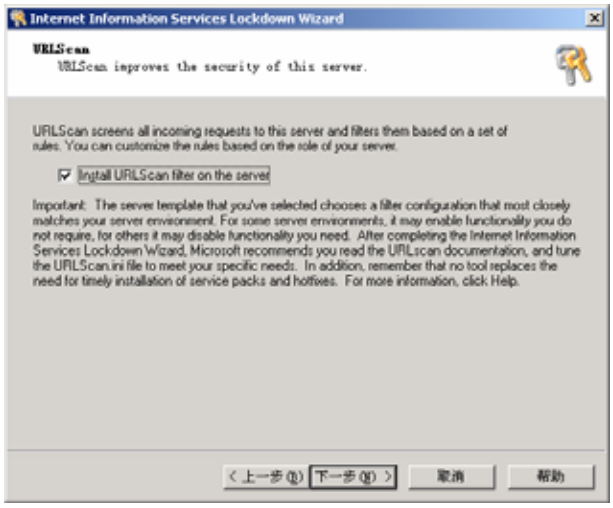

图 9-18　IIS Lockdown 中集成的 URLScan

单击“ 下一步 ”继续操作即可完成对 IIS 服务器的安全设置。

（3）URLScan 的配置和使用

URLScan 安装完成后可以在 System32/InetSvr/URLScan 目录（此目录无法更改）下找到以下文件。

- urlscan.dll：动态连接库文件
- urlscan.inf：安装信息文件
- urlscan.txt：软件说明文件
- urlscan.ini：软件配置文件

URLScan 的配置由 urlscan.ini 文件来完成。下面对此文件进行一些说明。

- 该文件的名称必须为 urlscan.ini。

- urlscan.ini 必须和 urlscan.dll 在同一目录中。
- urlscan.ini 必须是标准的 ini 文件结构，也就是由节，串和值所组成。
- urlscan.ini 修改以后，必须重新启动 IIS，才能使配置生效。

urlscan.ini 由以下各节组成。

- [Option]节：主要设置节。[Option]节的设置直接影响到以后的配置，因此该节的设置特别重要。该节主要进行以下属性的设置。
  - UseAllowVerbs 使用允许模式检查 URL 请求，默认为 1。如果设置为 1，所有未在 AllowVerbs 节设置的请求都被拒绝 如果设置为 0，所有未在 DenyVerbs 节设置的 URL 请求都认为合法。
  - UseAllowExtensions 使用允许模式检测文件扩展名，默认为 0。如果设置为 1，所有未在 AllowExtensions 节设置的文件扩展名均认为是非法请求；如果设置为 0,所有未在 DenyExtensions 节设置的扩展名均被认为是合法请求。
  - EnableLogging 是否允许使用 Log 文件，如果为 1，将在 urlscan.dll 的相同目录设置名为 urlscan.log 的文件记录所有过滤。
  - AllowLateScanning 允许其他 URL 过滤在 URLScan 过滤之前进行，系统默认为不允许 0。
  - AlternateServerName 使用服务名代替。如果此节存在而且 RemoveServerHeader 节设置为 0，IIS 将在这里设置的服务器名代替默认的“Server”。
  - NormalizeUrlBeforeScan 在检测 URL 之前规格化 URL，默认为 1。如果为 1，URLScan 将在 IIS 编码 URL 之前 URL 进行检测。只有在管理员对 URL 解析非常熟悉的情况下才可以将其设置为 0。
  - VerifyNormalization 默认为 1。如果设置为 1，UrlScan 将校验 URL 规则，该节的设定与 NormalizeUrlBeforeScan 有关。
  - AllowHighBitCharacters 默认为 1。如果设置为 1，将允许 URL 中存在所有字节；如果为 0，含有非 ASCII 字符的 URL 将被拒绝。
  - AllowDotInPath 如果设置为 1，将拒绝所有含有多个“.”的 URL 请求。由于 URL 检测在 IIS 解析 URL 之前，所以，对这一检测的准确性不能保证，默认为 0。
  - RemoveServerHeader 如果设置为 1，将把所有应答的服务头清除。默认为 0。
- [AllowVerbs]节：配置认定为合法 URL 规则设定，该设定与 Option 节有关。如果 UseAllowVerbs 设置为 1，该节设置的所有请求将被允许。一般设置 GET、HEAD、POST 等请求。
- [DenyVerbs] 节：配置认定为非法 URL 规则设定，该设定与[Option]节有关。如果 UseAllowVerbs 设置为 0，该节设置的所有请求将拒绝。一般设置 PROPFIND,PROPPATCH,MKCOL,DELETE,PUT,COPY,MOVE,LOCK,UNLOCK 等请求。
- [DenyHeaders]节：配置认定为非法的 header 在这里设置。
- [AllowExtensions]节：配置认定为合法的文件扩展名在这里设置，该设定与[Option]节有关。在该节设置的所有扩展名文件将被允许请求，一般设置为.asp、.htm、.html、.txt、.jpg、.jpeg、.gif 等。如果需要提供文件下载服务，通常还要增加.rar、.zip。
- [DenyExtensions]节：配置认定为非法的文件扩展名在这里设置，该设定与[Option]节有关。在该节设置的所有扩展名文件请求将被拒绝，一般设置为.asa 文件、可执

行文件、批处理文件、日志文件、不常见扩展如.shtml、.printer 等。

9.2 终端服务

9.2.1 终端服务简介

终端服务是在 Windows 2000 操作系统系列（不包括 Professional）中提供的一种技术，用于在一个远端的 Windows 2000 系统上执行基于 Windows 的应用程序或进行相应的管理工作。

终端服务技术的起源可以追溯至几年以前的 NC 与 NetPC 讨论，这次为达到降低企业总体拥有成本的目的而进行的讨论导致了 Windows 家族中一种新产品的出现——终端服务系列产品。

对于大部分的公司而言，他们所采用的计算模型是各不相同的。使用 Windows2000 操作系统系列平台，用户可以选择最适合他们的计算模型，这有可能是高度分布的客户机/服务器模型，也可能是高度集中的中央计算模型。通过 Windows 2000 服务器操作系统与终端服务的集成，用户可以在一个中央计算模型中部署最新的基于 Windows 的应用程序，从而使应用程序完全运行在服务器端。

1. 终端服务的优势

终端服务技术允许把进程、软件与数据存储、软件安装、配置和管理集中化。可以把应用程序安装在服务器上，并通过服务器运行，从而不再需要客户机具有十分强大的功能。包括数据处理和存储在内的所有处理，都可以在服务器上运行。因为应用程序是安装在服务器上的，所以只需要在服务器上对应用程序做一次全局性的改动，就会影响到连接终端服务的所有客户，这就与普通的对等或客户/服务器模式不同。应用程序的集中式管理减少了网络的管理成本，并向用户提供了一个统一的工作环境，而与用来登录终端服务的平台或地理位置无关。

终端服务的实现还具有以下好处：

- 对桌面硬件功能要求的降低，从而降低了初始购买客户机的价格。
- 服务器能够满足应用程序对更大内存或处理能力的任何需求，所以减少了硬件升级的需要，从而有益于所有用户。
- 数据和应用程序集中存储，所以能够集中的查杀病毒。
- 数据和应用程序集中存储，所以使得审核和备份变得更加容易，从而提高了安全性。而且，因为本地数据存储很少，所以使得用户恶意移动数据会很困难。
- 客户机趋于更简单，通常由一个终端或一个功能简单的计算机所组成，所以减少了客户端硬件出错的可能性。
- 通过终端服务把用户和 WAN 访问合并到一起。

2. 终端服务的工作原理

终端服务的工作原理是：客户机和服务器通过 TCP/IP 协议和标准的局域网构架联系。通过客户端终端，客户机的鼠标、键盘的输入传递到终端服务器上，再把服务器上的显示传递回客户端。客户端不需要具有计算能力，至多只需提供一定的缓存能力。众多的客户端可以同时登录到服务器上，仿佛同时在服务器上工作一样，它们之间作为不同的会话连接是互相独立的。终端服务的机制如图 9-19 所示。

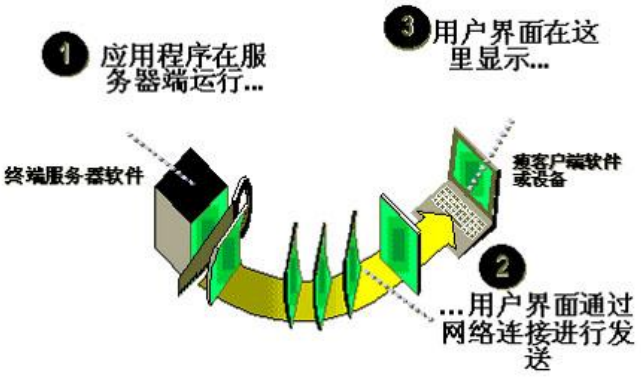

图 9-19 终端服务的工作机制

9.2.2 终端服务的操作模式

运行终端服务的终端服务器有两种具体的操作模式：应用服务器（Application Server）模式和远程管理（Remote Administration）模式。

1. 应用服务器模式

在应用服务器模式下，管理员可以从一个中心位置部署和管理应用程序，从而节省部署、维护以及升级等工作所需的时间与精力。一旦应用程序通过终端服务部署完成，客户端就可以通过远程访问服务、局域网（LAN）、广域网（WAN）等进行连接，而且这些客户端可以是基于 Windows 的、基于 Windows CE 的，甚至可以是基于非 Windows 的操作平台。

如果启用了终端服务的服务器被配置为应用服务器，那么各个客户端就必须要有一个终端服务客户端访问许可证（Client Access License, CAL）和一个标准的 Windows 2000 客户端访问许可证。不管客户端的操作系统或用来连接终端服务的连接协议是什么，客户端访问许可证都是必需的。而终端服务所支持的客户端数量只受限于购买的客户端访问许可证的数量和服务器的处理能力。

应用服务器模式是终端服务初始配置时的默认模式。这种模式的设计用来向众多用户提供从服务器上运行的基于 Windows 的应用程序。应用服务器模式以许多特定的方式来配置终端服务，包括：

- 用适合于交互应用的方式利用存储器和 CPU。
- 增强终端服务应用程序的兼容性，以帮助那些不支持终端服务环境的应用程序。
- 为连接了终端服务会话的各个设备分配许可证。

终端服务也可以被最优化以便能够处理许多会话，但由此也增加了服务器系统的开销。尽管在一台主要用于应用服务的服务器上使用应用服务器模式所需的成本是合理的，但如果在一台具有关键性任务的服务器上使用该模式的话，就有可能是有害的。同样的道理，专门的安装和设备的许可证对于一台应用服务器来说是至关重要的，但在一个集中化的操作环境却又是麻烦和不必要的。

2. 远程管理模式

远程管理模式是 Windows 2000 的一个新的终端服务特性。远程管理模式可使管理员能够使用任何 TCP/IP 连接对网络上的任何 Windows 2000 Server 计算机进行远程管理。管理员可以通过内置的图形化（GUI）管理工具来对远程的计算机进行完全的控制和管理，就如同坐在那台计算机前面进行操作一样。

远程管理模式只安装终端服务的远程访问组件，而不会安装应用程序共享组件。这就是

说，可以在运行关键任务的服务器上以很小的开销来使用远程管理。使用远程管理模式的终端服务最多允许两个同时的远程管理连接。对于那些连接不需要附加的授权，也不需要一个许可证服务器。

终端服务的远程管理模式包括以下特性和优势：

- 任一终端服务客户都可以对 Windows 2000 服务器进行管理。
- 可以远程对与控制器进行改进、重启、升级和降级。
- 可以通过窄带连接来访问服务器，并且可以使用达到 128 位的加密。
- 允许数据敏感的或耗时的任务在远程会话被故意切断或因网络问题而被切断时仍然能够成功地完成。
- 可以进行远程应用程序安装与执行，并且可以快速访问本地磁盘和存储介质。
- 进行远程管理时不影响控制台会话，从而消除了被窃听的威胁。
- 可以忽略对服务器性能的影响，并且不会影响应用程序的兼容性。
- 无需终端服务的客户授权。
- 设置了远程桌面协议（RDP）特性，包括本地打印、剪贴板操作和对本地驱动器映射等任何 RDP 虚拟信道应用的支持。

9.2.3 终端服务的组件

Windows 2000 终端服务由以下五个组件组成。

- Windows 2000 服务器多用户内核：最初为 Windows NT Server 4.0 终端服务器开发的多用户内核扩展在 Windows 2000 中作了很大的增强，并且成为 Windows 2000 内核的标准部分。不管终端服务安装与否，这种内核是一直内嵌在服务器操作系统内。
- 远程桌面协议（RDP）：Windows 2000 终端服务的一个核心组件就是允许客户端与网络上的终端服务器进行通信所使用的协议。这种协议是基于国际电信联盟制定的国际标准 T.120 的一种多通道协议。它是一种双字节兼容的协议，使用在各种网络环境下用来实现网络定位、自动断开连接以及远程配置。
- 终端服务客户端软件：客户端软件用于在客户机上显示用户熟悉的 32 位 Windows 用户界面。这是一个非常小的应用程序，用来建立和维护客户端与运行终端服务的服务器之间的连接。它将所有的用户输入如键盘录入或鼠标移动传送给服务器，并且将所用服务器端的输出如应用程序显示信息及打印流返回给客户端。
- 终端服务许可服务：当终端服务被安装为应用服务器模式时就需要用到该服务。该服务使得终端服务能够获得和管理连接设备的终端服务客户访问许可证（CAL）。当终端服务安装为远程管理模式时不需要终端访问许可服务。终端服务许可服务是 Window 2000 Server、Advanced Server 和 Datacenter Server 的组件。
- 终端服务系统管理工具：管理工具由管理终端服务的软件组成，其中包括终端服务许可证管理器、终端服务客户端生成器、终端服务客户端配置工具以及终端服务管理器。

1. 终端服务许可服务

如上所述，Windows 2000 终端服务在配置成应用服务器模式时需要所有初始终端服务会话的客户端具有许可，这种许可可以是 Windows 2000 的客户端许可证（CAL）也可以是终端服务的的客户访问许可证。在 Windows 2000 之前，管理和分发 CAL 的工作由管理员完成，这使得跟踪部署终端服务的客户端的 CAL 变得非常困难。

Windows 2000 的终端服务首次实现了安全可靠的客户端认证机制，这就是内置在

Windows 2000 Server 中的终端服务许可服务。通过这种服务可以使终端服务获得和管理所有连接到终端服务器的客户端的 CAL。它可以管理未许可的、以前许可的、临时许可的以及 CAL 许可的各种客户端。这样极大地简化了管理员的许可证管理工作。

终端服务许可的模型如图 9-20 所示。从图中可以看出，终端服务许可在以下几个组件之间进行：启用了终端服务许可服务的许可服务器、Microsoft Clearinghouse、终端服务器以及终端服务客户端。一个许可服务器可以支持多个终端服务器，而在一个域或企业内可以有一个或多个许可服务器。

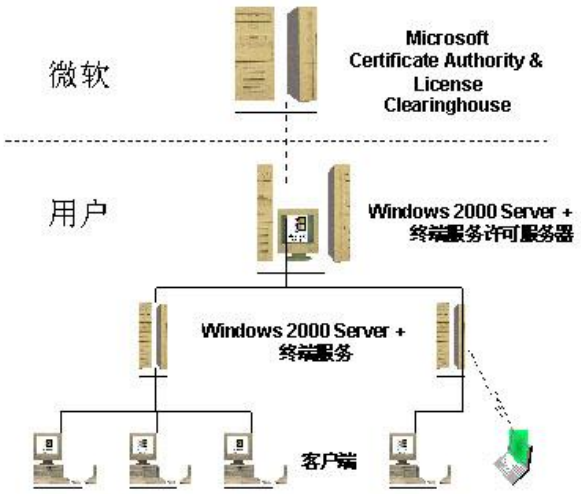

图 9-20　终端服务许可模型

Microsoft Clearinghouse 由微软维护用以激活许可服务器并且向许可服务器发放客户端许可包。可以通过终端服务许可工具中的许可向导访问 Clearinghouse。许可服务器存放对于一组终端服务器所有已经安装的终端服务许可以及所有已经发放的许可。终端服务器使得客户端能够访问基于 Windows 的应用程序，这些应用程序完全运行在服务器端，并且支持多个客户端到服务器的会话。当客户端登录到终端服务器时，服务器将验证客户端的许可证。具有一个有效的 CAL 或运行 Windows2000 操作系统的客户端将被允许连接并且不需要终端服务器与许可服务器进行通信。如果客户端不具有许可证，或给出一个临时许可，终端服务器将与许可服务器联系为客户端申请一个永久许可证。许可服务器将查看其自身的数据库，如果具有可用的 CAL，服务器将会将该 CAL 标记为被该客户端使用并将其从可用 CAL 池中删除。与该许可证相对应的标志将发送至服务器并且被传给客户端。客户端在后续的连接中将向终端服务器出示该标识作为该许可证的证明。

2. 终端服务客户端

终端服务支持对大量客户端计算平台和硬件提供熟悉的 Windows 图形界面。客户端计算机在本地运行终端服务客户端软件。它用来管理客户端与运行终端服务的服务器之间的通信。Windows 2000 的终端服务支持以下类型的设备：

- 基于 Windows CE 的终端
- 基于 Windows CE 的 H/PC
- 运行 Windows 95、Windows 98、Windows NT 等基于 32 位 Windows 的 PC
- 运行 Windows for Workgroup 3.11 的基于 16 位 Windows 的 PC
- 第三方软件厂商（如 Citrix 等）的基于非 Windows 的平台。

3. 终端服务管理工具

终端服务管理工具用于管理和配置终端服务中的功能、用户以及会话。

- 终端服务管理器 :终端服务管理器允许系统管理员管理终端服务器上的终端服务会话、用户及进程。它具有以下一些主要功能。
  - 断开或重置一个会话
  - 远程控制其他会话
  - 终止进程
  - 显示连接状态
  - 显示用户和客户端信息
  - 显示用户和系统进程
  - 向会话或用户发送消息
- 终端服务配置工具 :终端服务配置工具用于创建、修改或删除终端服务器上的会话或会话集。
- 终端服务客户端生成器 :终端服务客户端生成器可以生成安装终端服务客户端软件的软盘集。

9.2.4 终端服务配置

终端服务配置工具允许重新配置现有连接的属性、创建新的连接，以及删除旧的连接。当打开终端服务配置工具时，就已经配置好了一个 RDP 连接。RDP 通常是需要为用户使用终端服务而配置的惟一连接。只能为每个网络适配器（网卡）配置一个 RDP 连接。要想配置额外的 RDP 连接，就需要增加网络适配器。

既可以针对每个用户设置一些连接属性，也可以针对每个服务器设置一些属性。前者通过“ 本地用户和组 ”的 MMC 管理单元来配置，而后者则通过终端服务配置工具来配置。还可以使用终端服务配置工具来配置与服务器有关的设置，如图 9-21 所示。

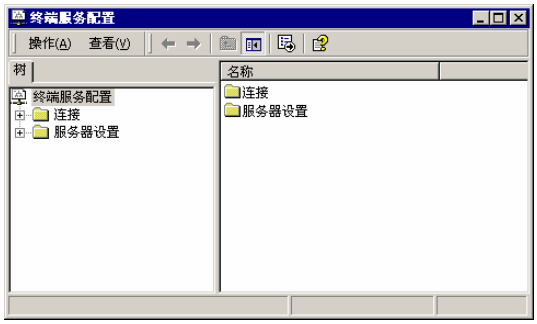

图 9-21 终端服务配置工具

1. 管理连接

可以使用终端服务配置工具来配置客户端与服务器之间的连接：

- 创建一个新的连接
- 停用一个连接
- 重新启用一个连接
- 重命名一个连接
- 删除一个连接

2. 配置连接属性

一旦创建了一个连接，就可以通过在终端服务配置工具窗口中双击该连接的节点，来对它的属性进行设置或者调整。

- 设置连接到服务器上的最大会话连接数 :默认情况下，连接被配制成允许数量不限

的会话连接到服务器上。限制会话的数量可以提高性能，因为这样做使得只有更少的会话需要系统资源，其设置界面如图 9-22 所示。

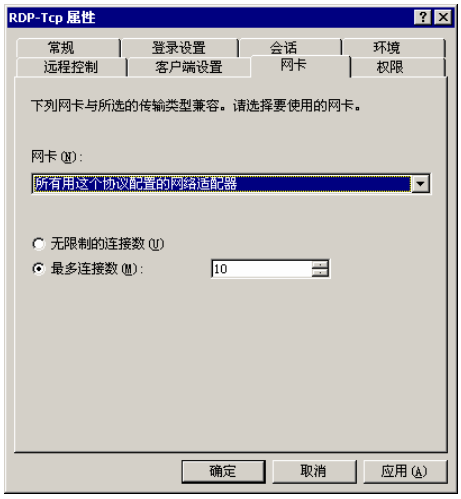

图 9-22 终端服务器的最大连接数

- 更改数据加密级别：可以从三个加密级别中进行选择，即低级、中级和高级，如图 9-23 所示。提高加密级别为每个远程会话增强了对客户/服务器 CPU 的要求。
  - 低级加密只是对从客户端到服务器的数据使用 40 位或 56 位的密钥来加密。运行终端服务的 Windows 2000 服务器在 Windows 2000 客户与它连接时使用 56 位的密钥，而以前版本的客户与它连接时使用 40 位密钥。该加密级别只对输入进行加密的方式保护了用户口令等敏感数据。
  - 中级加密使用 40 位或 56 位的密钥来加密出入服务器的数据。该级别的加密一般用于保护通过网络上传输然后在远程客户机上显示的数据。
  - 高级加密使用高强度的 128 位加密技术对从客户到服务器以及从服务器到客户的数据进行加密。

  此外，即使服务器上已经安装了另一个验证程序包，也可以通过选中“使用标准 Windows 验证”以使用标准的 Windows 验证来产生连接。

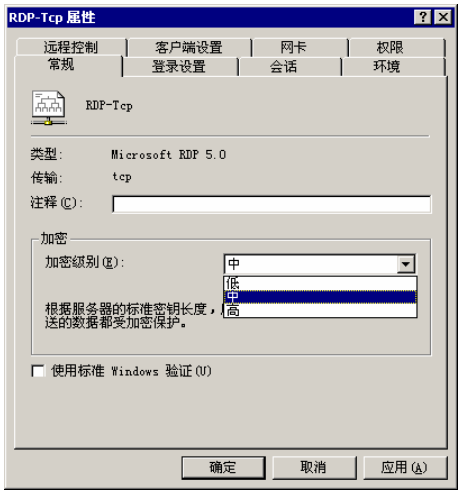

图 9-23 终端服务连接的加密级别

- 登录设置：可以从两个选项中选择。后一个选项“总是使用下列登录信息”允许自动登录服务器，或者允许总是使用同一个账户来使用终端服务。
- 会话设置：对于一个终端服务连接来说，可以限制服务器上保持的活动会话、断开的会话和空闲会话的数量。在服务器上无限运行的会话需要消耗宝贵的系统资源。

当一个活动会话或空闲会话达到会话数限制时，就可以把用户从这个会话中断开或终止该会话。一般地，从一个会话中断开的用户可以在以后重新连接到该会话上。而当一个会话终止时，该会话就被从服务器中永久地删除，并且任何正在运行的应用程序都被迫关闭，这可能会导致客户端的数据丢失。当一个断开的会话达到会话数限制时，该会话就会终止，并被从服务器中永久地删除。在终端服务配置工具中配置的会话数限制适用于所有使用连接登录服务器的会话，也可以使用管理用户和组的工具来对每个用户配置会话数限制。在终端服务配置工具的“ 会话 ”选项卡中可以配置超时与重新连接的延时和操作，也可以创建覆盖用户自身设置的规则，如图 9-23 所示。

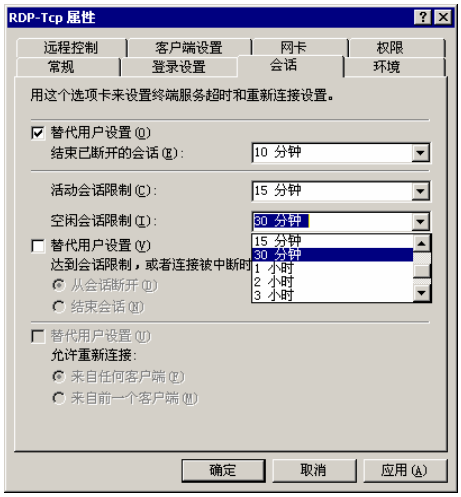

图 9-23　终端服务的会话设置

- 环境设置：可以设置用户登录的时候自动启动的程序。
- 远程控制设置 :可以通过从另一会话上远程控制用户会话来监视客户登录终端服务的活动，如图 9-24 所示。远程控制允许观察或积极地控制另一个会话（在“ 控制级别 ”中选择“ 与会话交互 ”）。如果选择积极地控制一个会话，那么将能够把键盘和鼠标的活动输入会话中。在会话被远程控制之前，可以在客户会话中显示一条消息，请求观察或参与会话（选中“ 需要用户权限 ” 复选框）。

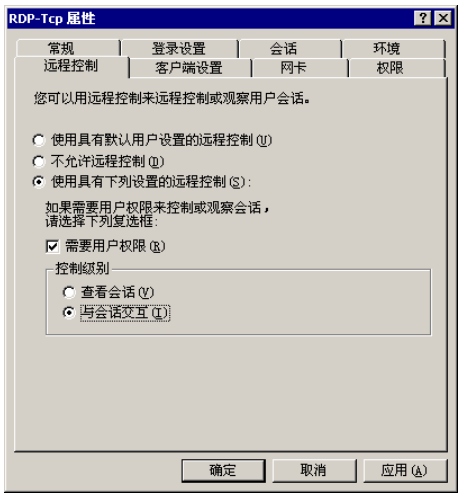

图 9-24　终端服务的远程控制设置

- 客户端设置：设置客户登录时能够自动重新连接的设备。因为客户会话可以在客户与服务器之间创建多个数据信道，所以用户可以映射到驱动器和打印机等本地设备中。默认情况下，用户在客户会话中设置的驱动器和打印机映射是暂时的，不会在

用户下一次登录服务器时还存在。但可以配置成无论用户何时登录，客户映射都自动保存。另外，还可以禁用某些特定的客户设备从而使用户无法映射这些设备。

- 权限设置：使用“ 权限 ”选项卡可以配置用户和组使用终端服务的权限，基本的权限组合有“ 完全控制 ”、“ 用户访问 ”和“ 来宾访问 ”三种，他们包含的具体权限如表 9-8 所示。

表 9-8 终端服务的权限

权限组合	包含的具体权限
完全控制	查询有关会话的信息 配置连接属性 终止一个会话 远程控制另一用户的会话 登录到服务器上的一个会话 把用户从一个会话中注销 给另一用户的会话发送消息 连接另一个会话 断开一个会话
用户访问	登录到服务器上的一个会话 查询有关会话的信息 给另一用户的会话发送消息 连接另一个会话
来宾访问	登录到服务器上的一个会话

也可以通过单击“ 权限 ”选项卡的“ 高级 ”按钮打开“ RDP-TCP 的权限项目 ”对话框，为用户和组更改访问控制权限，如图 9-25 所示。

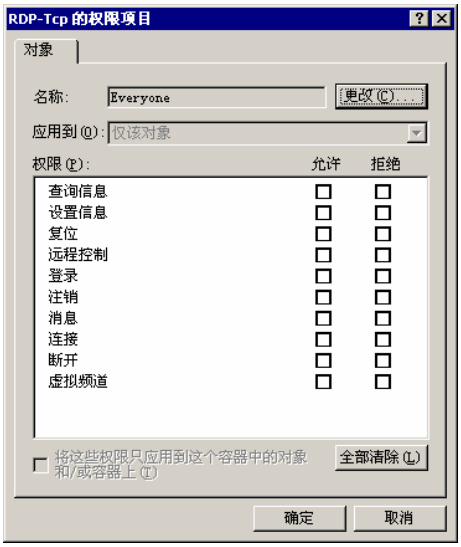

图 9-25 终端服务的权限设置

3. 配置服务器设置

可以在终端服务配置工具窗口中使用“ 服务器设置 ”节点来配置终端服务的设置，如图 9-26 所示。

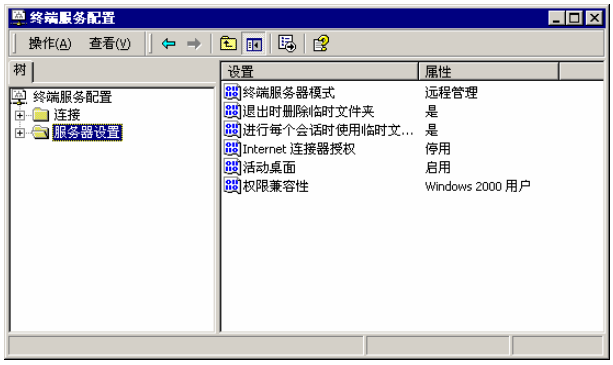

图 9-26 终端服务的服务器配置

- 查看终端服务模式：应用服务器模式还是远程管理模式。
- 退出时是否删除临时文件夹：默认情况下，运行终端服务的服务器为它上面的每个新会话创建单独的临时文件夹，使得每个用户都能够保存各自的临时文件。为了节省硬盘空间，当用户从一个会话中退出时，这些临时文件夹会被自动删除。
- 每个会话是否都使用单独的临时文件夹。
- 启用或禁用 Internet 连接器授权。
- 启用或禁用活动桌面（Active Desktop）。
- 更改权限兼容性：这只能在终端服务运行在应用服务模式下才可以设置。“ 与 Windows 2000 用户兼容 ” 可以提供最安全的环境，而 “ 与 Windows NT 4.0 兼容 ” 可以提供与大多数传统的应用程序相兼容的环境。如果选择前者，那么用户将拥有与 Users 组成员相同的权限，并且可能无法运行许多传统的应用程序。而选择后者，则用户将可以拥有对关键性注册表和文件系统的完全访问权限，适用于用户需要运行许多传统应用程序的环境。

9.2.5 终端服务管理

管理员可以使用 “ 终端服务管理器 ” 来观察在可信任域中运行终端服务的服务器上的信息。终端服务管理器可以监视在每个运行终端服务的服务器上运行的用户、会话和应用程序，并且允许对服务器进行远程管理，如图 9-27 所示。

图 9-27 终端服务管理器

从客户连接到终端服务上的任一会话都会出现在终端服务管理器的 “ 用户 ” 列表中，并且可以监视从 “ 进程 ” 列表中的用户会话运行的任一应用程序。因此，可以从一个位置监视运行终端服务的服务器上的所有用户、会话和应用程序。

下面描述了终端服务中不同类型的会话。

- 控制台会话

在终端服务管理器中，系统控制台会话（Console Session）会在客户连接到终端服务器时自动出现在 “ 会话 ” 列表中。控制台被定义为在安装了终端服务器上的计算机的键盘、鼠

标和视频监视器。可以使用控制台会话登录到终端服务器，就像是从客户会话中登录一样。尽管可以给控制台会话发送消息，但却不能对它执行任何其他的管理操作。

- 侦听者会话

侦听者会话(Listener Session)与正常会话不同。这些类型的会话将侦听并接受新的 RDP 客户连接，为客户请求创建新的会话。如果已在“终端服务配置”程序中配置了多个连接，则会有多个侦听者会话。虽然可以选择重置侦听者会话，但不推荐这么做，因为这样做将使用相同的终端服务连接重置所有会话。没有警告地重置用户会话将导致客户机上的数据丢失。

- 空闲会话

要优化终端服务器的性能，在建立客户连接之前服务器将自动初始化空闲会话（Idle Session)。这些会话可由客户机使用以便进行连接。默认情况下将创建两种空闲会话。

终端服务管理器用于监视信任域中终端服务器的会话、用户和进程。除监视以外，还可以使用终端服务管理器提供的操作来管理终端服务器。可以在“操作”菜单上找到这些操作，表 9-9 中介绍了这些操作。大多数操作都需要有特殊的权限才能执行（可参照表 9-8)。

表 9-9 终端服务操作

操作	说明
连接	允许用户连接到另一个会话。注意：连接到目前正由另一个用户使用的会话可能导致该用户的数据丢失。连接到另一个会话时，将从以前的会话中断开连接。如果在服务器上创建多个会话，则可以使用此选项在这些会话之间切换。不能从系统控制台连接到另一会话
断开连接	从会话中断开用户连接。在断开连接状态下，该会话会依然保持与终端服务器的连接，而且目前运行的应用程序将继续运行。当尝试重新连接到该服务器时，即使从不同的计算机重新连接，也将使用断开连接的同一会话重新连接。在断开连接时仍打开着的应用程序在重新连接到该会话时仍会运行，而不会有数据丢失。如果经常变换地点（例如，从办公室到家中），那么该特性将非常有用
发送消息	允许用户向另一个用户的会话发送消息。例如，在从会话中断开连接或注销用户之前，管理员可能需要向用户发送消息
远程控制	使用户可以观察或远程控制另一用户会话，允许监视会话中的活动并在必要时与之交互作用。要监视其会话的用户在开始监视之前将收到警告。远程控制可使用“终端服务配置”功能进行配置，也可使用“本地用户和组”以及“Active Directory 用户和计算机”的终端服务扩展程序在每用户基础上配置。不能从控制台远程控制另一会话
重置	允许立即删除会话。请注意，没有警告地重置用户会话可能导致该会话中的数据丢失。应该只在会话出现故障或停止响应时重置会话。重置侦听者会话将使用该连接重新设置所有会话
状态	允许监视与会话相关的计数器，如传入和传出的字节和帧。控制台和侦听者会话的状态信息无法显示
注销	允许从服务器上的会话中注销用户。注意：没有警告的注销用户可能会导致用户会话中的数据丢失。当注销用户时，所有进程都将结束而且该会话将从服务器上删除
结束进程	允许结束运行在用户会话上的进程。这在应用程序停止响应时非常有用。注意：没有警告地结束进程可能导致用户会话中的数据丢失

终端服务器与远程控制台之间的会话有许多不同的状态，并受终端服务管理器所控制。表 9-10 则描述了每一种可能的会话状态。

表 9-10 终端服务的会话状态表

会话状态	说明
活动	该会话已经连接，而且用户已登录到服务器上
已连接	该会话已经连接，但没有用户登录到服务器上

连接查询	该会话正在连接过程中。如果一直是这种状态，表明连接有问题
远程控制	该会话正在远程控制另一会话
侦听	该会话准备接受客户机连接
已断开连接	此用户已从会话中断开连接，但该会话仍连接在服务器上，而且可以随时重新连接
空闲	该会话将被初始化并准备接受连接。要优化服务器的性能，两个默认（空闲）会话将在任何客户机连接之前自动初始化
关闭	会话不能正确初始化或者不能被终止，因此无法使用。如果一直是这种状态，表明会话的连接有问题
初始化	正在初始化该会话

9.2.6 终端服务安全性增强

终端服务的默认监听端口为 3389，这是非常不安全的。因为包括攻击者在内的任何客户都可以通过终端服务客户连接器（远程桌面连接）连接这个默认的端口，尝试登录终端服务器来达到远程控制的目的。

可以参考以下方法更改终端服务的默认端口号。

（1）服务器端设置

运行 regedit.exe，展开注册表子键 HKLM \SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp，将 PortNumber 键值在十进制状态下设置成自定义的端口号，如 8888（只要该端口还未使用，不会产生冲突即可）。此外，展开注册表子键 HKLM \SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp，然后设置方法同上（端口号需要一致）。

（2）客户端设置

打开终端服务的客户端连接管理器，选择某个连接，导出连接文件（扩展名为 cns）。然后用文本编辑软件（如记事本）打开该 cns 文件，搜索“ Server Port ”字段，修改该值，使之与服务器的设置保持一致（注意进制的转换）。最后导入该 cns 文件至终端服务的客户端连接管理器即可，如图 9-28 所示。

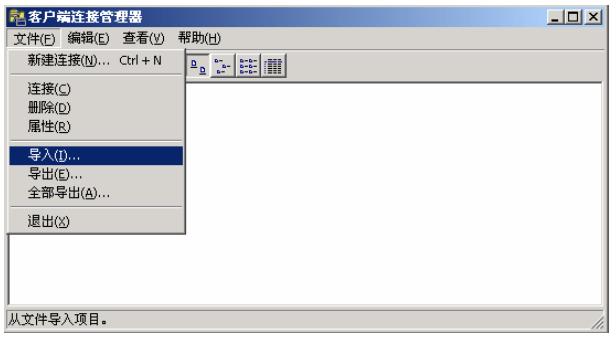

图 9-28 终端服务的客户端连接管理器