Windows安全原理与技术

— 第九章：应用服务安全

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

IIS 5.0

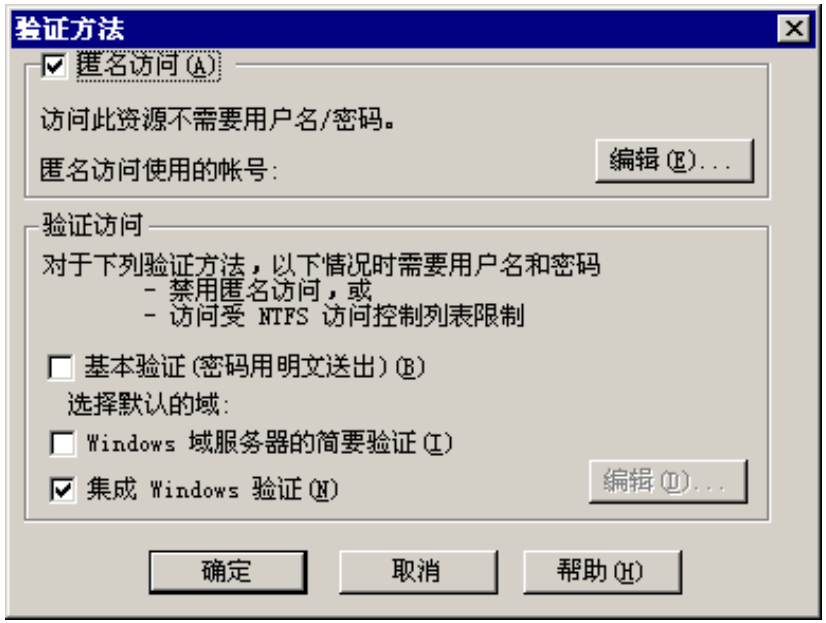
- IIS（Internet Information Server）5.0 是用来构建站点的Internet服务程序包。
- 组件：
  - Internet服务管理器
  - WWW服务器组件
  - FTP服务器组件
  - SMTP服务器组件
  - FrontPage 2000服务器扩展
  - …

IIS安全特性概述

- 身份验证
- 访问控制
- 权限设置
- 通信加密
  - SSL/TLS, IPSec
- 集成Windows 2000的其他安全特性
  - Kerberos协议
  - 活动目录服务
  - 证书服务
  - 高强度加密包

IIS的身份验证（1）

- **Web的身份验证**
  - Web站点的“属性”→ “目录安全性”→“匿名访问和访问控制” →“编辑”

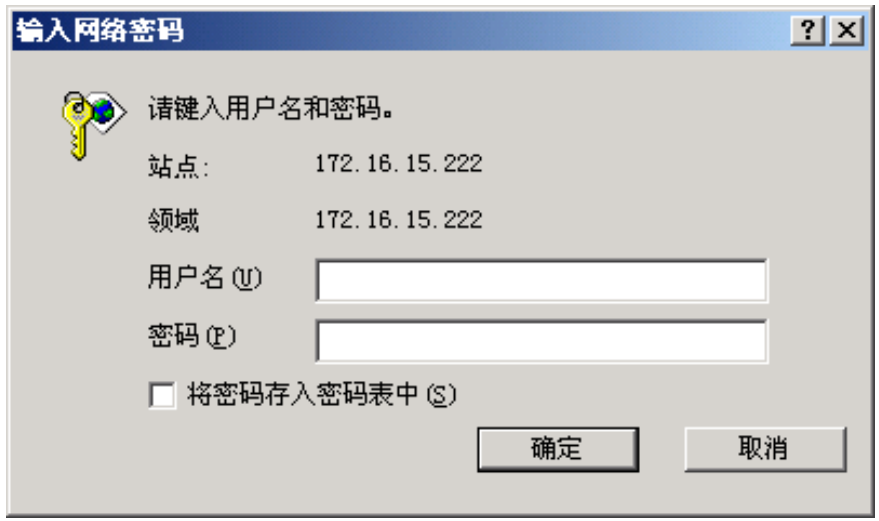


匿名访问

- 其实就没有身份验证。
- 在客户访问服务器资源时，IIS把用户映射到并模拟IUSR_COMPUTERNAME这个本地Guests组账户。

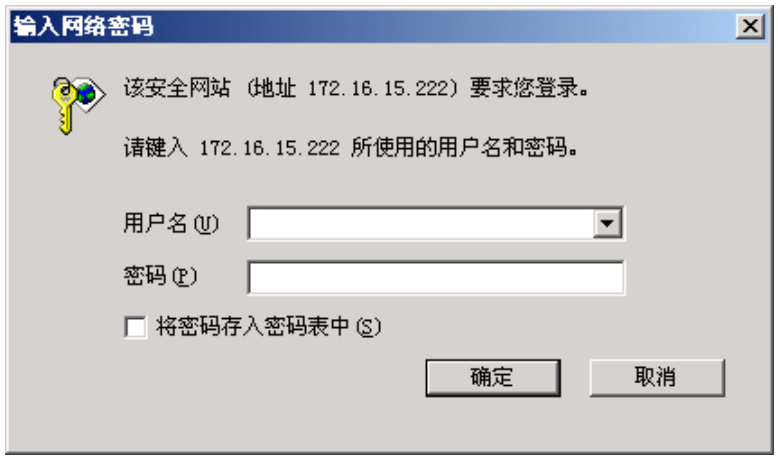
基本身份验证

- Web浏览器提示用户输入正确的登录用户名和口令，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。
- 优势：符合HTTP标准，在多数浏览器上已实现。
- 缺陷：明文传输（Base64编码），泄漏登录信息。



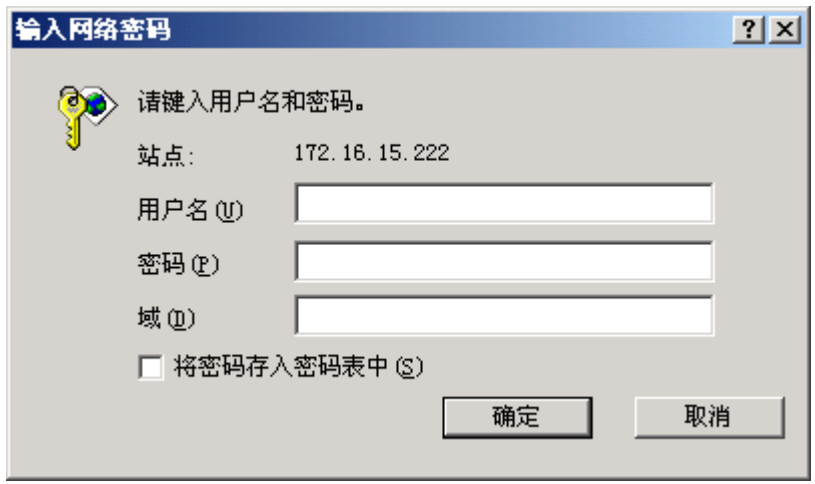
域服务器的简要（摘要）身份验证

- 是一种质询—应答（Challenge—Response）机制。
- 以非明文的传输形式提供关于用户口令的信息。
- 身份验证的处理过程：
  - 服务器向浏览器发送信息（质询）。
  - 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。
  - 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。
  - 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。如果两个摘要相同，则身份验证成功。



集成Windows身份验证

- 由Kerberos v5与质询—应答身份验证协议组成。
- 非明文的传输形式。
- 身份验证的处理过程
  - 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。
  - 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。

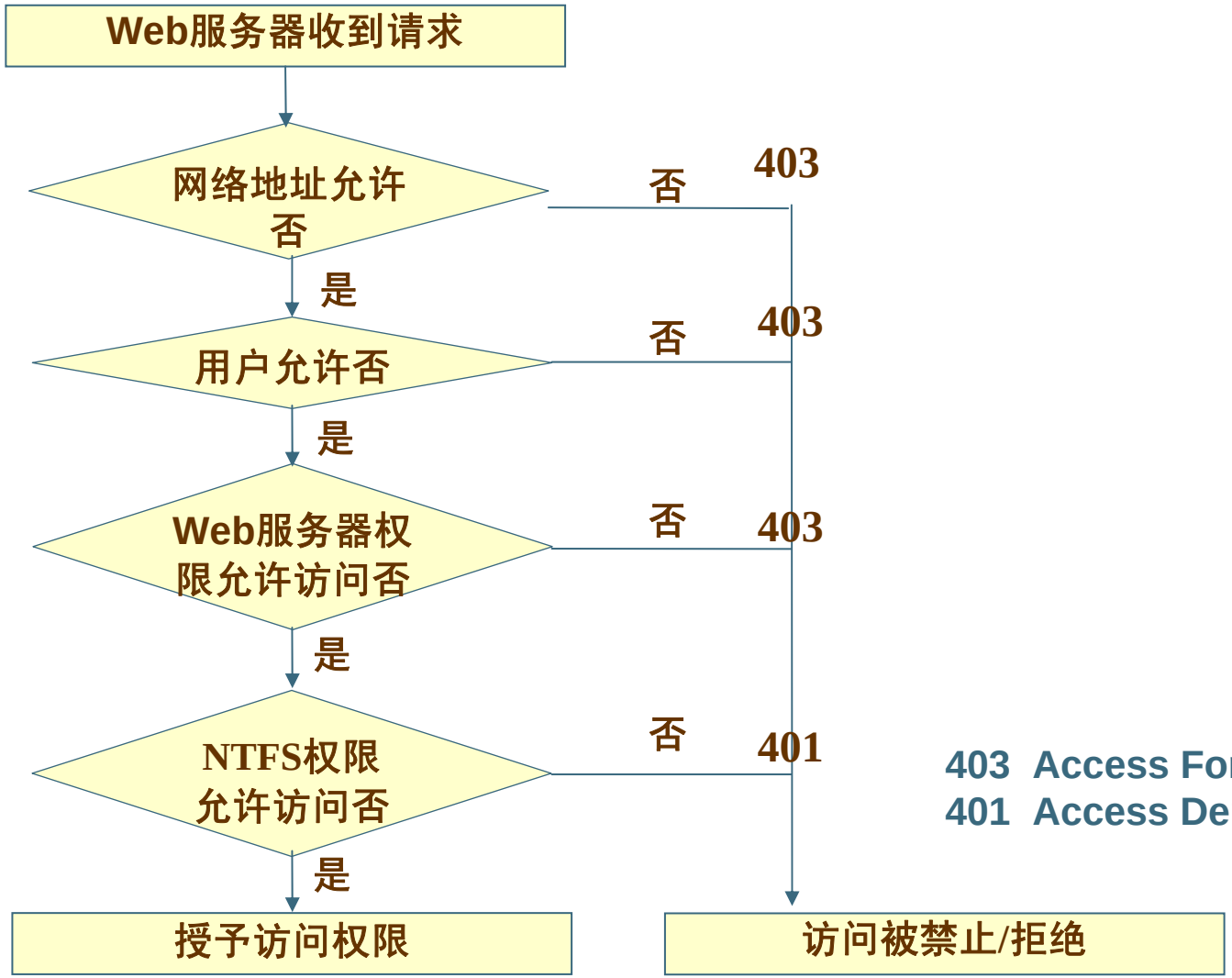


IIS的身份验证（2）

- FTP的身份验证
  - FTP站点的“属性”→ “安全账号”→“允许匿名连接”

- **FTP身份验证的不安全性**
  - 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。
  - 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。

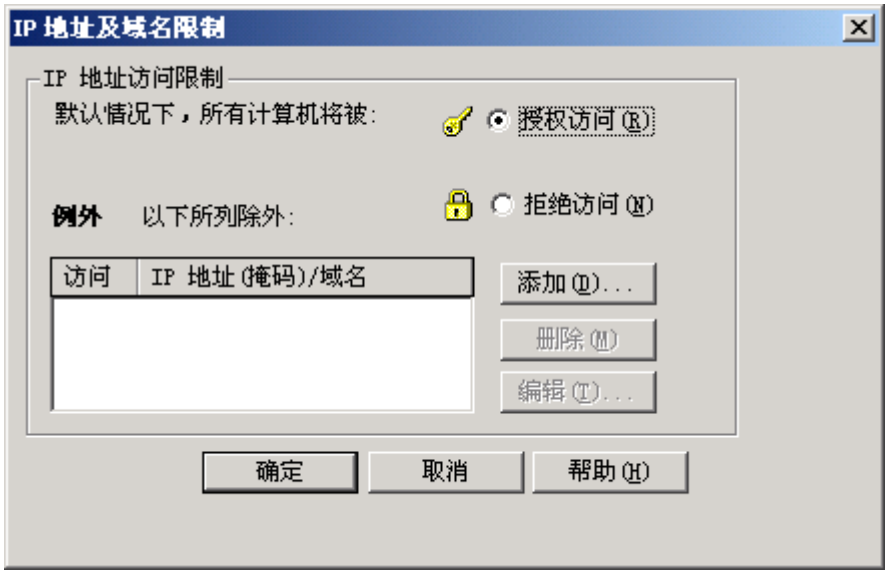
IIS的访问控制



403 Access Forbidden（访问被禁止）
401 Access Denied（访问被拒绝）

网络地址的访问控制

- Web站点的“属性”→ “目录安全性”→ “IP地址及域名限制” →“编辑”
- FTP站点的“属性”→ “目录安全性”→ “TCP/IP访问控制”

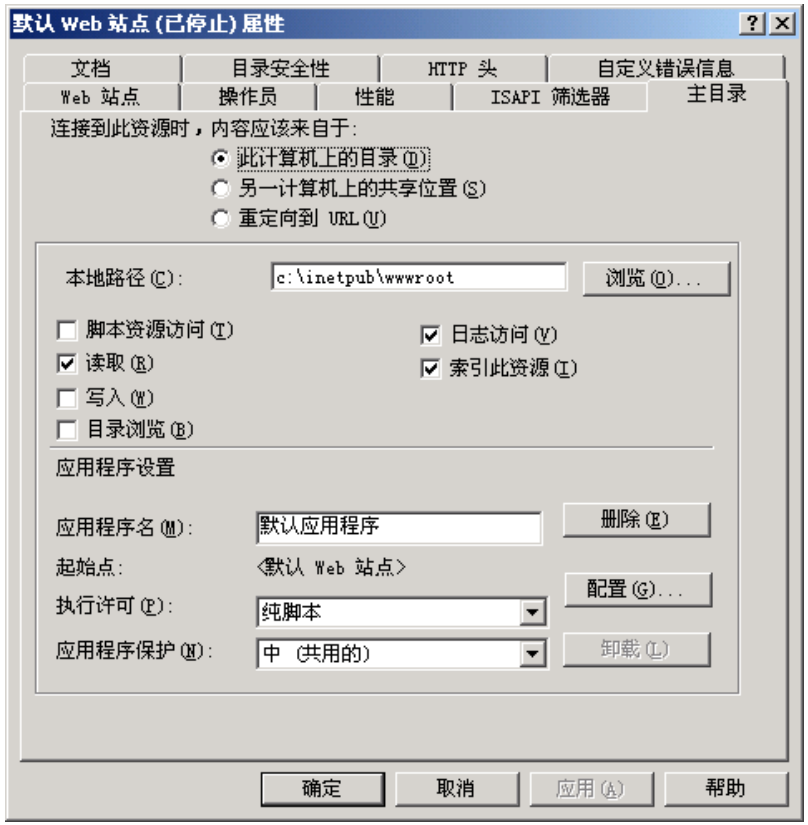


网络地址访问控制的方式

- 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。
- 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。

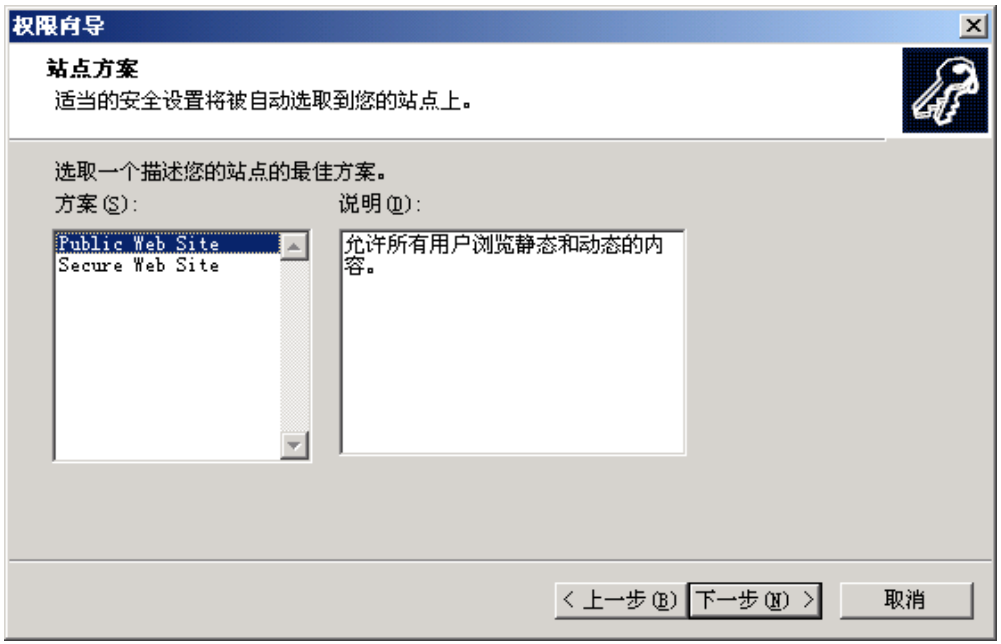
IIS服务器的权限

- 权限设置包括脚本资源访问、读取、写入、目录浏览等。
- 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。
- 在特定级别设置的权限会被其下面的子对象所继承。



权限向导

- Web/FTP站点的“属性”→ “所有任务”→“权限向导”



- **IIS的应用程序保护**
  - 低（IIS进程）
  - 中（公用的）
  - 高（独立的）
- **IIS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asp、jsp以及Perl脚本等）。
  - 脚本和可执行程序
    - 允许运行任何应用程序。

IIS的安全配置

- Windows 2000本身的安全配置
- IIS本身的安全配置

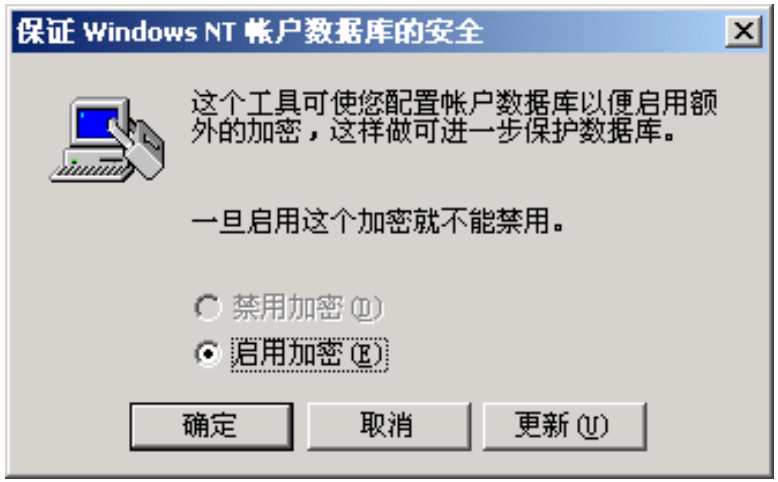
IIS的用户同时也是Windows操作系统的用户，并且IIS目录的权限受到Windows中NTFS文件系统的权限控制，因此，要创建一个安全可靠的Web服务器，必须要实现Windows操作系统与IIS服务器的双重安全。

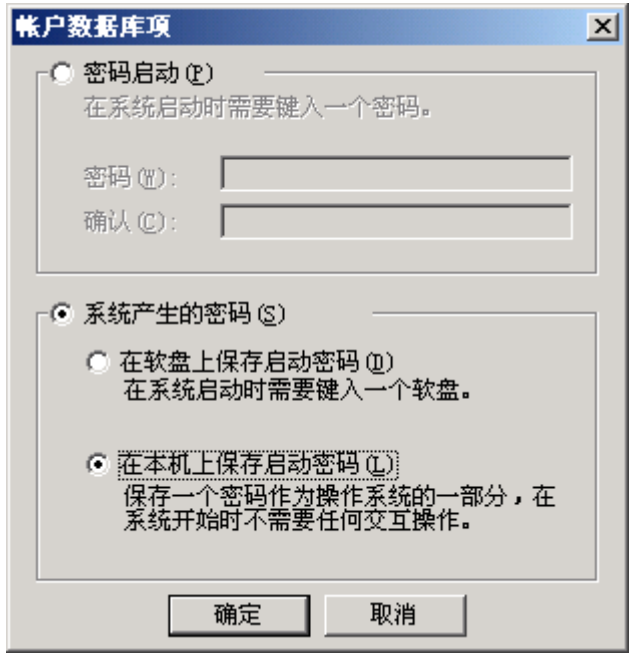
Windows 2000的基本安全配置

- 安装最新的补丁，包括Service Packs和Hotfixes
- 对系统服务的启动方式重新进行规划
- 强化SAM数据库的保护
- 更改网络连接属性
- 增强密码的复杂度
- 消除空连接安全漏洞
- 删除默认网络共享
- 改写注册表降低被攻击风险
- 去除对其他操作系统的支持
- 合理调整页面文件的设置

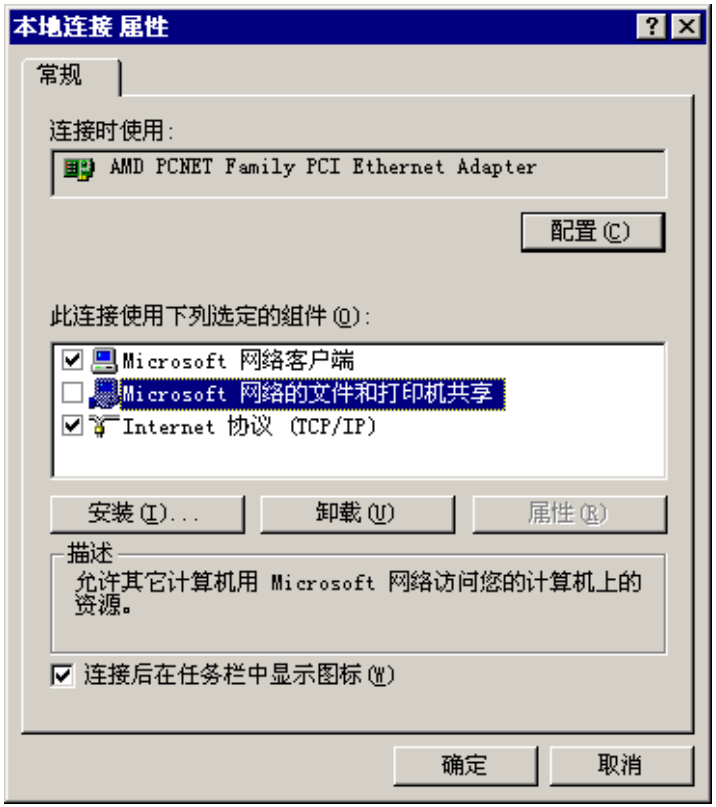
强化SAM数据库的保护

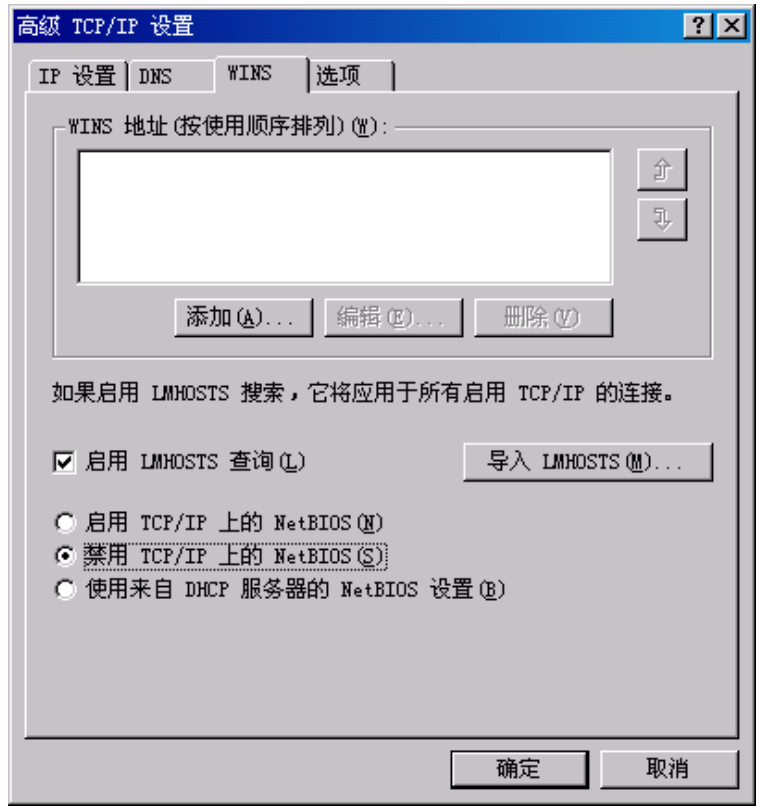
- **Syskey.exe**
  - 管理员创建密码，使用密码启动。
  - 系统生成密码，在软盘上存储启动密码。
  - 系统生成密码，本地存储启动密钥。





更改网络连接属性





禁用Netbios协议

删除默认网络共享

对于服务器而言:

Key:
HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Name: AutoShareServer
Type: DWORD
Value: 0

对于工作站而言:

Key:
HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Name: AutoShareWks
Type: DWORD
Value: 0

改写注册表降低被攻击风险

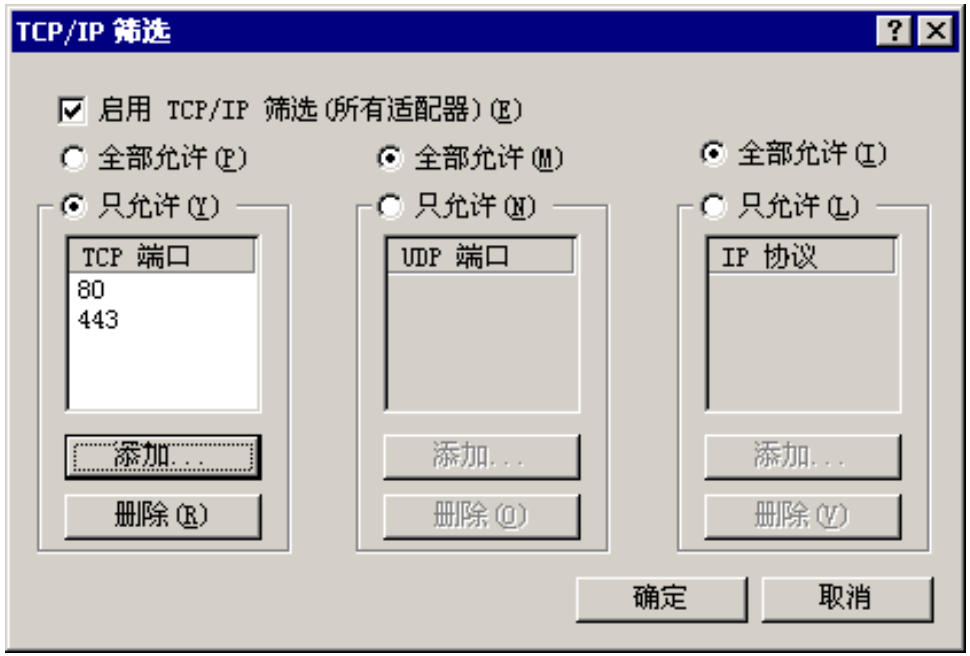
- 抵抗拒绝服务攻击
  - 更改注册表中关于TCP/IP协议栈的参数 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

SynAttackProtect	REG_DWORD	2
EnablePMTUDiscovery	REG_DWORD	0
NoNameReleaseOnDemand	REG_DWORD	1
EnableDeadGWDetect	REG_DWORD	0
KeepAliveTime	REG_DWORD	300,000
PerformRouterDiscovery	REG_DWORD	0
EnableICMPRedirects	REG_DWORD	0

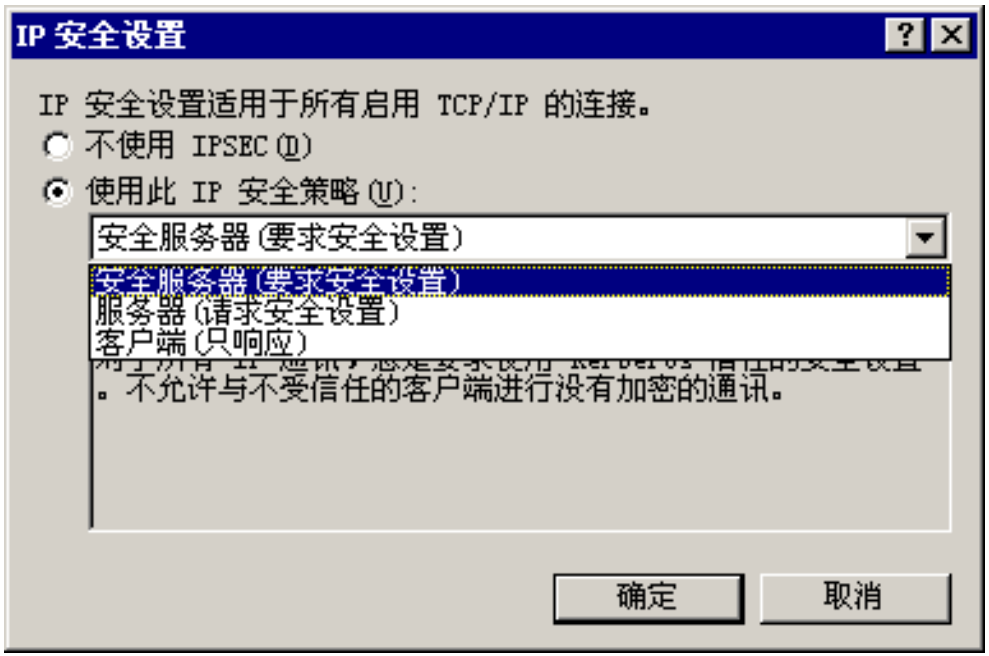
安全配置IIS 5.0

- TCP/IP筛选配置
- IP安全策略过滤器
- 单独设置IIS服务器
- 合理设置Web根文件夹
- 为重要系统文件改头换面
- 删除危险的IIS组件
- 简化IIS5中的验证方法
- 为IIS5中的文件分类设置权限
- 全力保护IIS metabase
- 使用IP地址和域名限制访问

TCP/IP筛选配置


TCP/IP 筛选
启用 TCP/IP 筛选(所有适配器)(E)
全部允许(P)
只允许(Y)
TCP 端口
80
443
添加...
删除(R)
全部允许(M)
只允许(N)
UDP 端口
添加...
删除(O)
全部允许(I)
只允许(L)
IP 协议
添加...
删除(V)
确定
取消

IPSec安全策略过滤器



单独设置IIS服务器

- 安装在一个单独的服务器上
  - 非域成员
  - 不传递任何认证信息
- 禁止不必要的服务

Alerter	Netlogon	Spooler
Clipbook Server	Network DDE	NetBIOS Interface
Computer Browser	Network DDE DSDM	TCP/IP NetBIOS Helper
DHCP Client	Network Monitor Agent	NWLink NetBIOS
Messenger	Simple TCP/IP Services	

合理设置Web根文件夹

- 在新的目录下新建WWW服务与FTP服务，建议不使用默认路径。（%SYSTEMDRIVE%\Inetpub\wwwroot）
  - 不同目录上
  - 不同磁盘分区上
  - 另一台服务器上
- 对能够被写入文件的目录启用磁盘配额限制功能。

为重要系统文件改头换面

- 对下列重要系统文件
  - 删除
  - 重命名
  - 设置严格的NTFS权限

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		

删除危险的IIS组件

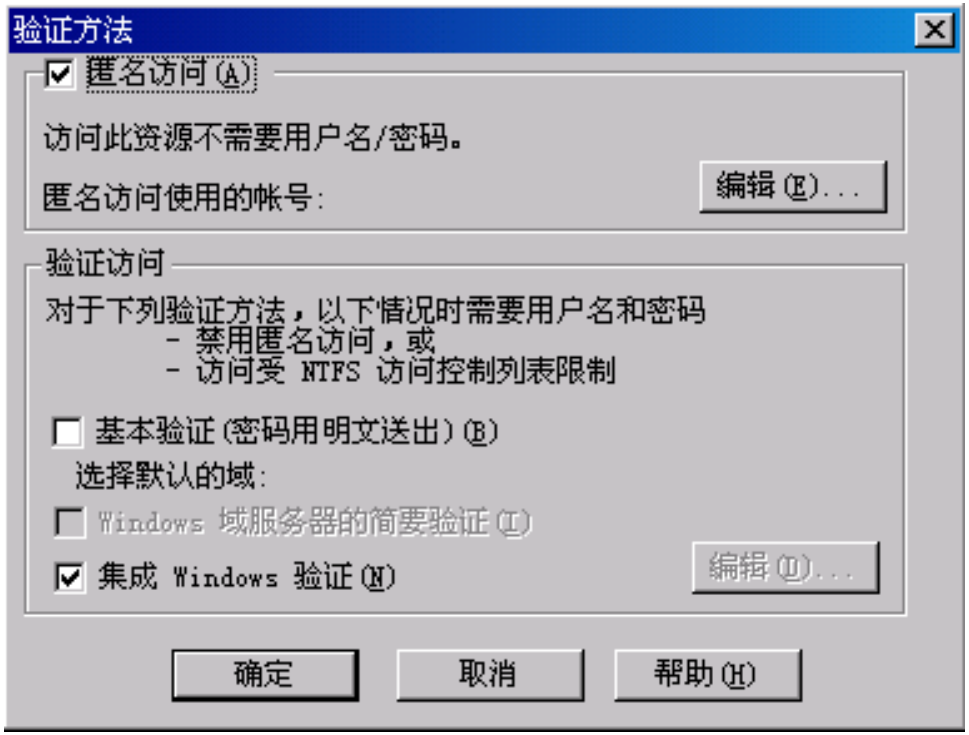
- 删除所有示例程序
- 删除虚拟目录
- 删除不使用的应用程序映射关联

删除不使用的应用程序映射关联

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	.stm, .shtm .shtml
Internet打印	.printer
索引服务（Index Server）	.htw, .ida, .idq

安装新的Service Pack后，IIS的应用程序映射应重新设置。

简化IIS中的验证方法



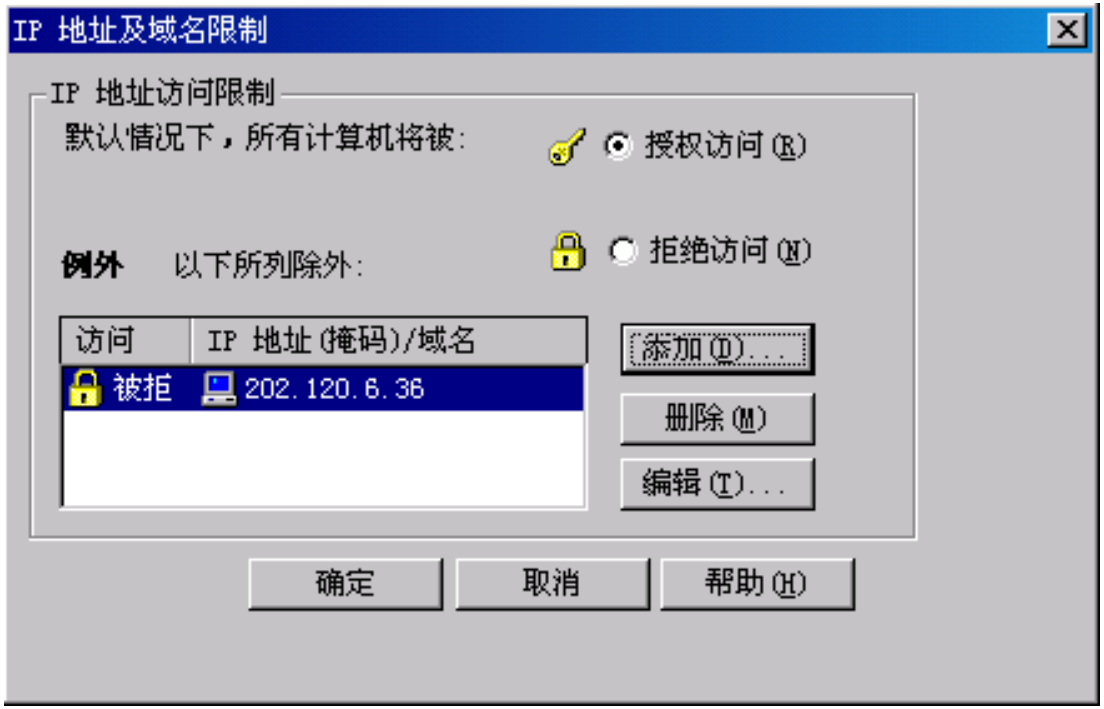
为IIS服务器的文件分类设置权限

- 为不同类型的文件创建不同的目录
  - 静态文件
  - 脚本文件
  - 程序文件
  - 包含文件
- 为不同类型的虚拟目录设置适当的访问权限
  - Everyone：Read/Execute
  - Administrators：Full Control
  - System：Full Control

保护IIS Metabase

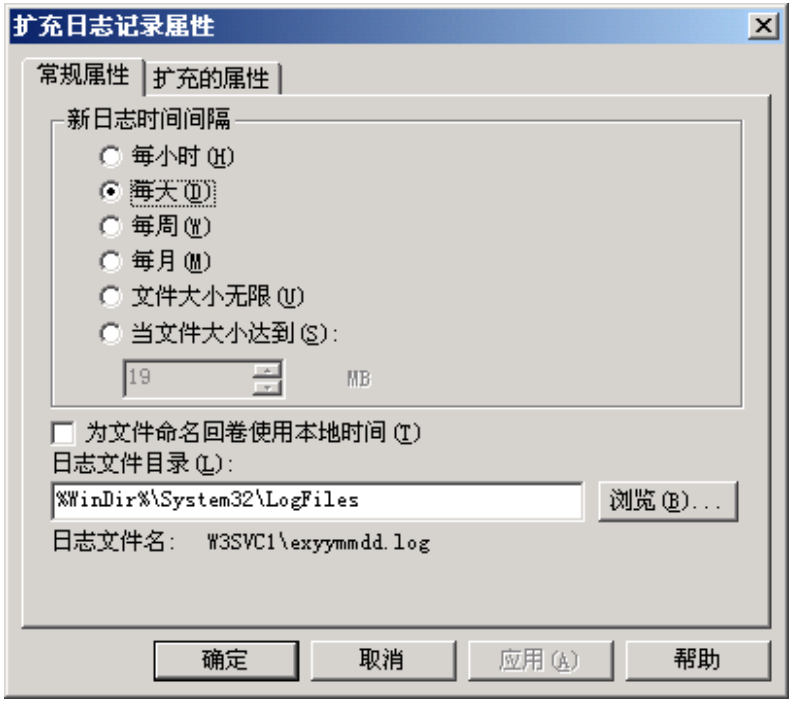
- IIS Metabase
  - 保存着包括口令在内的几乎IIS配置各个方面的内容，而且这些信息都以明文形式存储。
  - 位于%systemroot%\system32\inetsrv\
- 安全保护措施
  - 设置访问权限。
    - Administrators:Full Control，System:Full Control
  - 审核对MetaBack目录的所有失败访问尝试。
  - 转移包含IIS所有管理脚本的目录。
    - %systemdrive%\Inetpub\Adminscripts

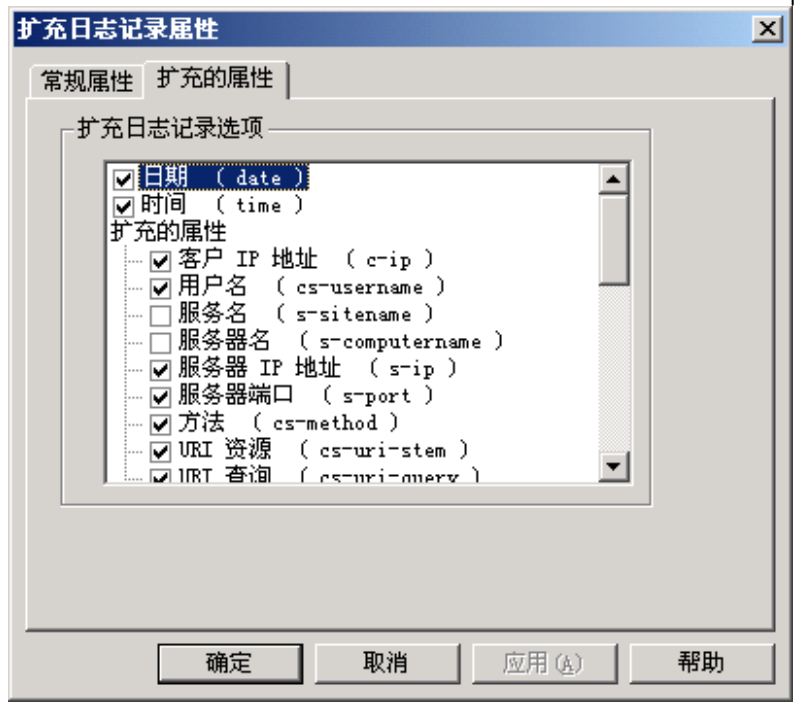
使用IP地址和域名限制访问



IIS的安全审计

- 管理
  - 站点属性 → 启用日志记录
- 日志格式
  - W3C扩充日志文件格式
- 日志属性
  - 日志存放路径：%WinDir%\System32\LogFiles。
  - 日志记录间隔：每天。
  - 日志记录格式。
- 设置合适的日志目录访问权限
  - Administrators：完全控制。
  - System：完全控制。
  - Everyone：读取，写入，更改。


扩充日志记录属性
常规属性
扩充的属性
新日志时间间隔
每小时(H)
每天(D)
每周(W)
每月(M)
文件大小无限(U)
当文件大小达到(S):
19
MB
为文件命名回卷使用本地时间(T)
日志文件目录(L):
%WinDir%\System32\LogFiles
浏览(B)...
日志文件名: W3SVC1\exyymmdd.log
确定
取消
应用(A)
帮助


扩充日志记录属性
常规属性
扩充的属性
扩充日志记录选项
日期 (date)
时间 (time)
扩充的属性
客户 IP 地址 (c-ip)
用户名 (cs-username)
服务名 (s-sitename)
服务器名 (s-computername)
服务器 IP 地址 (s-ip)
服务器端口 (s-port)
方法 (cs-method)
URI 资源 (cs-uri-stem)
确定
取消
应用(A)
帮助

使用IIS Lockdown和URLScan

- **IIS Lockdown**
  - 帮助管理员有效防止IIS的已知漏洞，关闭一些不需要的功能。
  - 提供了许多内置的模板。
- **URLScan**
  - 集成在Lockdown之中
  - 提供深层次的锁定
  - 实质是URL的过滤
    - HTTP协议字段
    - 请求文档的后缀

IIS Lockdown的执行步骤

- 锁定文件
- 禁用服务和组件
- 安装 URLScan
- 删除不需要的 Internet 服务器应用程序编程接口 (ISAPI) DLL 脚本映射
- 删除不需要的目录
- 更改 ACL

IIS 6.0的安全性 — 默认安全

- IIS 6.0的默认安装被设置为仅安装静态HTML页面显示所需的组件，而不允许动态内容。

IIS 组件	IIS 5.0 默认安装	IIS 6.0 默认安装
Static file support（静态文件支持）	启用	启用
ASP（动态服务器脚本）	启用	禁用
Server-side includes（服务器端包含）	启用	禁用
Internet Data Connector（Internet数据连接器）	启用	禁用
WebDAV	启用	禁用
Index Server ISAPI（索引服务）	启用	禁用
Internet Printing ISAPI（Internet打印）	启用	禁用
CGI（公共网关接口）	启用	禁用
Microsoft FrontPage server extensions （FrontPage服务器端扩展）	启用	禁用
Password change interface（更改密码界面）	启用	禁用
SMTP	启用	禁用
FTP	启用	禁用
ASP.NET	无	禁用
Background Intelligence Transfer Service（后台智能传输服务）	无	禁用

IIS 6.0的安全性 — 默认安全

- 默认不安装应用范例
  - 不再包括任何类似showcode.asp或codebrws.asp等的范例脚本或应用，这些程序原被设计来方便程序员快速察看和调试数据库的连接代码。
- 增强的文件访问控制
  - 匿名帐号不再具有web服务器根目录的写权限。
  - FTP用户被相互隔离在他们自己的根目录中。

IIS 6.0的安全性 — 默认安全

- 虚拟目录不再具有执行权限
  - 虚拟目录中不再允许执行可执行程序。这样避免了大量的存在于早期IIS系统中的目录遍历漏洞、上传代码漏洞以及MDAC漏洞。
- 去除了子验证模块
  - 去除了IISSUBA.dll。任何在早期IIS版本中，需要该DLL模块来验证的账号，现在需要具有“从网络上访问这台计算机”的权限。
- 父目录被禁用
  - 默认禁用了对父目录的访问，可以避免攻击者跨越web站点的目录结构，访问服务器上的其他敏感文件，如SAM文件等。

IIS 6.0的安全性 —安全设计

- 改善的数据有效性
  - IIS 6.0设计上的一个主要新特性是工作在内核模式的HTTP驱动—HTTP.sys。它不仅提高了web服务器的性能和可伸缩性，而且极大程度的加强了服务器的安全性。
  - HTTP.sys首先解析用户对web服务器的请求，然后指派一个合适的用户级工作进程来处理请求。工作进程被限制在用户模式以避免它访问未授权的系统核心资源。从而极大的限制了攻击者对服务器保护资源的访问。

改善的数据有效性

- 通过在HTTP.sys中进行特殊的URL解析设置以实现IIS 6.0安全设计中的深度防御原则。这些设置还可以通过修改注册表中特定的键值来进一步优化。

HKLM\System\CurrentControlSet\Services\HTTP\Parameters

AllowRestrictedChars	布尔值内容，非零值表明允许接受十六进制编码的URL请求。默认值为0。（推荐设置），以迫使请求在服务器级就进行输入检查。若设置为1可能导致攻击者通过十六进制编码的恶意请求来绕过输入检查。
MaxFieldLength	设置每个HTTP头的大小上限（以Byte为单位），默认值是16KB。
MaxRequestBytes	确定请求行和HTTP头的总大小上限。默认值也是16KB。
UrlSegmentMaxCount	决定服务器可以接受的URL地址中目录深度的最大值。它有效地限制用户URL请求中的反斜杠“/”的数量。建议将这个值根据web目录的深度进行严格控制，以避免遭受文件遍历攻击。默认值为255。
UrlSegmentMaxLength	决定URL请求中每个路径段的字符长度的最大值。这个值也应该根据主机的普通应用来设置，以避免接受超常地址请求而导致应用异常。默认值为260。
EnableNonUTF8	控制允许的字符编码格式。默认值1允许接受ANSI和DBCS编码的URL地址，其他值允许UTF8的编码格式。

IIS 6.0的安全性 —安全设计

- 增强的日志机制
  - HTTP.sys的错误日志：包括发生错误的时间戳、来源目的IP和端口、协议版本、HTTP动作、URL地址、协议状态、站点ID和HTTP.sys的原因解释等条目。
- 快速失败保护
  - 除了修改注册表，管理员还可以通过服务器设置，来使那些在一段时间内反复失败的进程关闭或者重新运行。
- 应用程序隔离
  - 在处理请求时，将应用程序隔离成一个个叫做应用程序池的孤立单元，成倍的提高了性能。

IIS 6.0的安全性 —安全设计

- 坚持最小特权原则
  - HTTP.sys中所有代码都是以Local System权限执行的，而所有的工作进程，都是以Network Service（Windows 2003中新内置的一个被严格限制的账号）的权限执行的。
  - 允许管理员执行命令行工具，从而避免命令行工具的恶意使用。

终端服务

- 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。

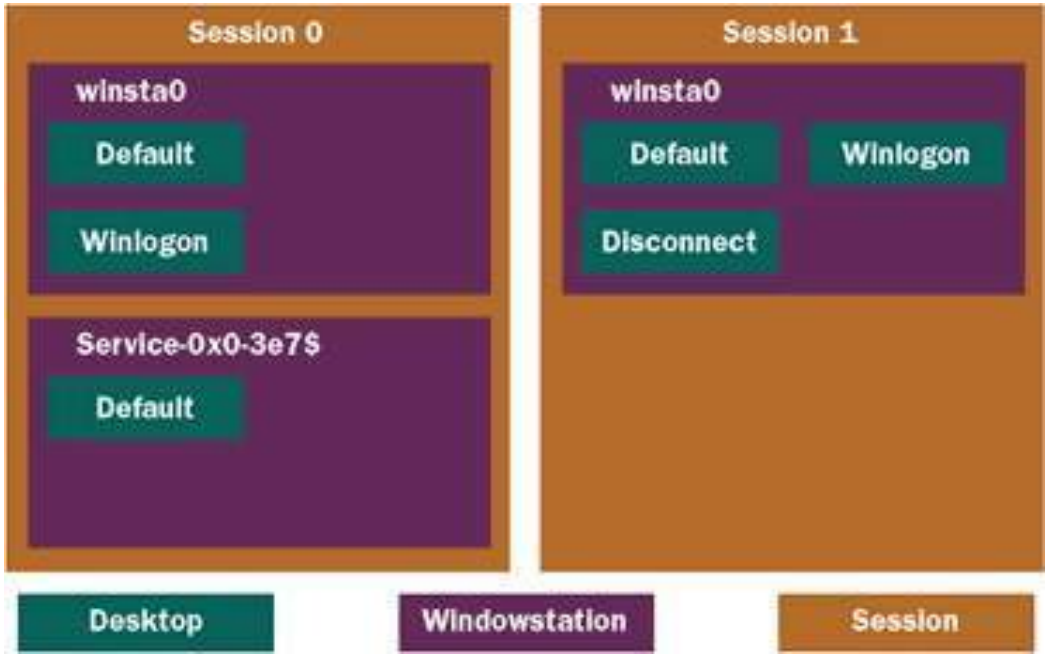
瘦客户端

终端服务的工作原理

- 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。

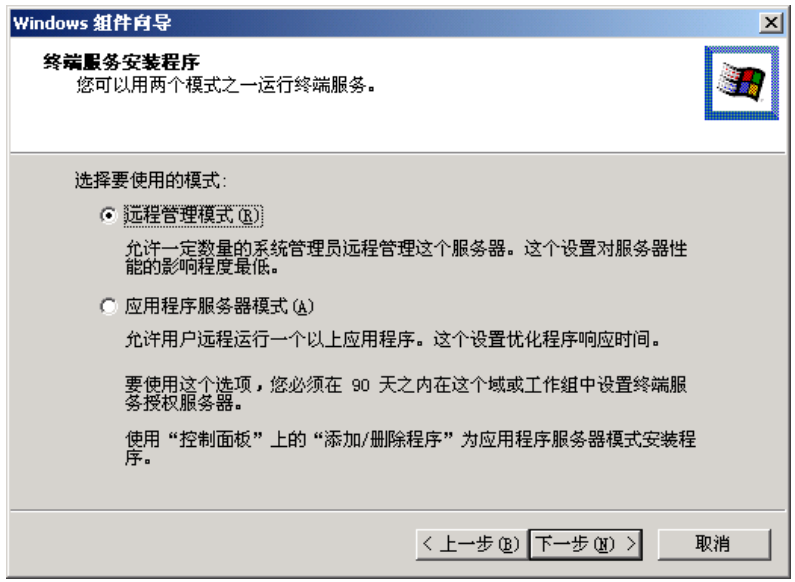
终端服务的会话隔离特性

- 本地控制台程序与系统服务程序运行在默认的会话0（Session 0）中，而第一个终端登录会话则为会话1（Session 1），第二个终端登录会话则为会话2（Session 2）。



终端服务的操作模式

- 远程管理模式
  - 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。
  - 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，所以开销很小。
  - 最多允许两个同时的远程管理连接。
- 应用程序模式
  - 管理员可以从一个中心位置部署和管理应用程序。
  - 客户端需要客户端访问许可证。

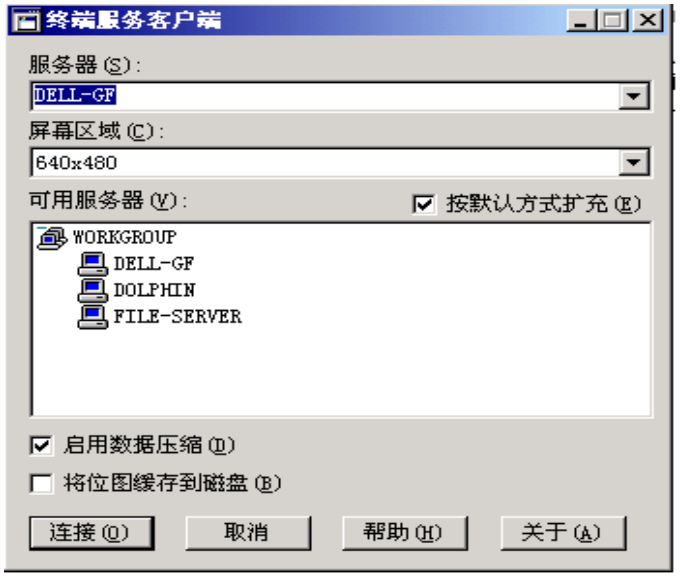


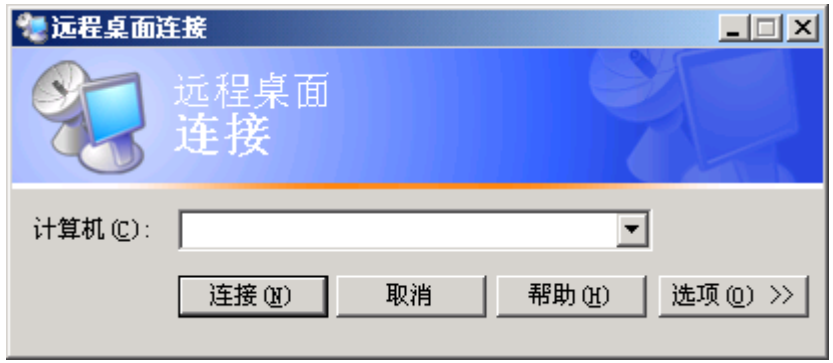
终端服务组件

- Windows 2000服务器多用户内核
- 远程桌面协议（RDP）
  - 客户端与网络上的终端服务器进行通信所使用的协议
- 终端服务客户端软件
- 终端服务许可服务
  - 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）。
- 终端服务系统管理工具
  - 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
  - 终端服务管理器

终端服务的客户端软件

- 用来在客户机上显示用户熟悉的Windows用户界面。
  - 建立和维护客户端与运行终端服务的服务器之间的连接。
  - 将所有的用户输入如键盘录入或鼠标移动传送给服务器。
  - 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。



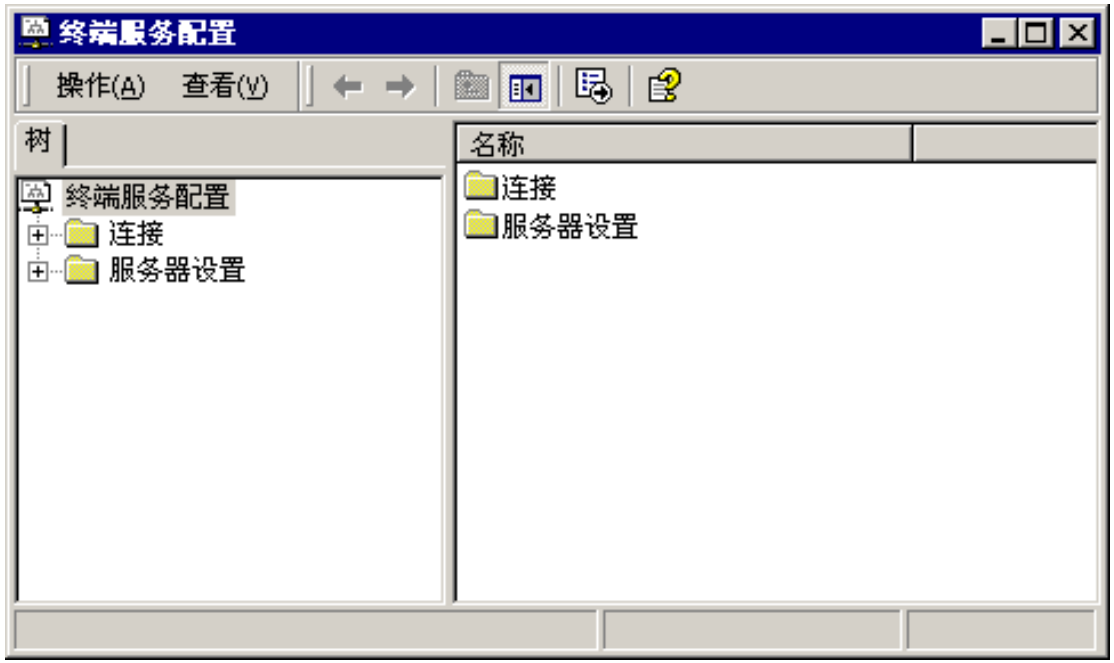


远程桌面连接 — Mstsc.exe

超过2个连接时，可以使用如下命令来强制登录:
mstsc /console /v:ip:port

终端服务的配置

- 可配置的内容
  - 管理连接
  - 配置连接属性
  - 配置服务器设置



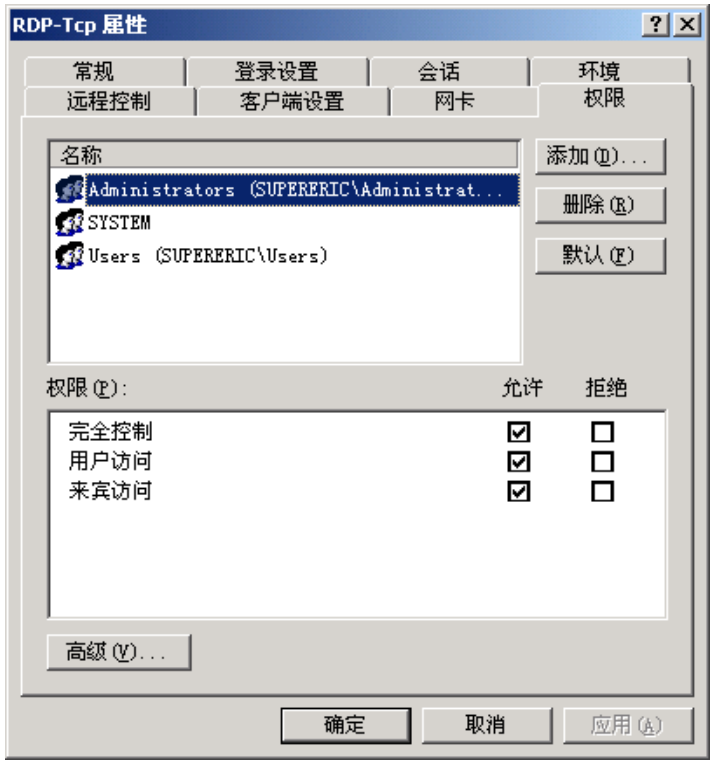
管理工具 → 终端服务配置

配置连接属性

- 最大连接数
- 数据加密级别
- 登录设置
- 会话设置
- 环境设置
- 远程控制设置
- 客户端设置
- 权限设置

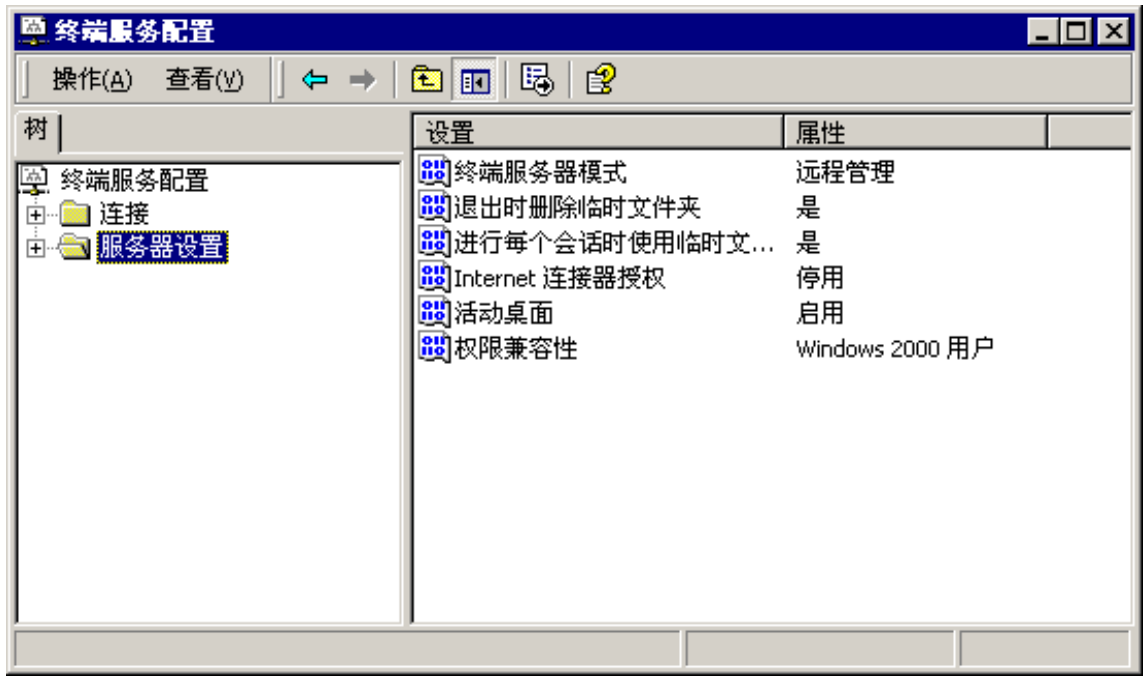
终端服务的权限

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



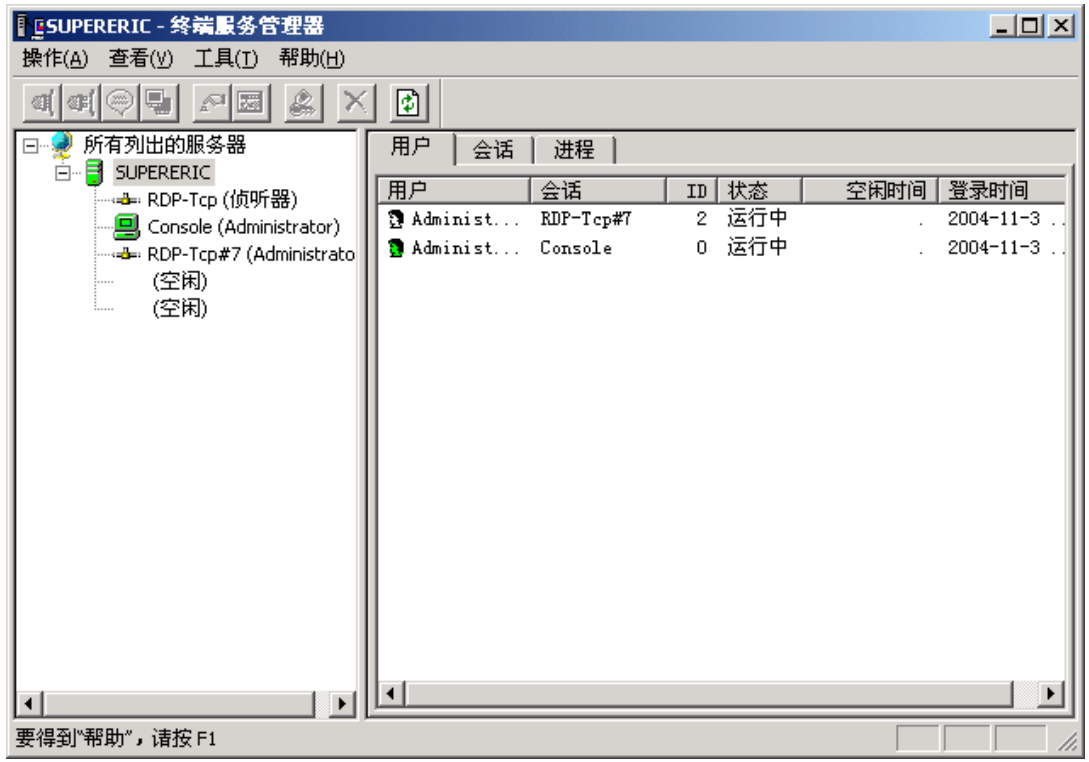
配置服务器设置

- 查看和更改终端服务模式
- 退出时是否删除临时文件夹
- 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
- 查看和更改权限兼容性



终端服务的管理

- 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。



管理工具 → 终端服务管理器

会话类型

- 控制台会话
  - 在客户连接到终端服务器时自动出现在“会话”列表中。
  - 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。
- 侦听会话
  - 侦听并接受新的 RDP 客户连接，为客户请求创建新的会话。
- 空闲会话
  - 为了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。

终端服务的安全性增强

- 更改通信端口
  - 服务器端
    - HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp中的PortNumber

      HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp中的PortNumber
  - 客户端
    - XP/Server 2003的客户端连接软件：在“计算机”对话框中输入“IP地址：端口号”。
    - 2000的客户端连接软件：打开Terminal Server Client的客户端管理器，导出连接文件（后缀名为cns），用记事本打开该cns文件，搜索“Server Port”，修改该值，与服务器保持一致即可（注意进制的转换），最后导入该cns文件至Terminal Server的客户端管理器。

终端服务的登录审计

- 启用：终端服务配置→连接→属性→权限→高级→审核。
- 审计内容：一般来说，只要记录登录、注销事件即可。
- 审计日志查看：程序→管理工具→事件察看器。
- 缺陷：只记录主机名，并不记录IP地址。

手动实现登录审计

- 编写脚本，例如**Tslog.bat**
  - time /t >> TSLog.log
    netstat -n -p tcp | find ":3389“ >> TSLog.log
    start Explorer
- 设置用户的启动脚本，步骤：
  - 管理工具→终端服务配置→连接→属性→环境

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消