目录

01 系统加固

- Windows操作系统加固
- Linux操作系统加固

02 中间件加固

- IIS加固
- Apache加固
- Nginx加固

03 数据库加固

- Mysql加固
- Mongodb加固

IIS 安全加固

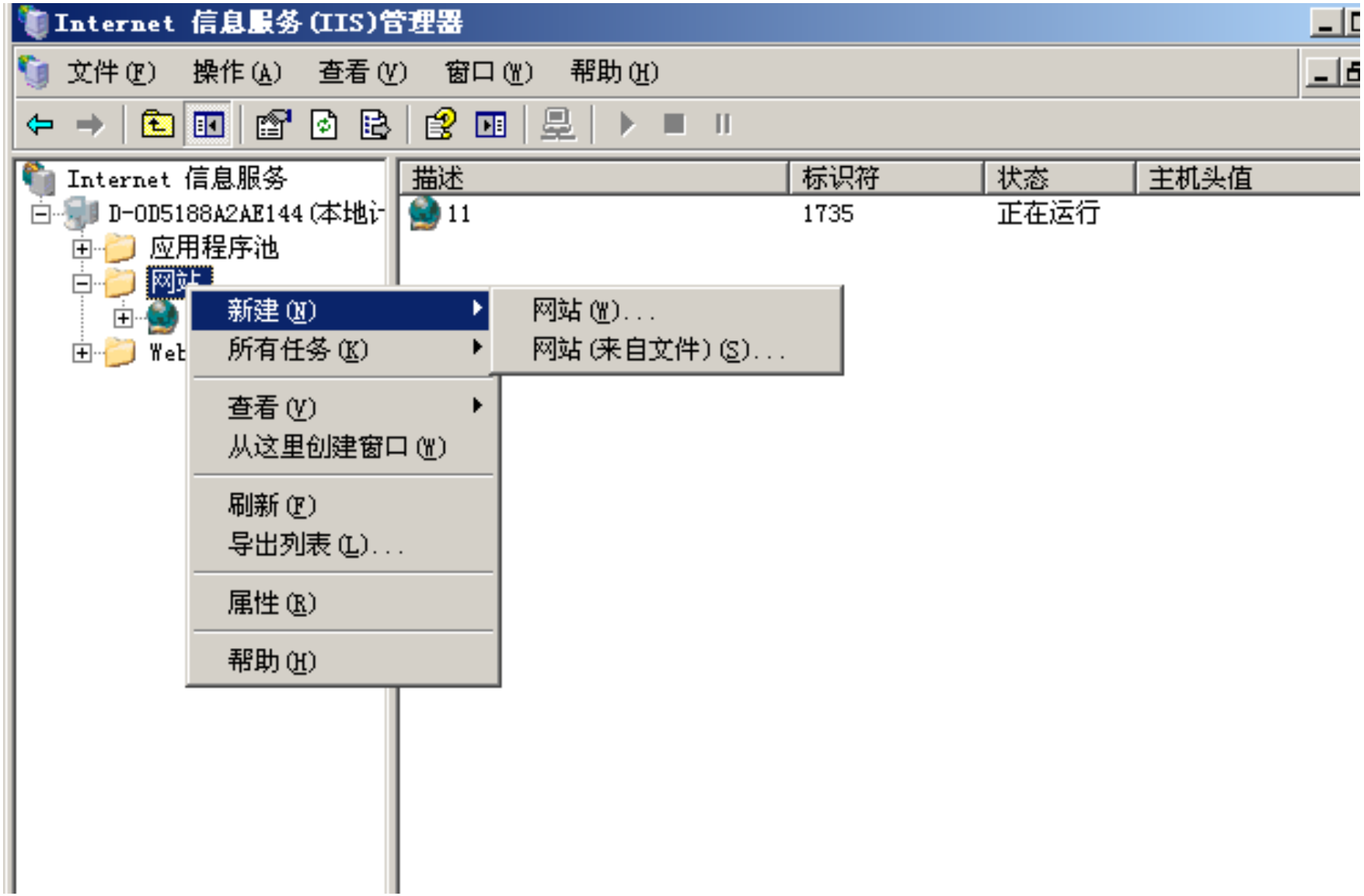
目录

01 IIS 网站搭建

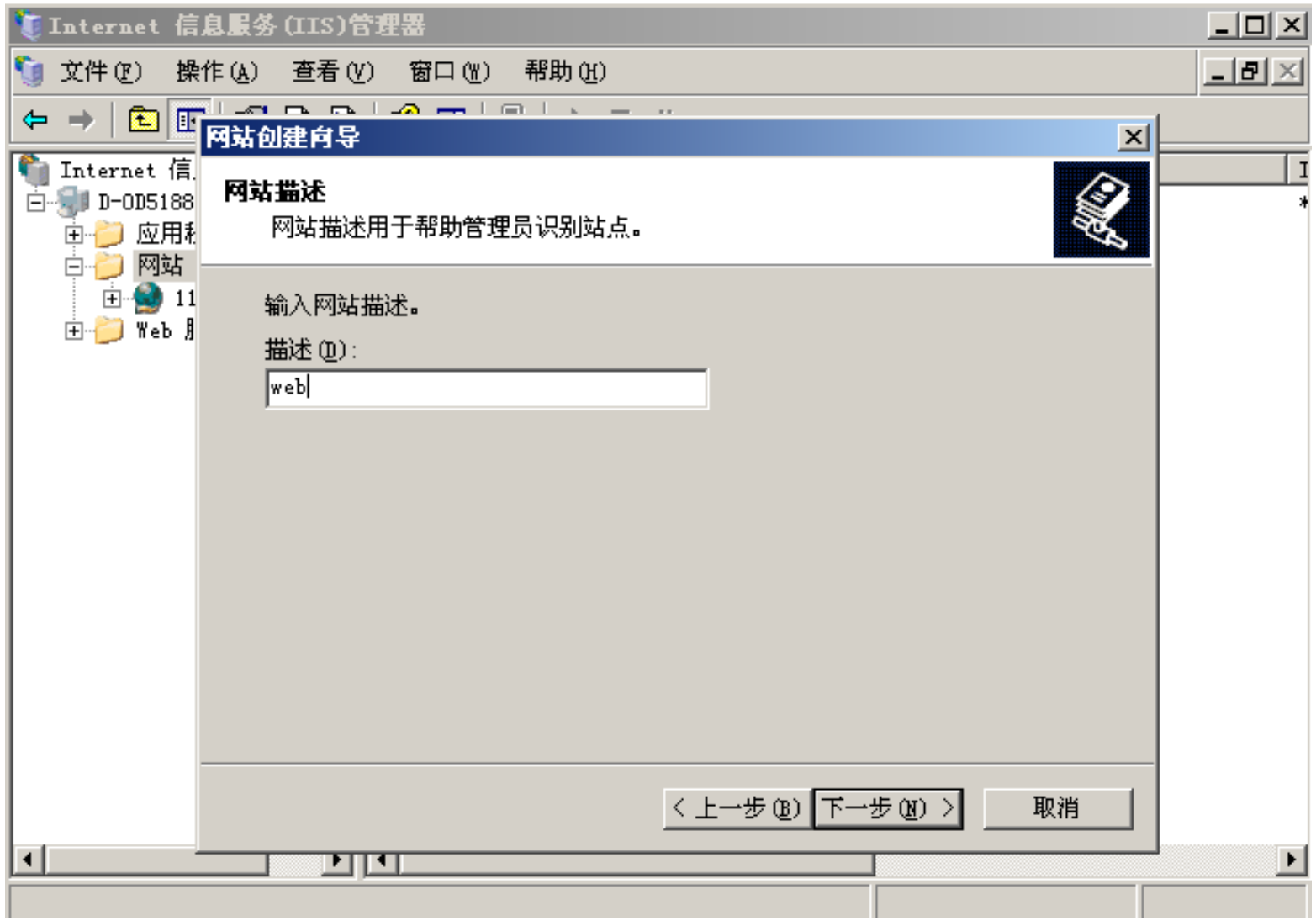
02 IIS 安全加固

IIS 网站搭建

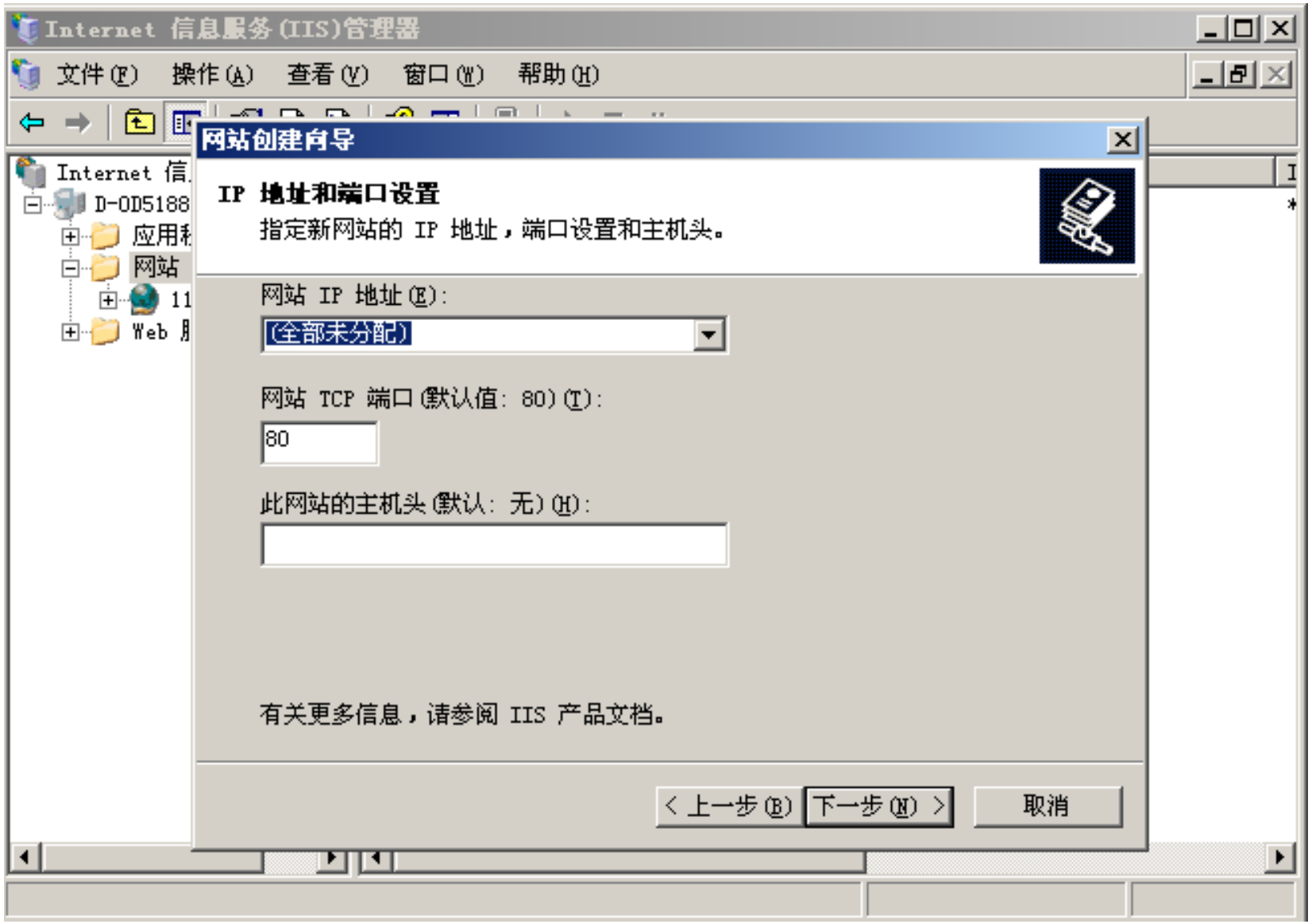
IIS新建网站


Internet 信息服务(IIS)管理器
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Internet 信息服务
D-OD5188A2AE144(本地计
应用程序池
网站
Web
描述
标识符
状态
主机头值
11
1735
正在运行
新建(N)
所有任务(K)
查看(V)
从这里创建窗口(W)
刷新(F)
导出列表(L)...
属性(R)
帮助(H)
网站(W)...
网站(来自文件)(S)...

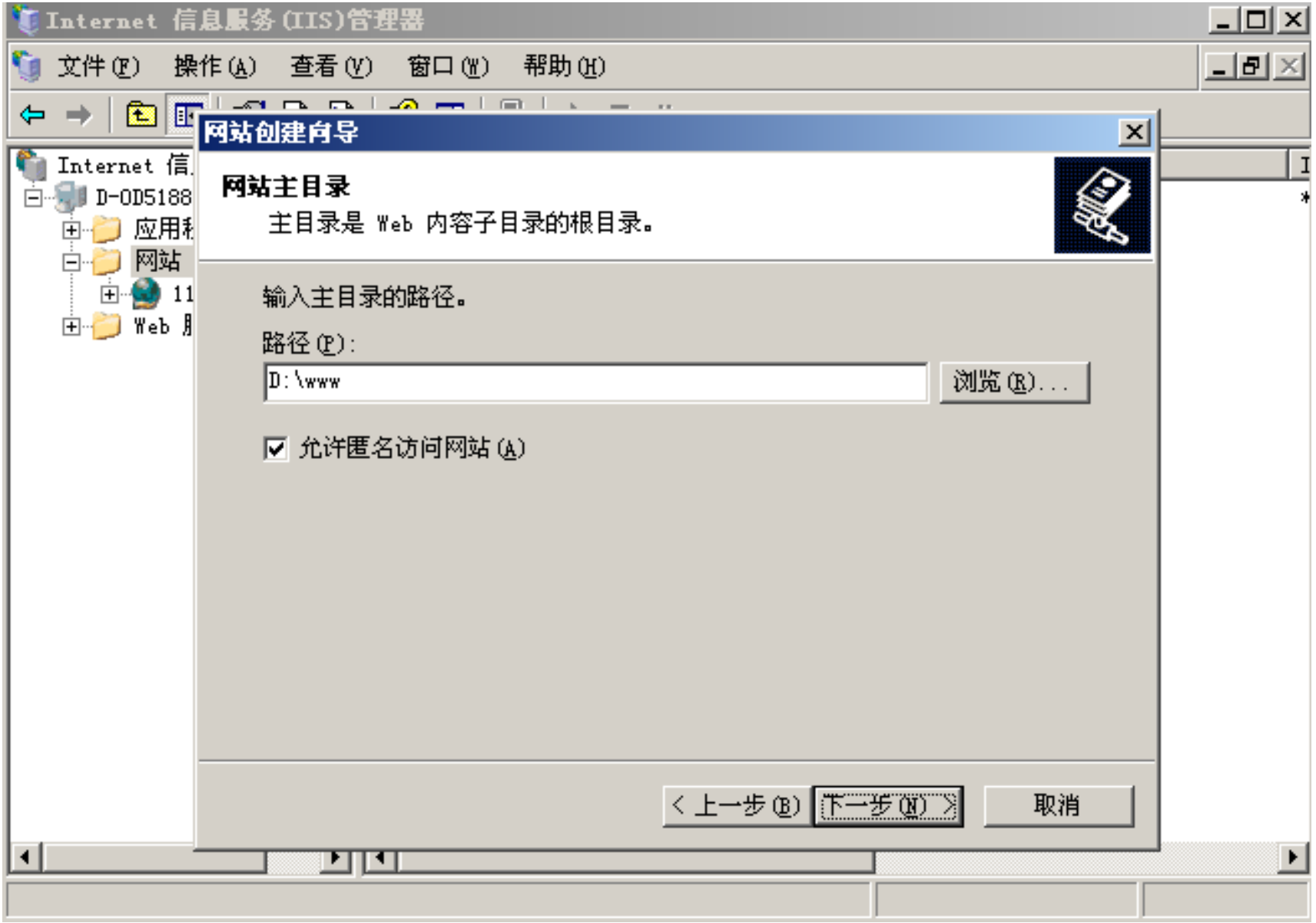
网站描述


Internet 信息服务(IIS)管理器
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Internet 信
D-OD5188
应用程
网站
11
Web 服
网站创建向导
网站描述
网站描述用于帮助管理员识别站点。
输入网站描述。
描述(D):
web
< 上一步(B)
下一步(N) >
取消

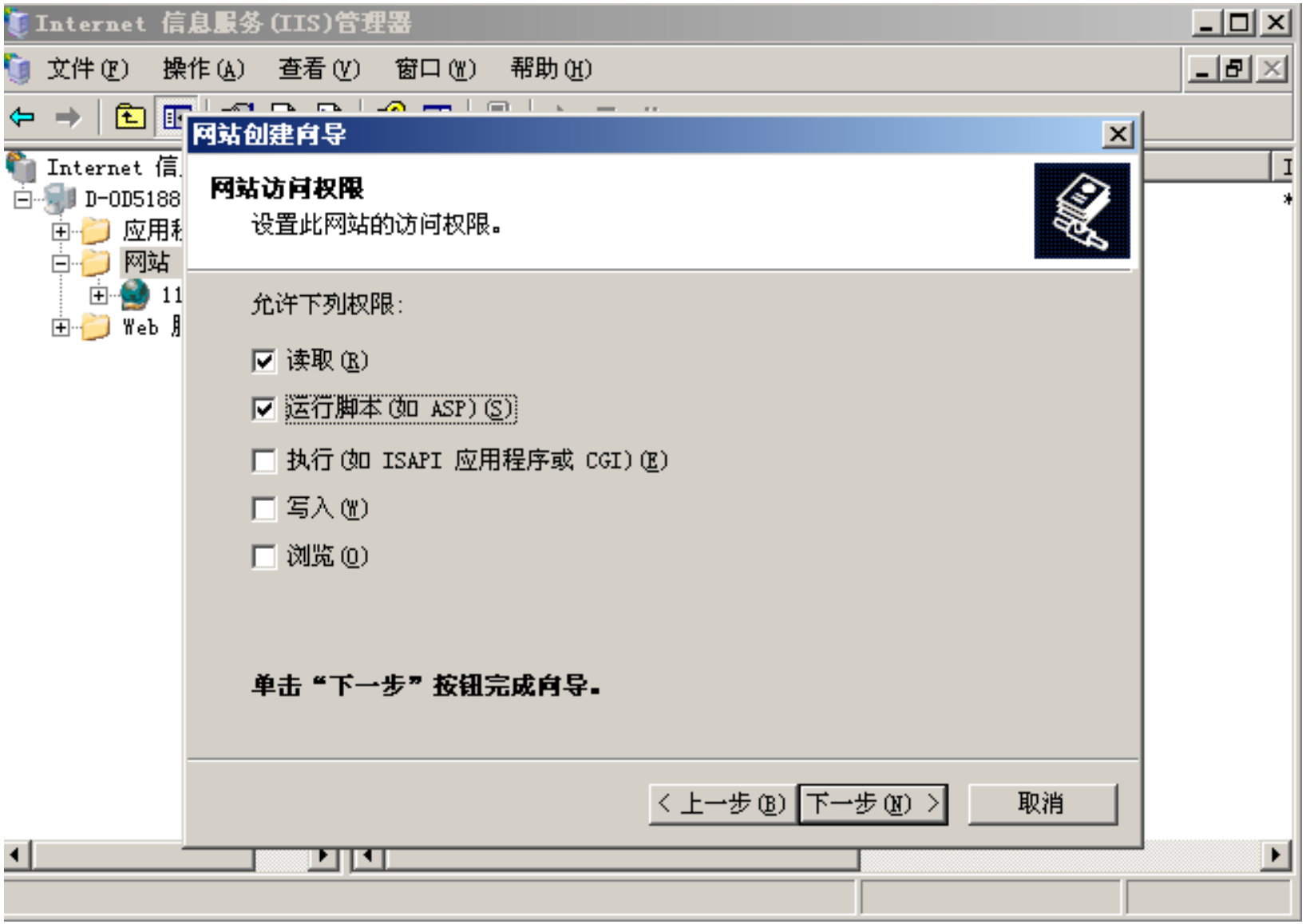
设置IP地址和端口


Internet 信息服务(IIS)管理器
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
网站创建向导
IP 地址和端口设置
指定新网站的 IP 地址，端口设置和主机头。
网站 IP 地址(I):
(全部未分配)
网站 TCP 端口(默认值: 80)(T):
80
此网站的主机头(默认: 无)(H):
有关更多信息，请参阅 IIS 产品文档。
< 上一步(B)
下一步(N) >
取消

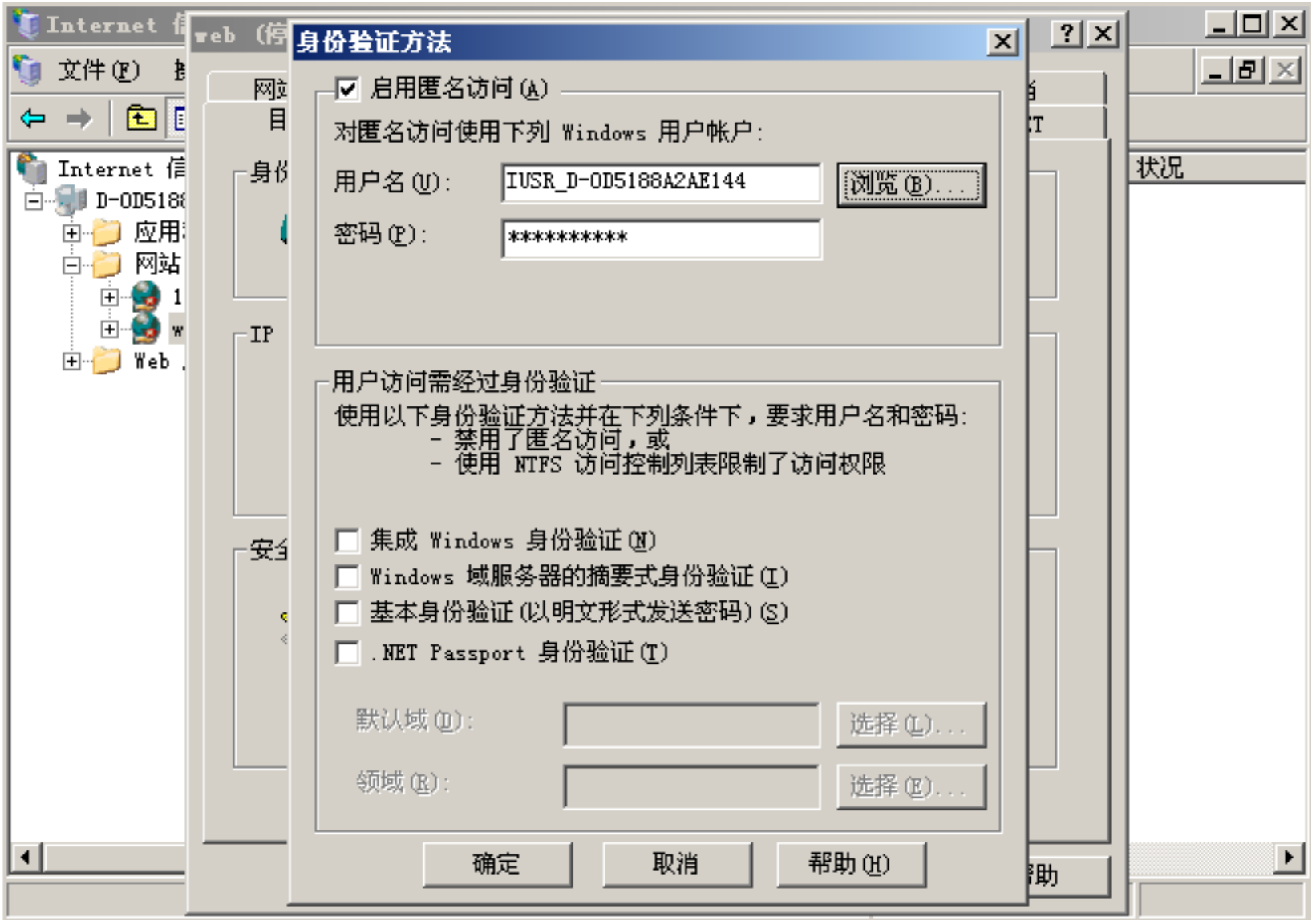
设置主目录路径


Internet 信息服务(IIS)管理器
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Internet 信
D-OD5188
应用程
网站
11
Web 服
网站创建向导
网站主目录
主目录是 Web 内容子目录的根目录。
输入主目录的路径。
路径(P):
D:\www
浏览(R)...
允许匿名访问网站(A)
< 上一步(B)
下一步(N) >
取消

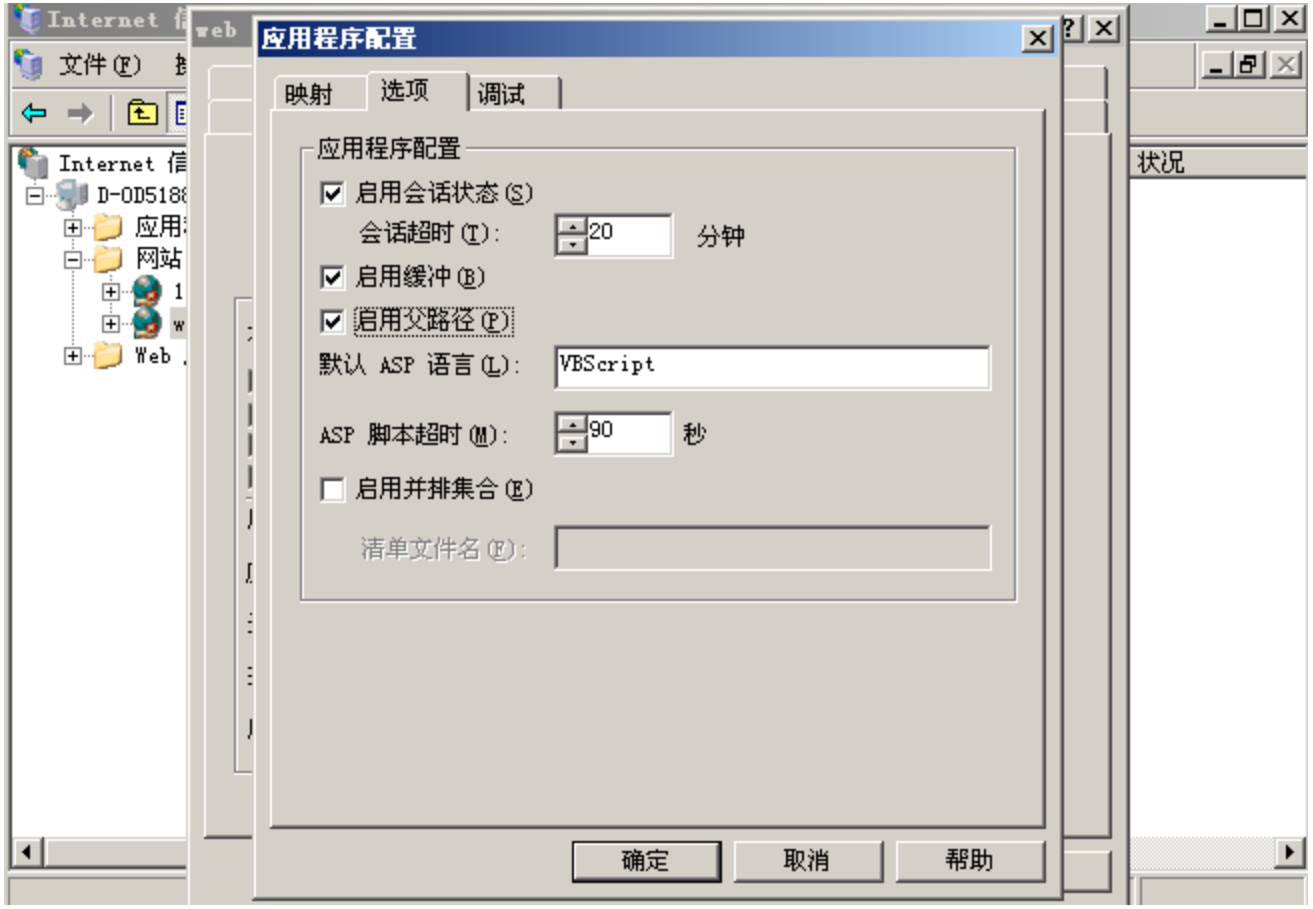
设置网站访问权限


Internet 信息服务(IIS)管理器
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Internet 信
D-OD5188
应用
网站
11
Web
网站创建向导
网站访问权限
设置此网站的访问权限。
允许下列权限:
读取(R)
运行脚本(如 ASP)(S)
执行(如 ISAPI 应用程序或 CGI)(E)
写入(W)
浏览(O)
单击“下一步”按钮完成向导。
< 上一步(B)
下一步(N) >
取消

启用匿名访问


身份验证方法
启用匿名访问(A)
对匿名访问使用下列 Windows 用户帐户:
用户名(U):
IUSR_D-OD5188A2AE144
浏览(B)...
密码(P):
****
用户访问需经过身份验证
使用以下身份验证方法并在下列条件下，要求用户名和密码:
- 禁用了匿名访问，或
- 使用 NTFS 访问控制列表限制了访问权限
集成 Windows 身份验证(N)
Windows 域服务器的摘要式身份验证(I)
基本身份验证(以明文形式发送密码)(S)
.NET Passport 身份验证(T)
默认域(D):
选择(L)...
领域(R):
选择(E)...
确定
取消
帮助(H)
状况

启用父路径


Internet
文件(F)
Internet 信
D-OD5188
应用
网站
1
w
Web
web
应用程序配置
映射
选项
调试
应用程序配置
启用会话状态(S)
会话超时(T):
20
分钟
启用缓冲(B)
启用父路径(P)
默认 ASP 语言(L):
VBScript
ASP 脚本超时(M):
90
秒
启用并排集合(E)
清单文件名(F):
确定
取消
帮助
状况

添加默认内容页


Internet
文件(F)
Internet 信
D-OD5188
应用
网站
1
w
Web
web (停止) 属性
目录安全性
HTTP 头
自定义错误
ASP.NET
网站
性能
ISAPI 筛选器
主目录
文档
添加内容页
默认内容页(D):
index.asp
确定
取消
除(R)
启用文档页脚(O)
附加一个 HTML 格式的页脚到您的 Web 服务器返回的每一个文档。
浏览(B)...
确定
取消
应用(A)
帮助
状况

IIS 安全加固

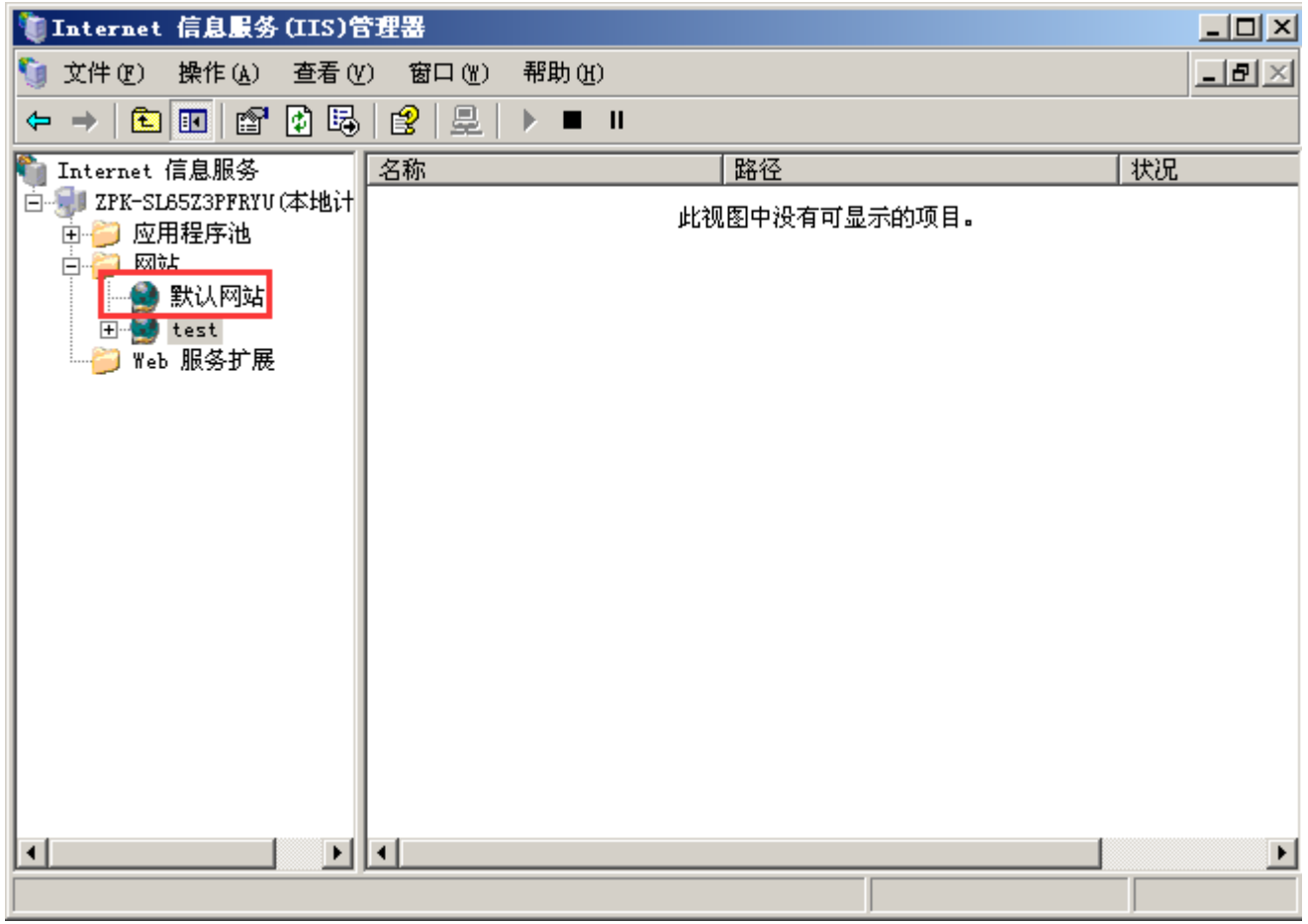
IIS安装及版本的选择

在IIS安装过程中，根据具体的业务需求，只安装必要的组件，以避免安装其他一切不必要的组件带来的安全风险。如网站正常运行只需要ASP环境，那我们就没必要安装.net组件。

对于IIS版本，至少要在6.0以上，IIS5.0存在严重的安全漏洞，不过现在运行IIS5.0的服务器已经非常少了，对于这一点不用太过担心。

删除默认网站

把IIS默认安装的站点删除或禁用掉

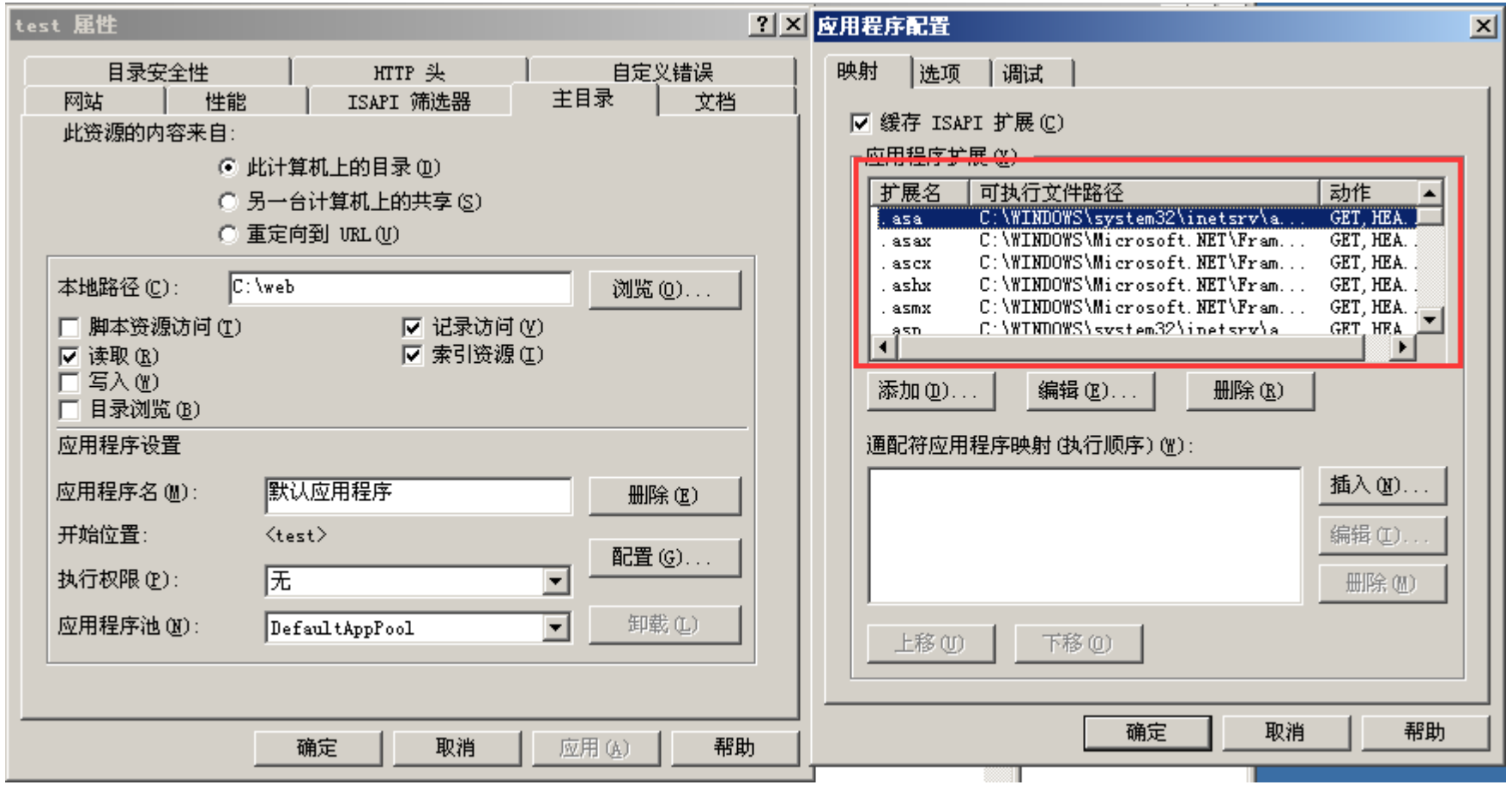


禁用不必要的Web服务扩展

打开IIS 管理器，检查是否有不必要的“Web服务扩展”，如果有则禁用掉。

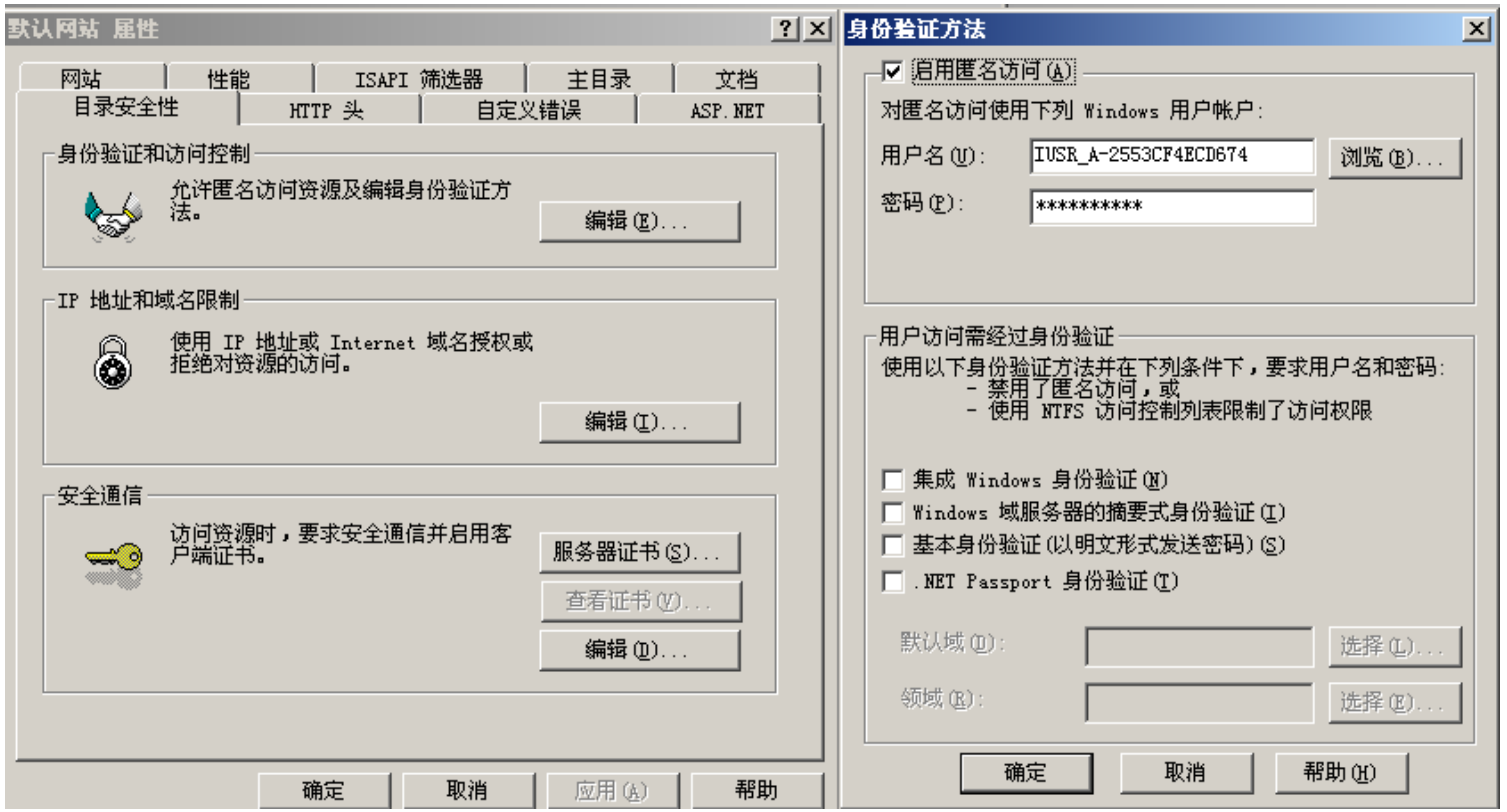
删除不使用的应用程序扩展

在IIS管理器中，右击网站“属性”，点击主目录选项卡，点击“应用程序设置”的配置按钮
根据网站的实际情况，只保留必要的应用程序扩展，其他的一律删除，尤其是像cer、asa这样极其危险的扩展，而且一般网站也不需要它



IIS访问权限配置

如果IIS中有多个网站，建议为每个网站配置不同的匿名访问账户。
方法：
a. 新建一个账号，加入Guests组
b. “网站属性”—>“目录安全性”—>“身份验证和访问控制”，把“启用匿名访问”处，用刚新建的账户代替默认账户



正确设置网站目录的权限和IIS权限

网站分区为NTFS分区。网站目录出system和administrator组有完全控制权限外，其他用户只需要有读取权限。
IIS6管理器中设置：
只选择“读取、记录访问、索引资源”
禁止“写入”和“脚本资源访问”，避免IIS Put上传攻击
禁止“目录浏览”，避免目录遍历攻击

正确设置网站目录的权限和IIS权限

应用程序设置中的执行权限设置为“纯脚本”

原则：

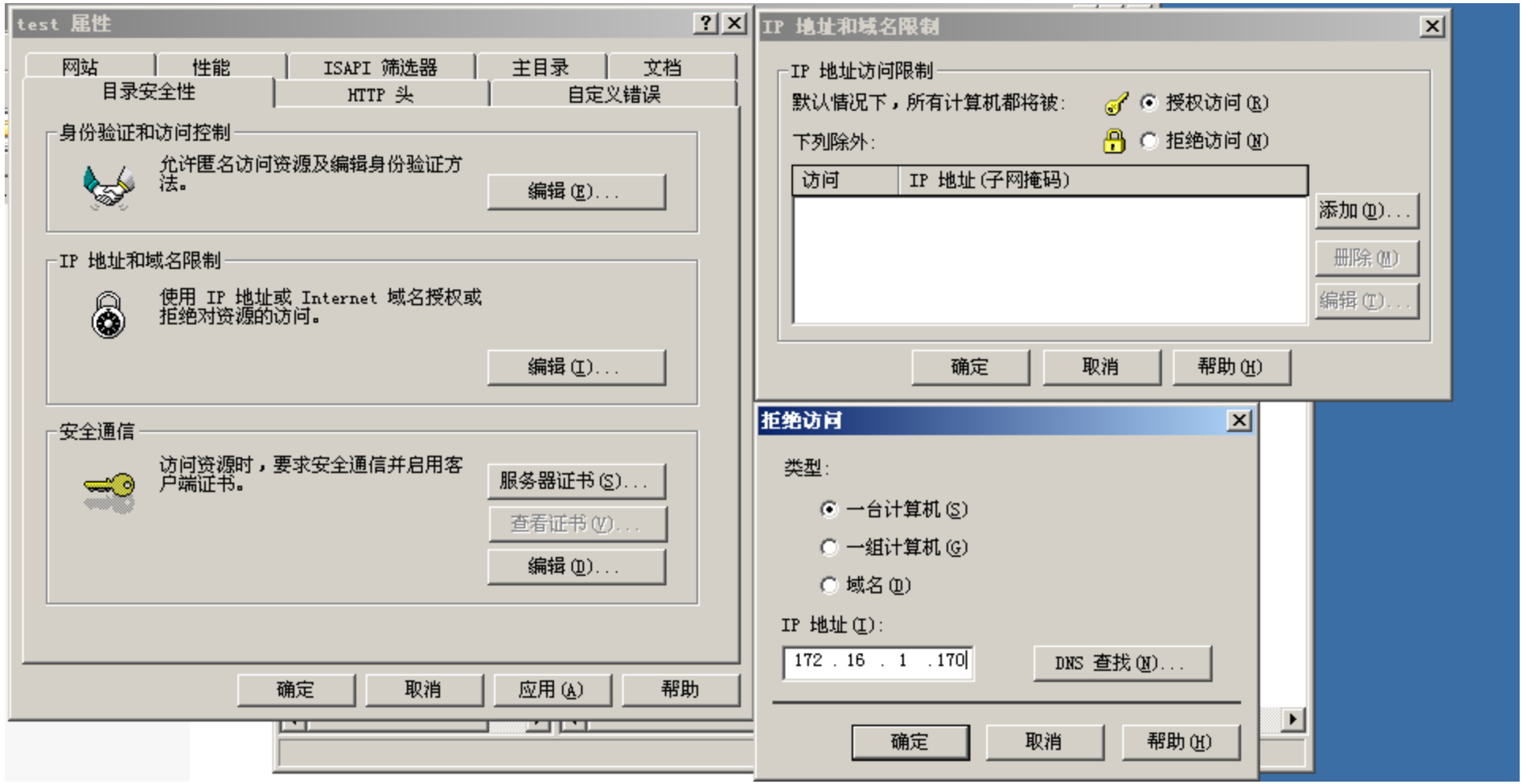
目录有写入权限，一定不要分配执行权限

目录有执行权限，一定不要分配写入权限

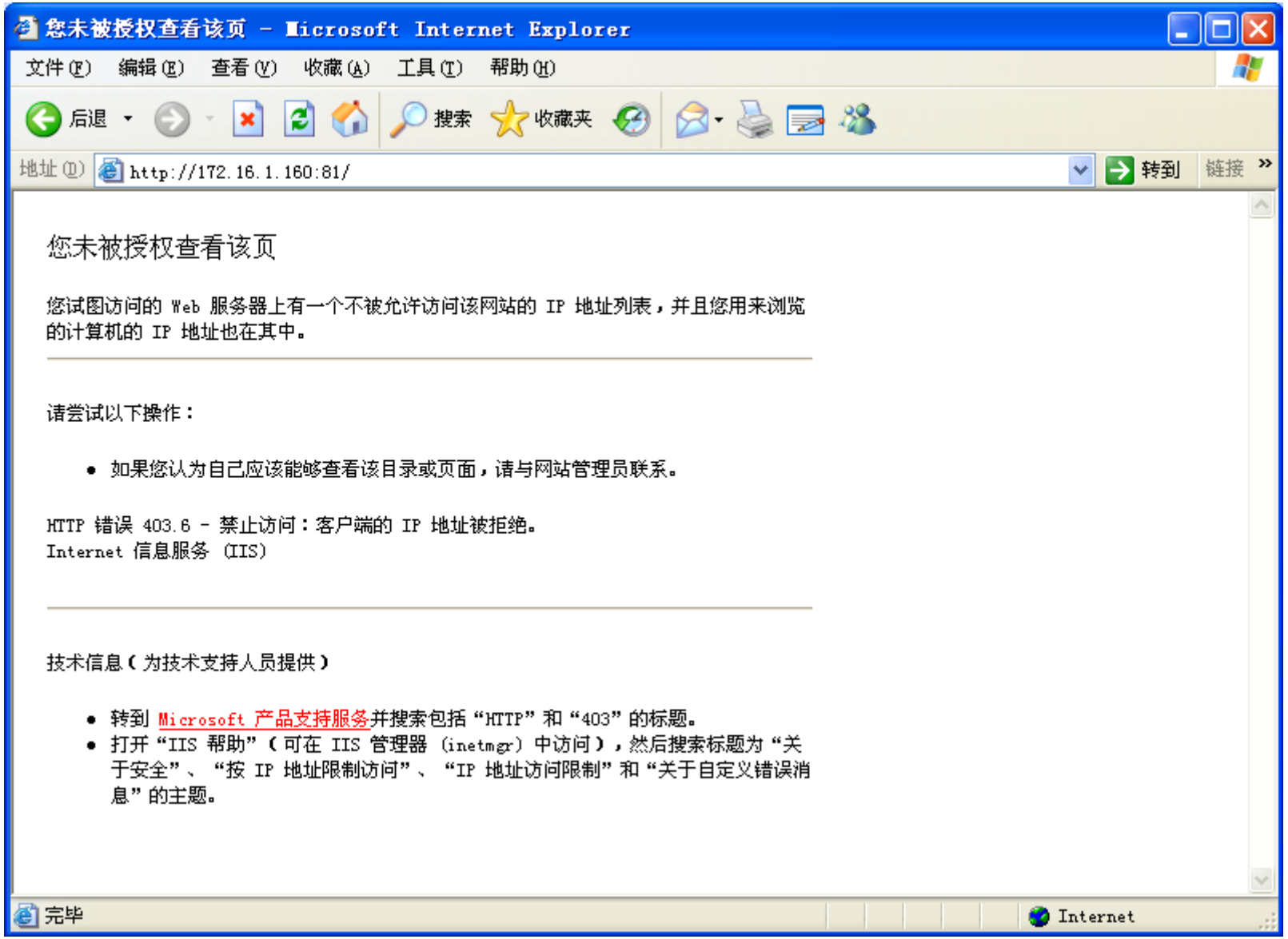
网站上传目录和数据库目录一般需要分配“写入”权限，但一定不要分配执行权限

其他目录一般只分配“读取”和“记录访问”权限即可

设置IP访问限制


test 属性
网站
性能
ISAPI 筛选器
主目录
文档
目录安全性
HTTP 头
自定义错误
身份验证和访问控制
允许匿名访问资源及编辑身份验证方法。
编辑(E)...
IP 地址和域名限制
使用 IP 地址或 Internet 域名授权或拒绝对资源的访问。
编辑(I)...
安全通信
访问资源时，要求安全通信并启用客户端证书。
服务器证书(S)...
查看证书(V)...
编辑(D)...
确定
取消
应用(A)
帮助
IP 地址和域名限制
IP 地址访问限制
默认情况下，所有计算机都将被:
授权访问(R)
下列除外:
拒绝访问(N)
访问
IP 地址(子网掩码)
添加(D)...
删除(M)
编辑(T)...
确定
取消
帮助(H)
拒绝访问
类型:
一台计算机(S)
一组计算机(G)
域名(D)
IP 地址(I):
172 . 16 . 1 . 170
DNS 查找(N)...
确定
取消
帮助(H)

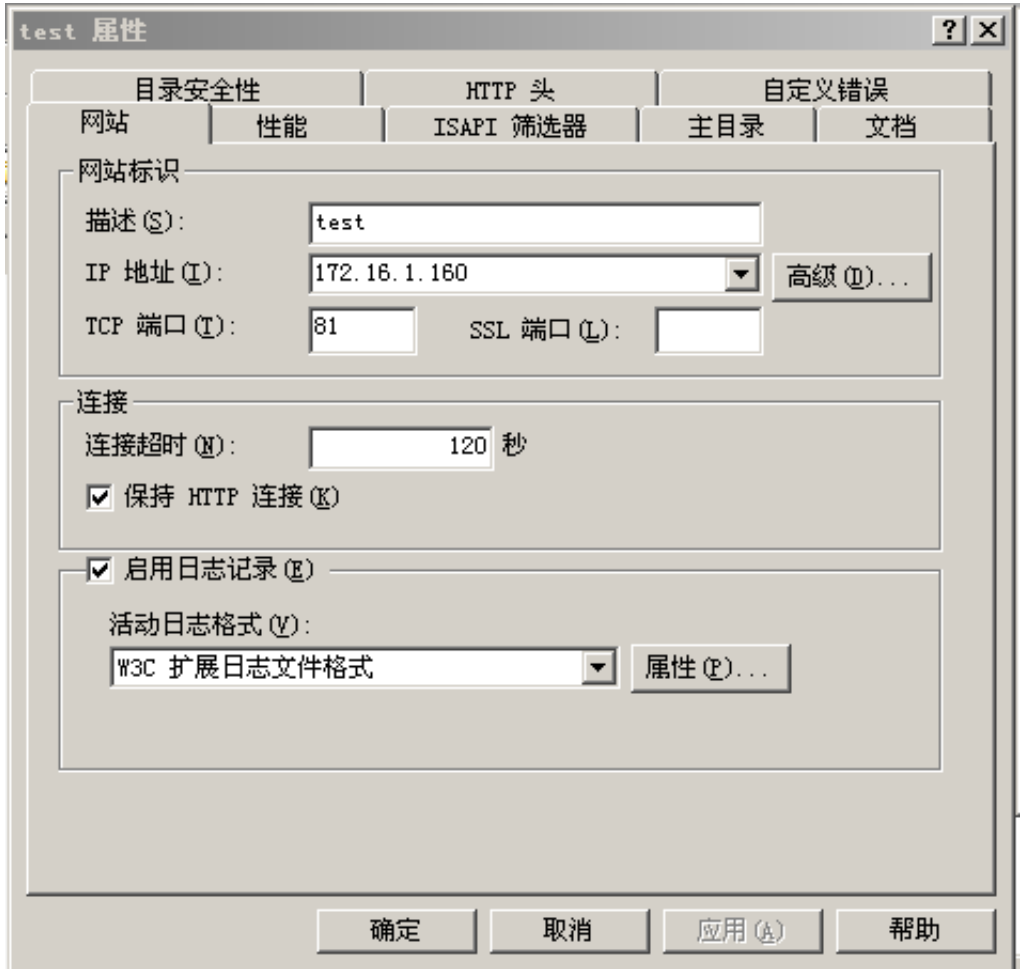
访问测试


您未被授权查看该页 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://172.16.1.160:81/
转到 链接
您未被授权查看该页
您试图访问的 Web 服务器上有一个不被允许访问该网站的 IP 地址列表，并且您用来浏览的计算机的 IP 地址也在其中。
请尝试以下操作：
如果您认为自己应该能够查看该目录或页面，请与网站管理员联系。
HTTP 错误 403.6 - 禁止访问：客户端的 IP 地址被拒绝。
Internet 信息服务 (IIS)
技术信息（为技术支持人员提供）
转到 Microsoft 产品支持服务并搜索包括“HTTP”和“403”的标题。
打开“IIS 帮助”（可在 IIS 管理器 (inetmgr) 中访问），然后搜索标题为“关于安全”、“按 IP 地址限制访问”、“IP 地址访问限制”和“关于自定义错误消息”的主题。
完毕
Internet

正确设置IIS日志

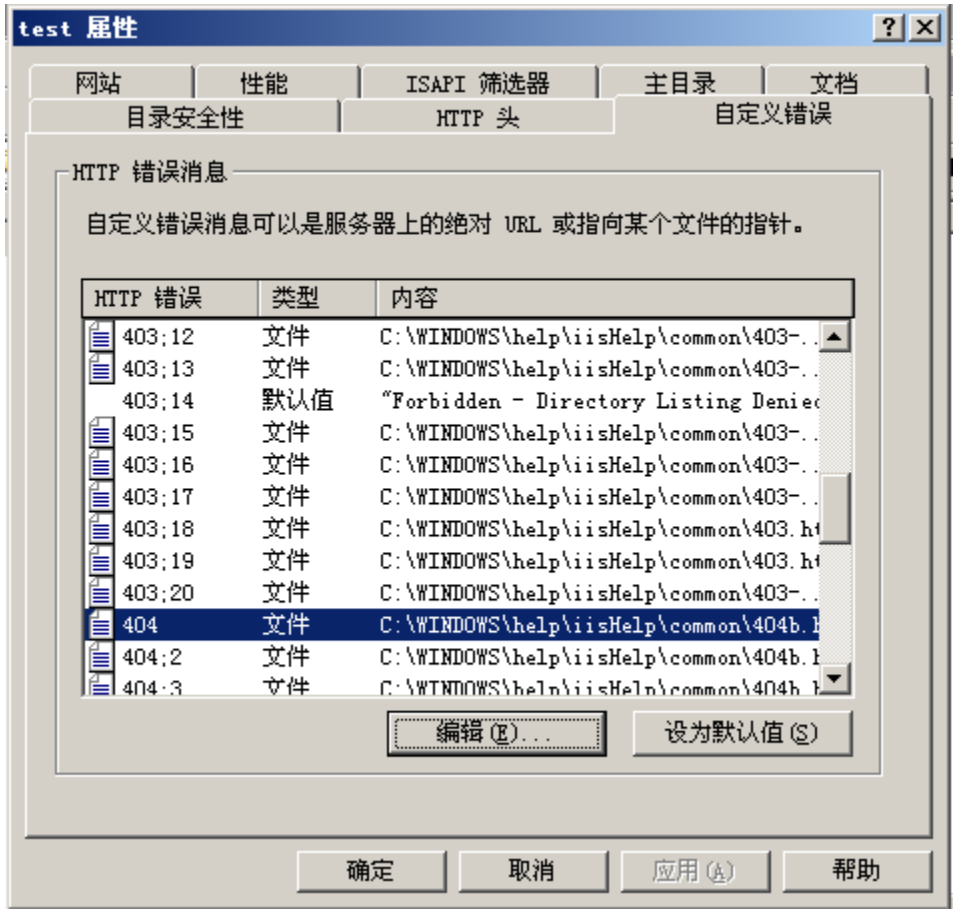
在IIS管理器中，右击网站“属性”，点击网站选项卡，确定已经选择“启用日志记录”，活动日志格式为“W3C扩充日志文件格式”

接着修改IIS日志文件保存路径，默认保存在“C:\WINDOWS\system32\LogFiles”目录下，这里修改为自定义路径。建议保存在非系统盘路径，并且IIS日志文件所在目录只允许Administrators组用户和SYSTEM用户访问

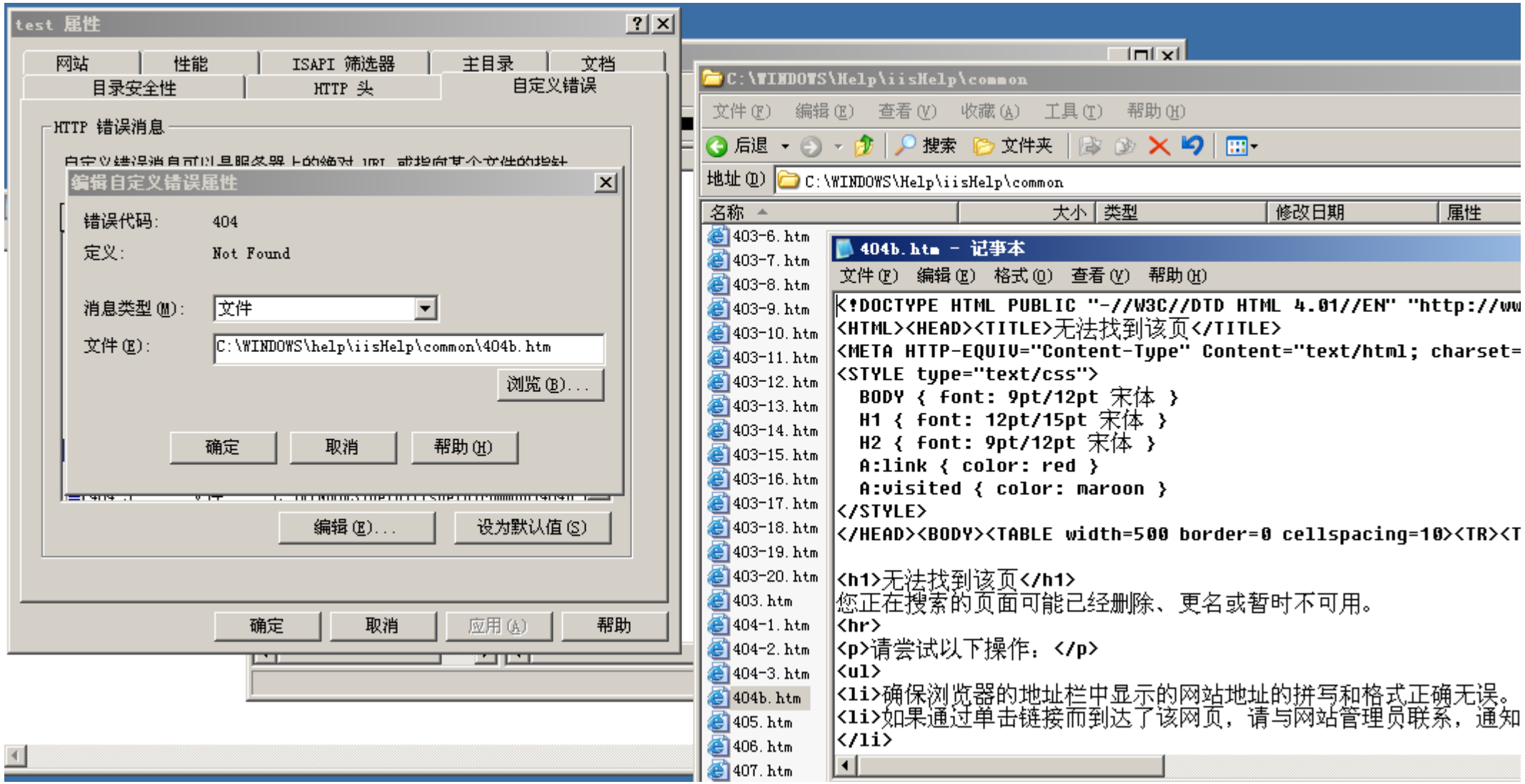


自定义IIS返回的错误信息

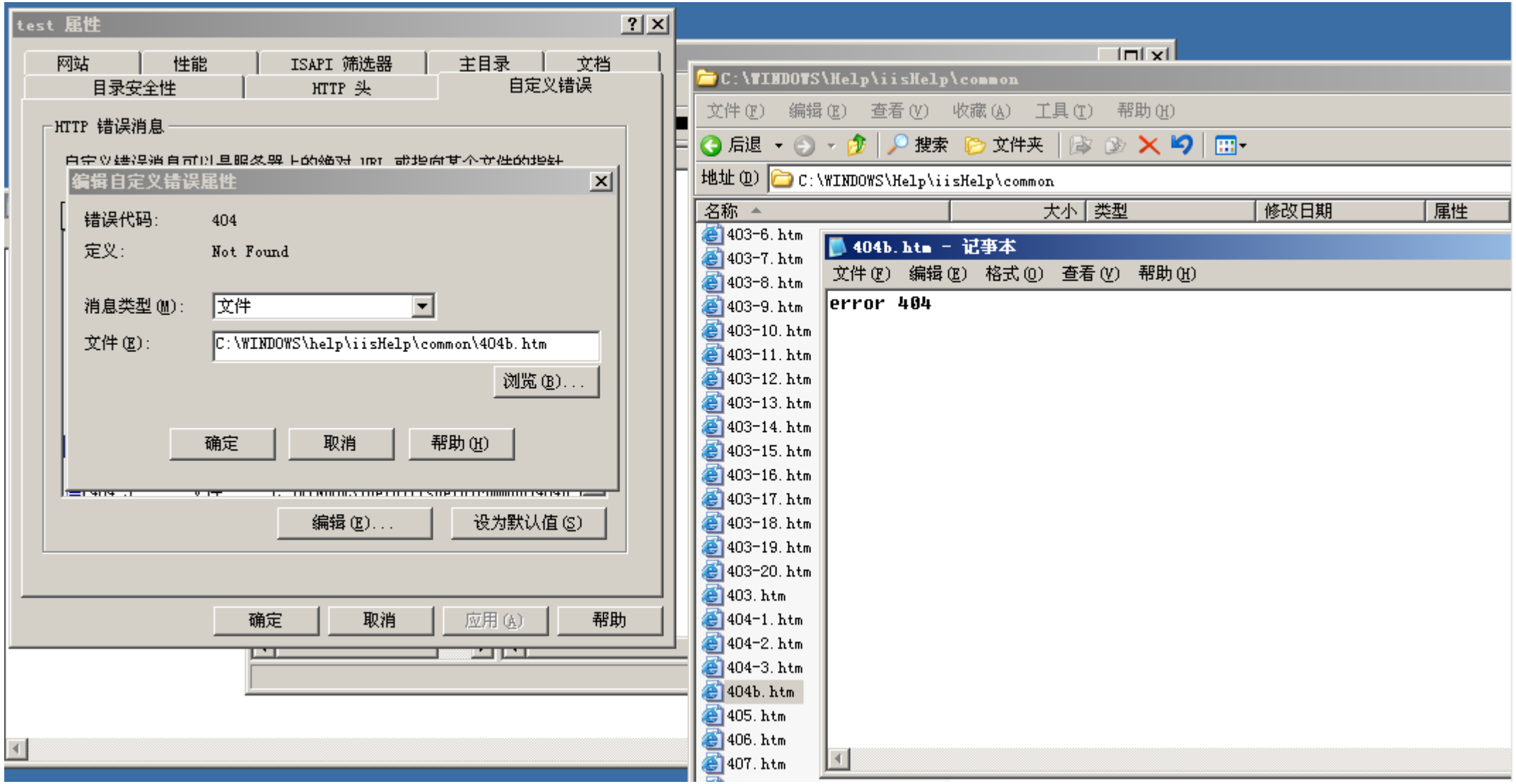
在IIS管理器中，右击网站“属性”，点击自定义错误选项卡，查看HTTP错误信息。双击其中一个HTTP错误，可以设置该HTTP错误发生时，返回自定义错误页面，或者定向到指定地址，常见错误代码：403禁止访问：404找不到页面：500是服务器内部错误



自定义IIS返回的错误信息

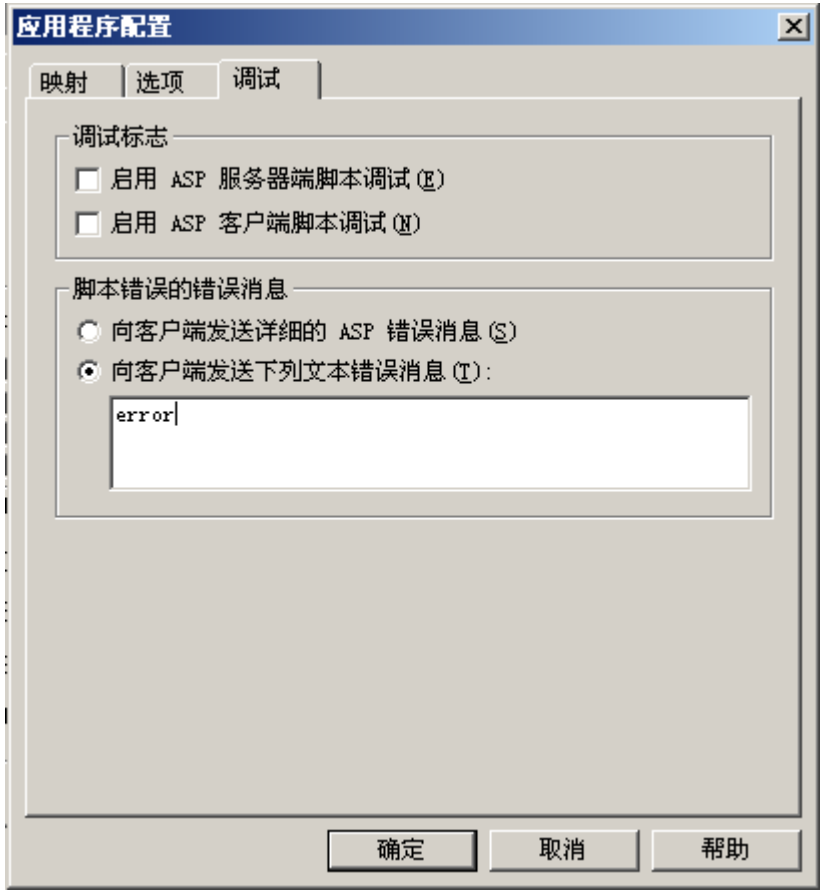


自定义IIS返回的错误信息



禁止向客户端发送详细的ASP错误信息

在IIS管理器中--->“属性”--->“主目录”--->“配置”--->“调试”，选择“向客户端发送下列文本错误消息”项，自定义出错时返回的错误信息



THANK YOU