Internet-Information-Server

Sicherheitstage WS 2007/2008

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

20.11.2007

Einleitung

Firewall

IIS

Securing & Auditing

Einschätzung/Empfehlung

Zusatz: WebDAV

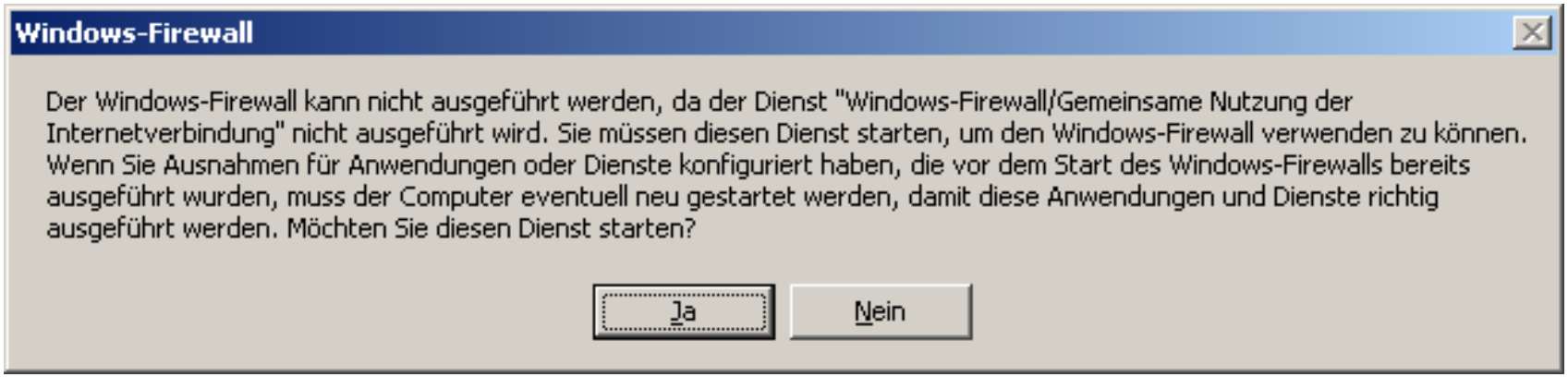
To help protect against malicious users and attackers, the default configuration for members of the Windows Server 2003 family does not install IIS. When it is installed, IIS is configured in a highly secure, “locked” mode. For example, in its default state IIS will only serve static content.
(Windows Server 2003 Security Guide, Chapter 9)

Beachte

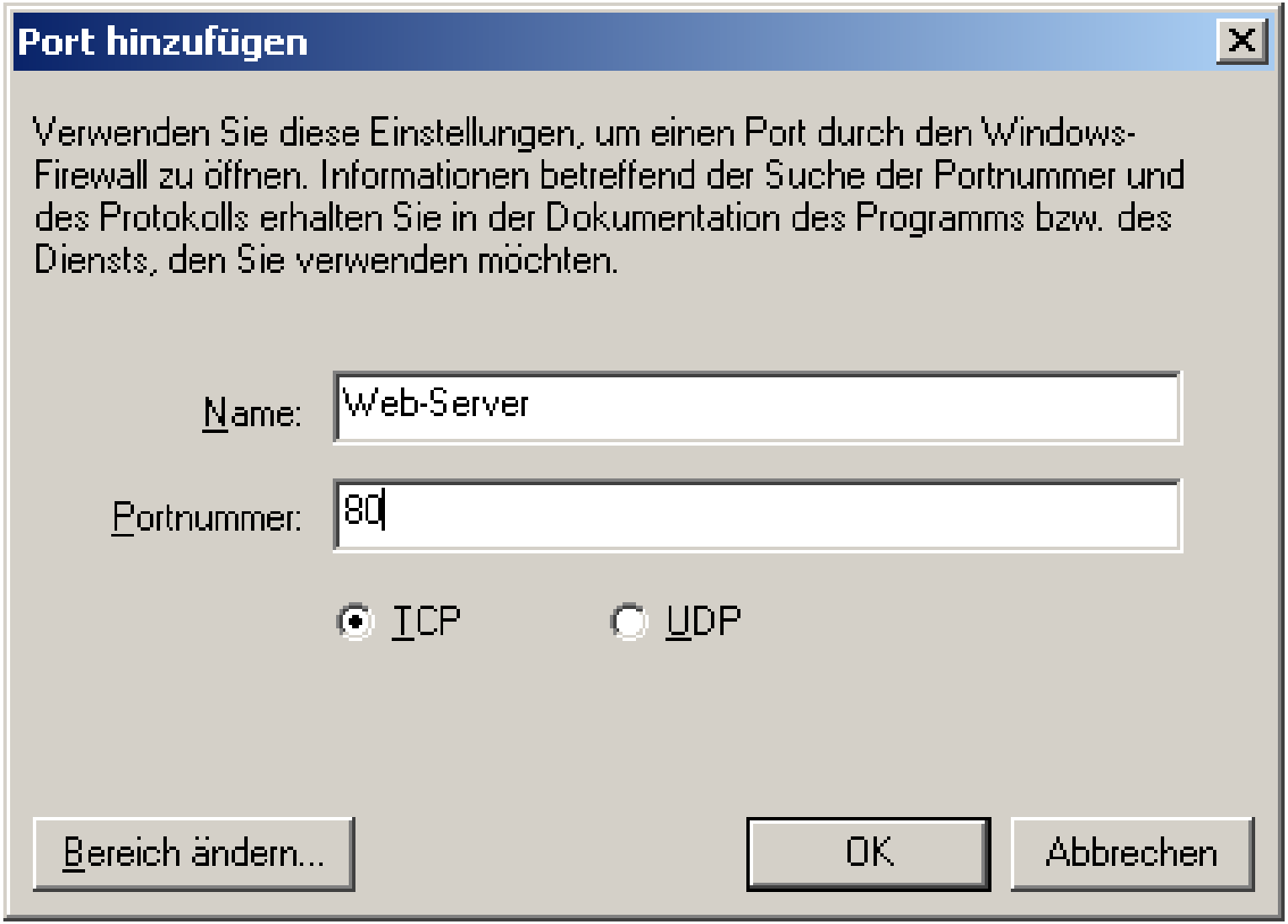
- Obiges gilt (angeblich) für IIS 6.0 auf Windows 2003 SP1/2, IIS 5 oder älter nicht mehr einsetzen!
- Selbst wenn Webserver-Daemon ansich sicher,
  - er muss auch sicher konfiguriert sein
  - Inhalte müssen sicher sein
  - Rechner als ganzes muss sicher sein

- bei Windows 2003 muss die Firewall aktiviert werden
- ICMP echo-request zulassen
- reinkommend Port 80, 443 zulassen,
  ggf. auch in FW IP-Bereich einschränken
  - heute keine Gefahr (ping of death) mehr
  - „guter Ton“ bei Webservern
  - generell Erleichterung bei Problemen

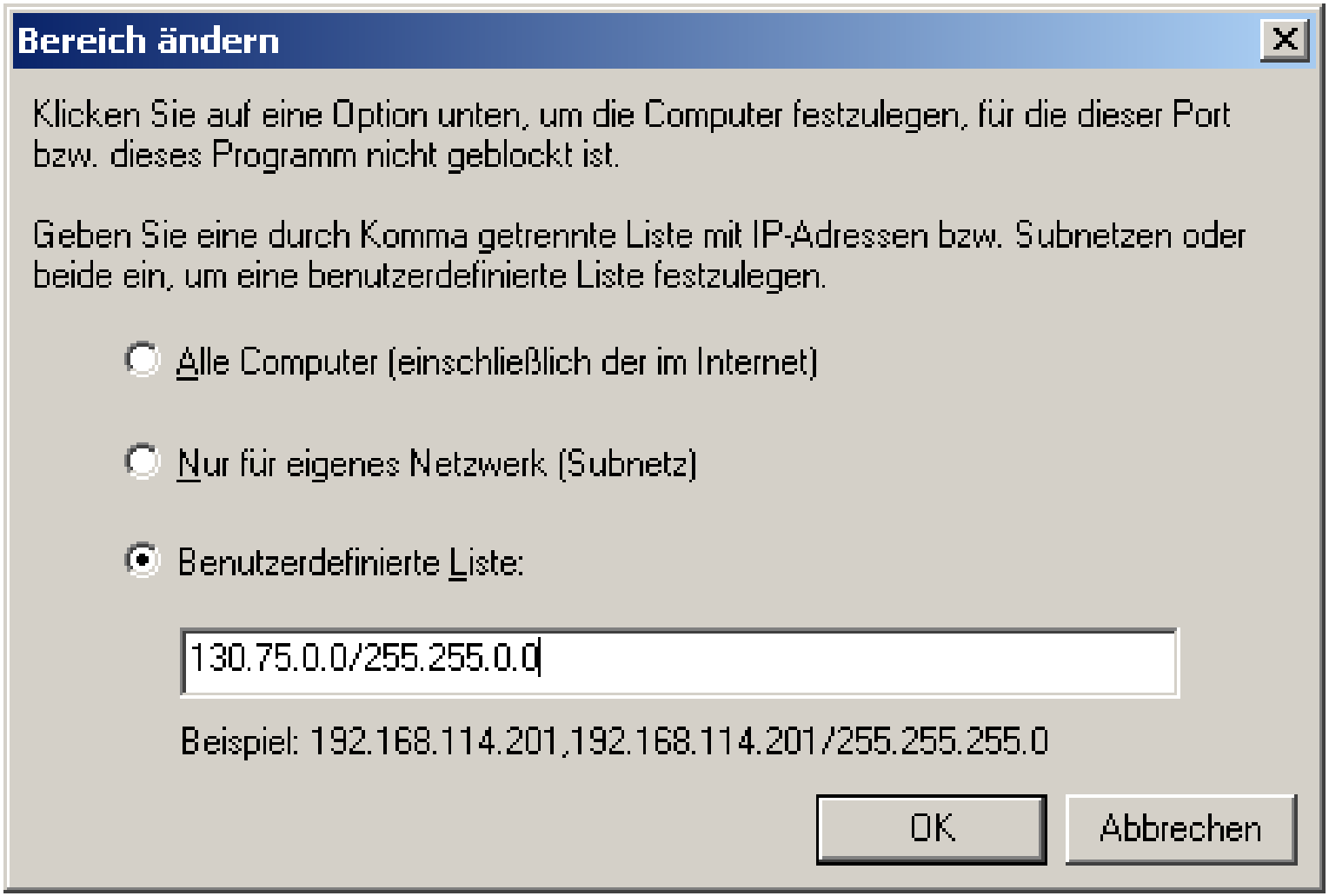
Firewall erst aktivieren



Firewall IIS

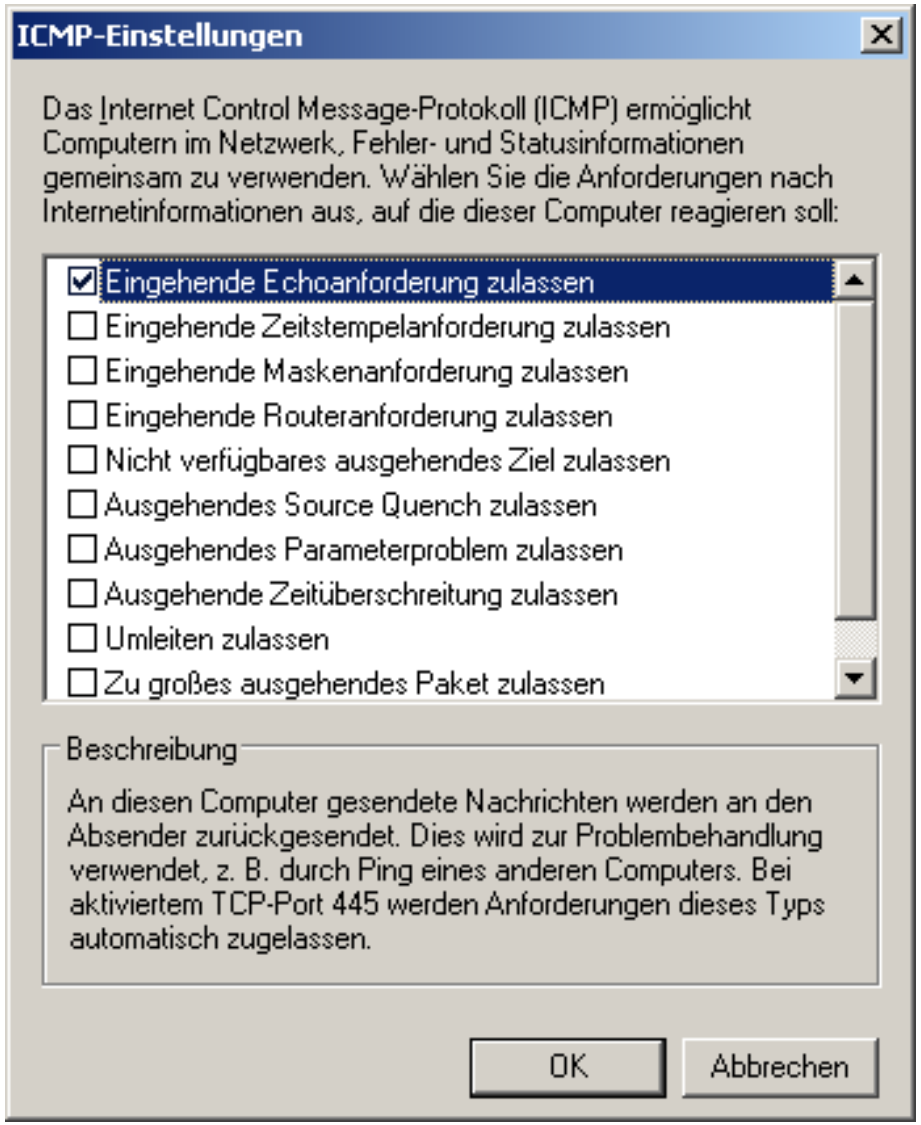


Firewall IP-Bereich



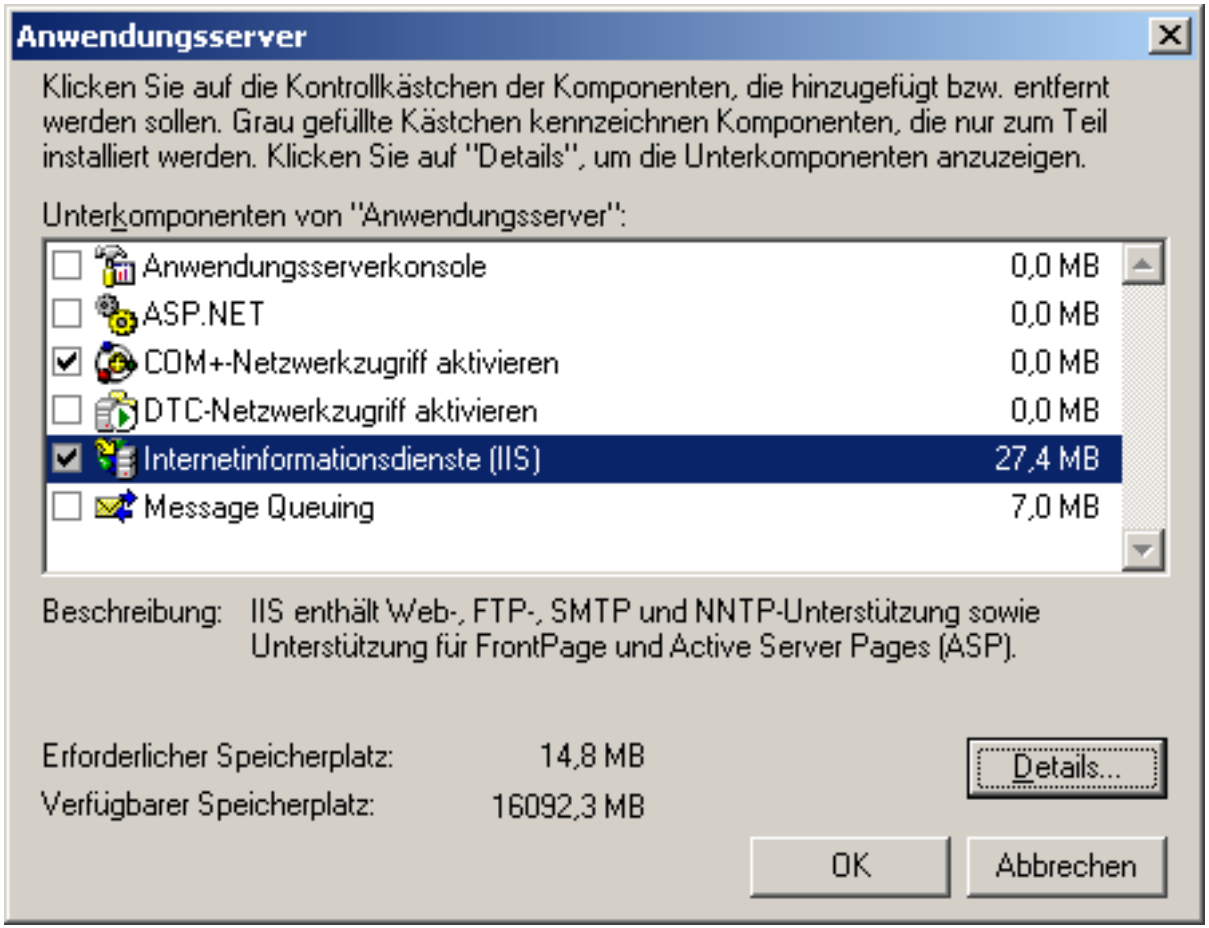
R|R|Z|N

Firewall ping



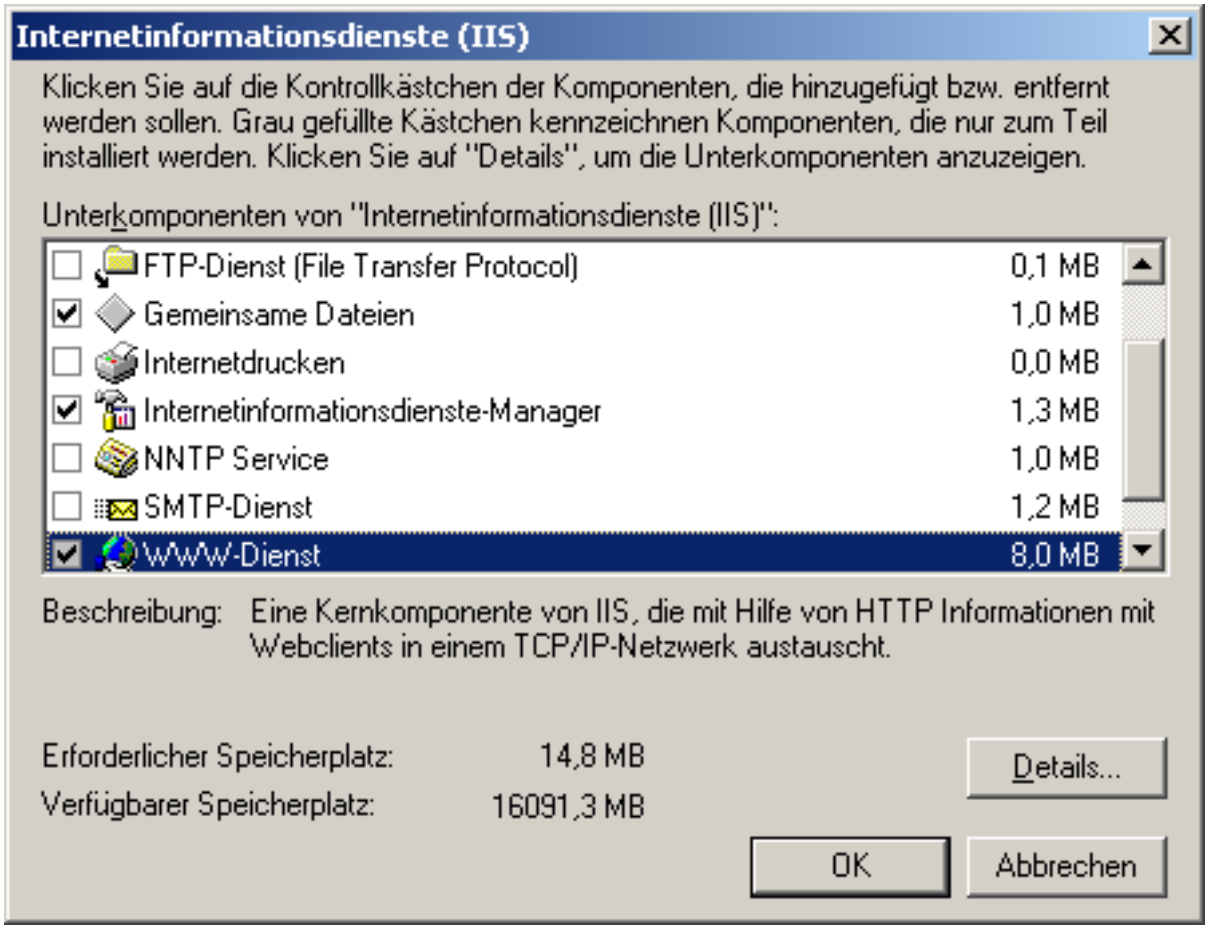
Installation

Über Serverassistenten oder gezielt über Systemsteuerung/Software, Windows-Komponenten



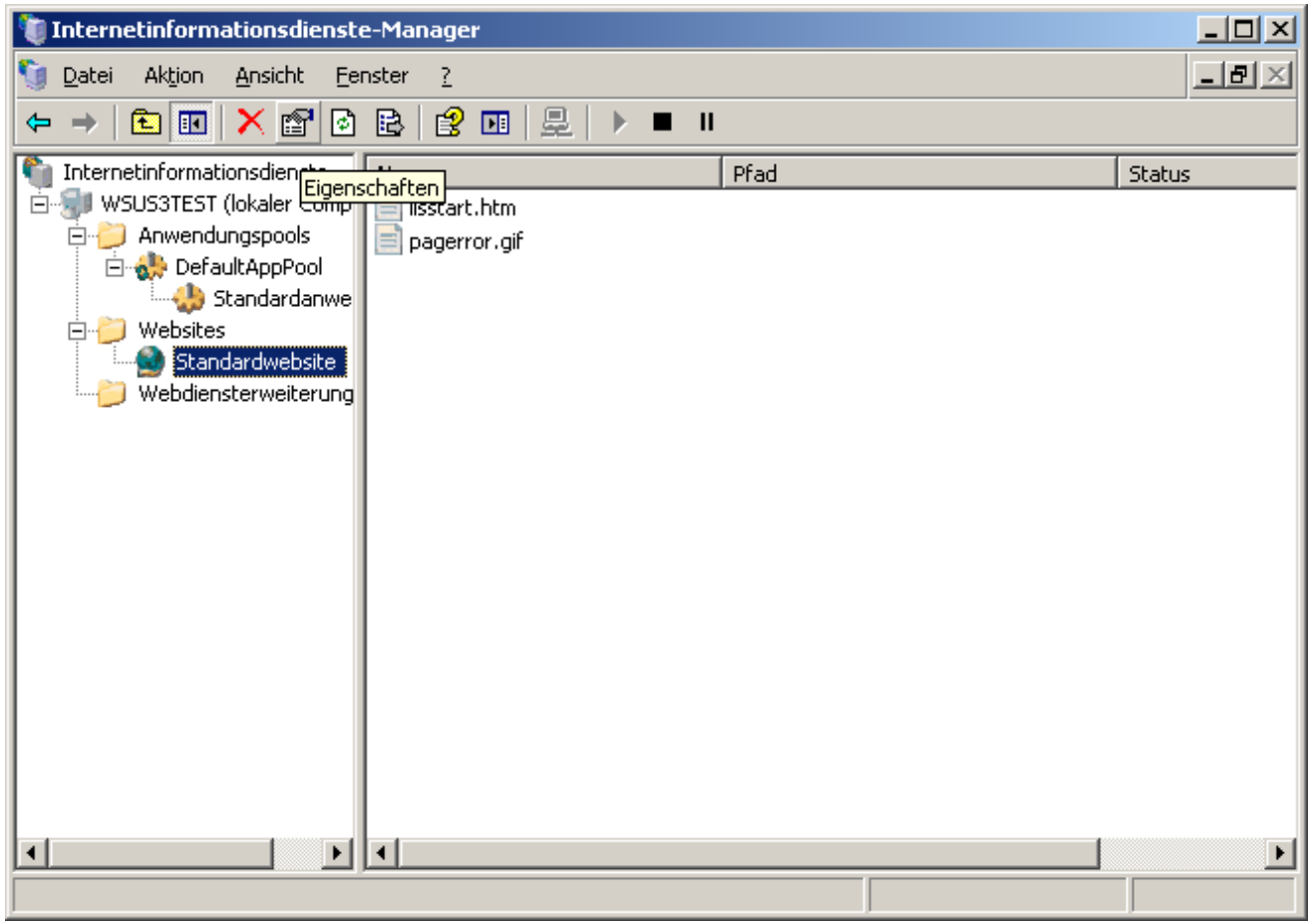
Installation

Über Serverassistenten oder gezielt über Systemsteuerung/Software, Windows-Komponenten

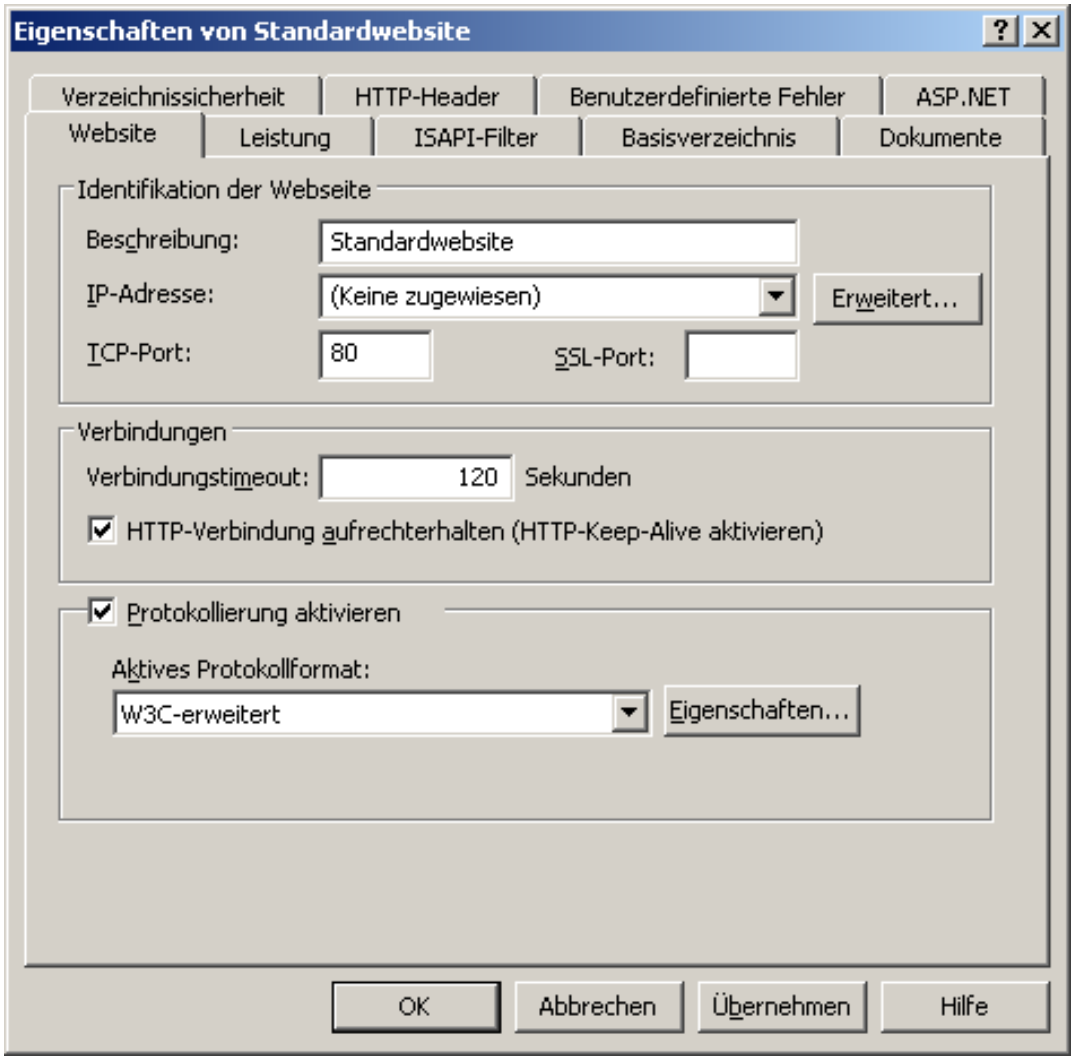


Konfiguration Webseite

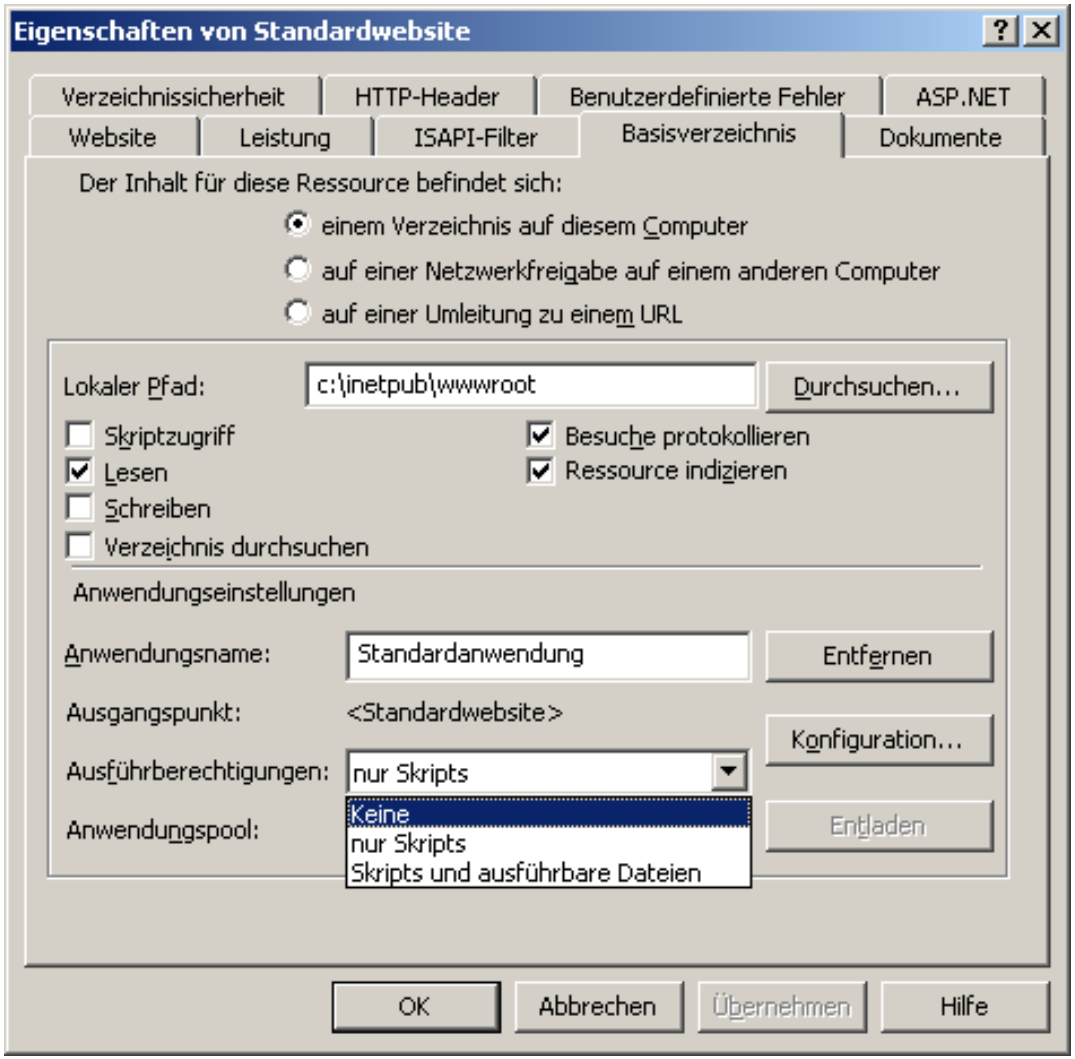
Standardwebseite ist bereits vorbereitet,
ASP.Net, WebDAV etc. nach Installation zunächst aus



Eigenschaften Webseite

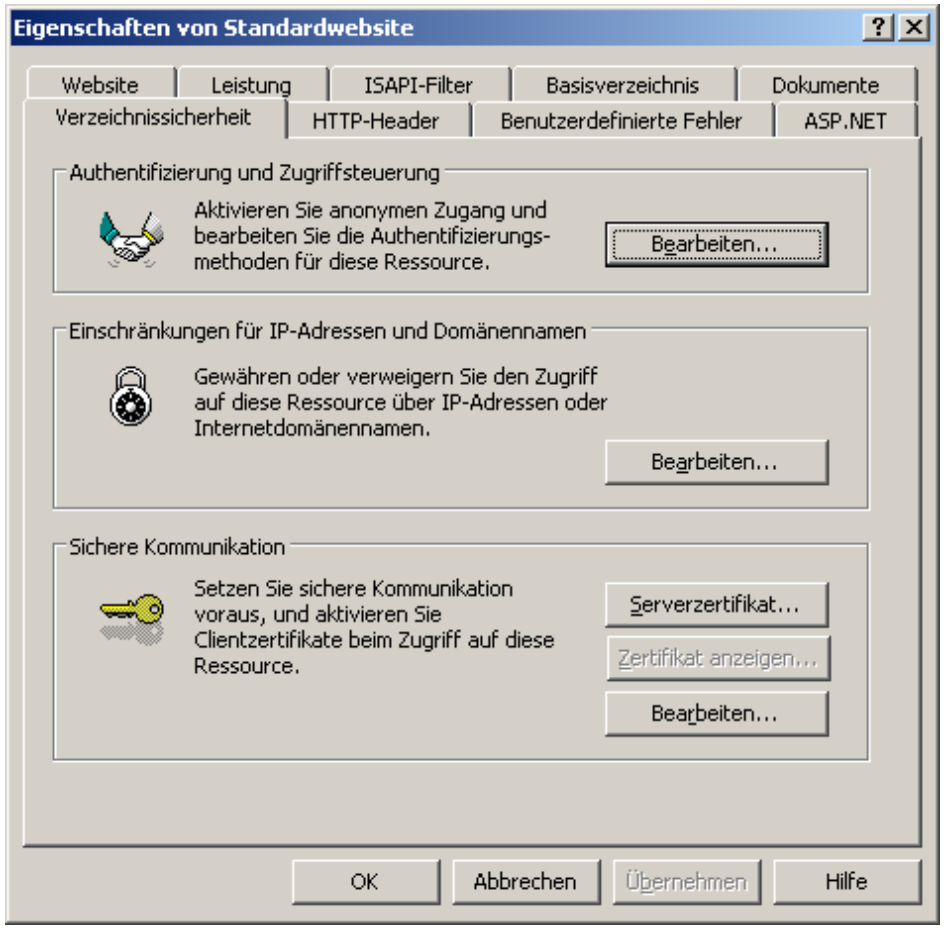


Eigenschaften Webseite



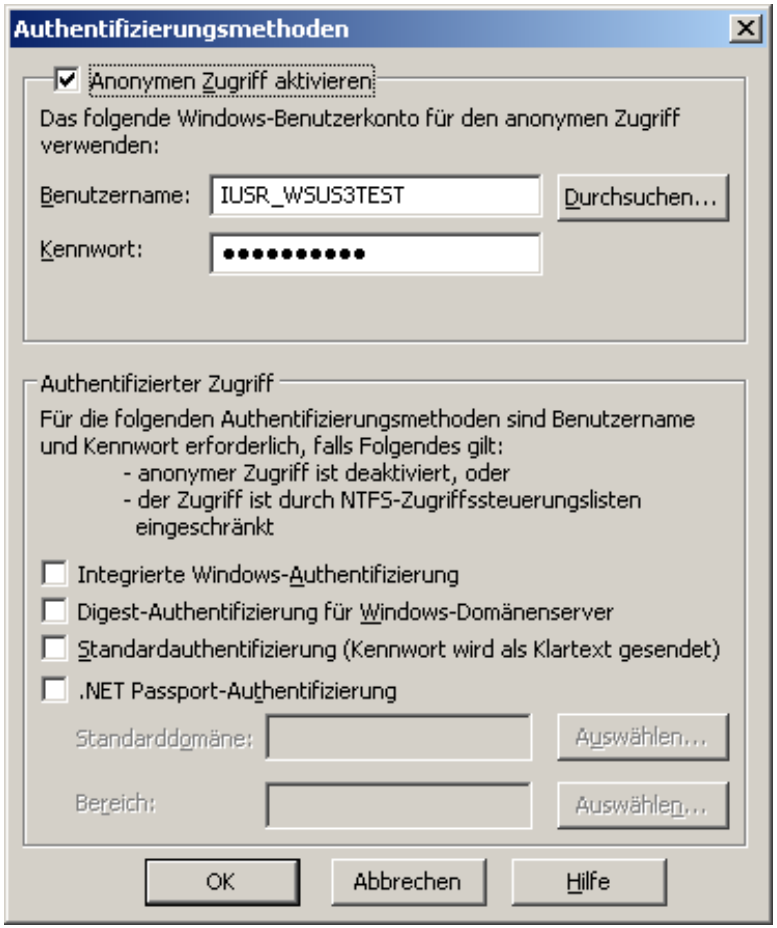
Verzeichnissicherheit

Bündelt http-Authentifizierung/NTFS-Zugriff, IP-Filterung, SSL-Einstellungen



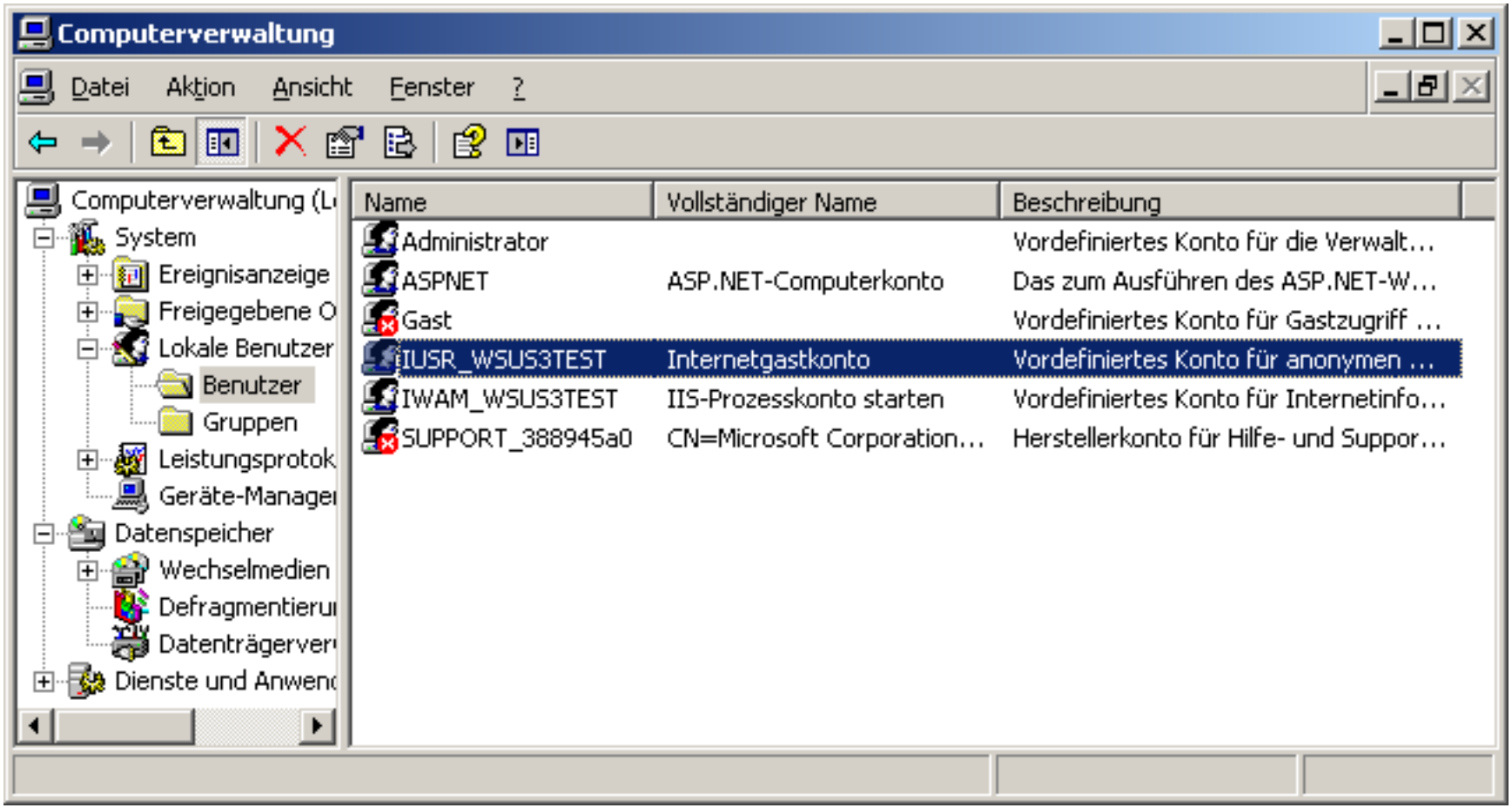
Authentifizierung/NTFS-Zugriff

Anonymen Zugriff wird Windowsnutzer zugeordnet (`IUSR_*`), HTTP-Authentifizierung immer als Windowsnutzer

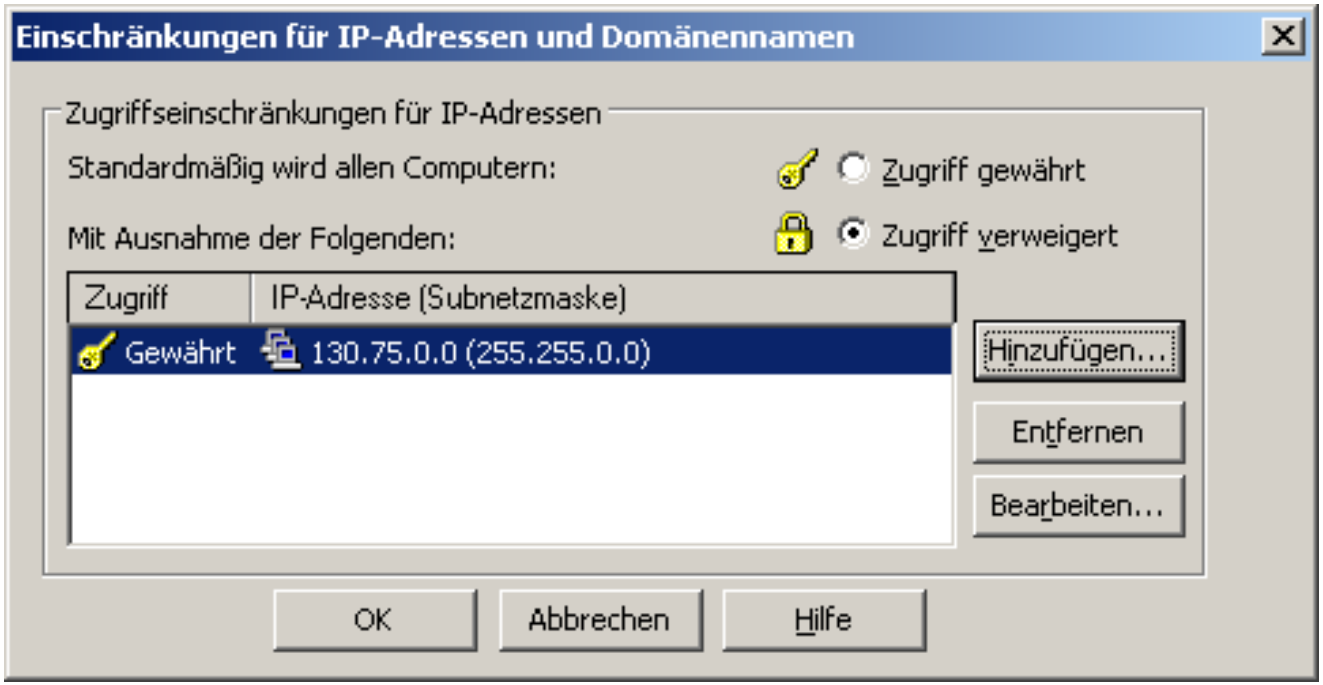


Authentifizierung/NTFS-Zugriff

Anonymen Zugriff wird Windowsnutzer zugeordnet (`IUSR_*`),
HTTP-Authentifizierung immer als Windowsnutzer

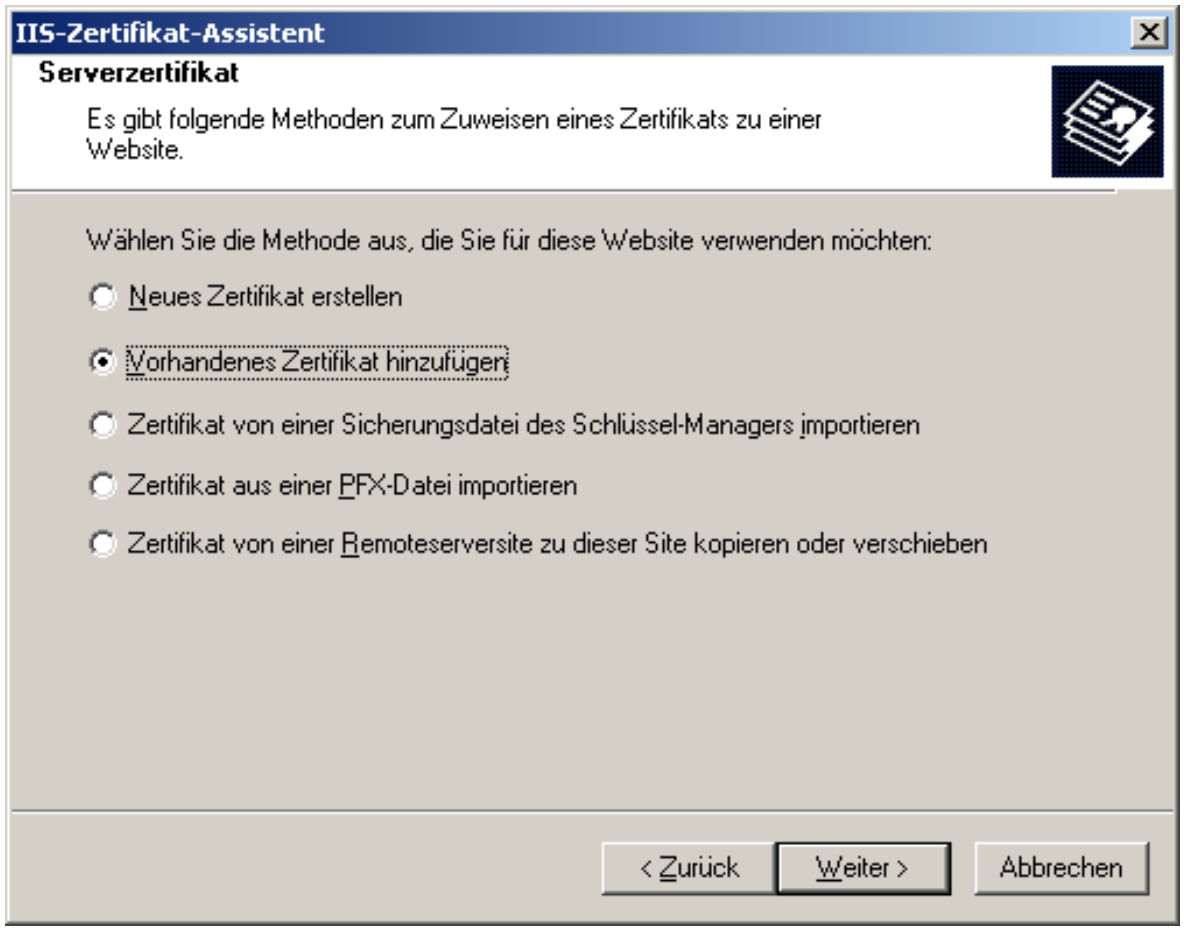


IP-Adressen-Filter



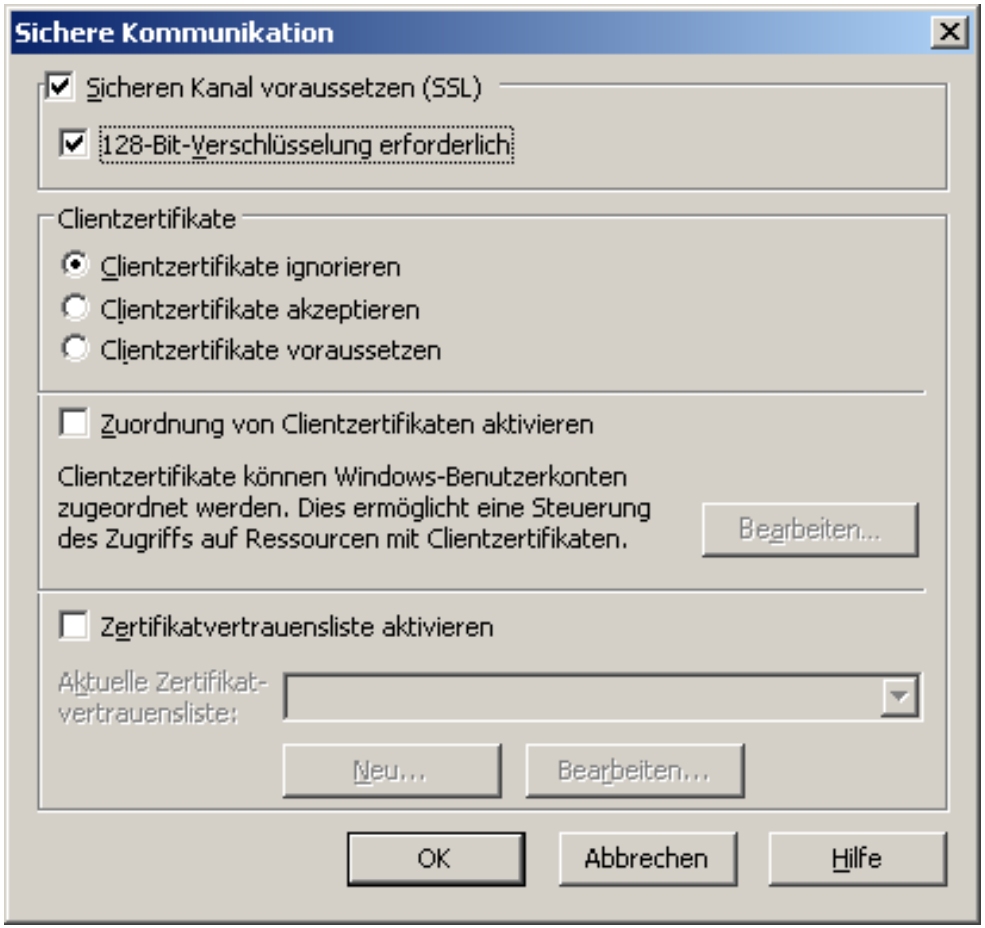
SSL

Server-Zertifikat einbinden

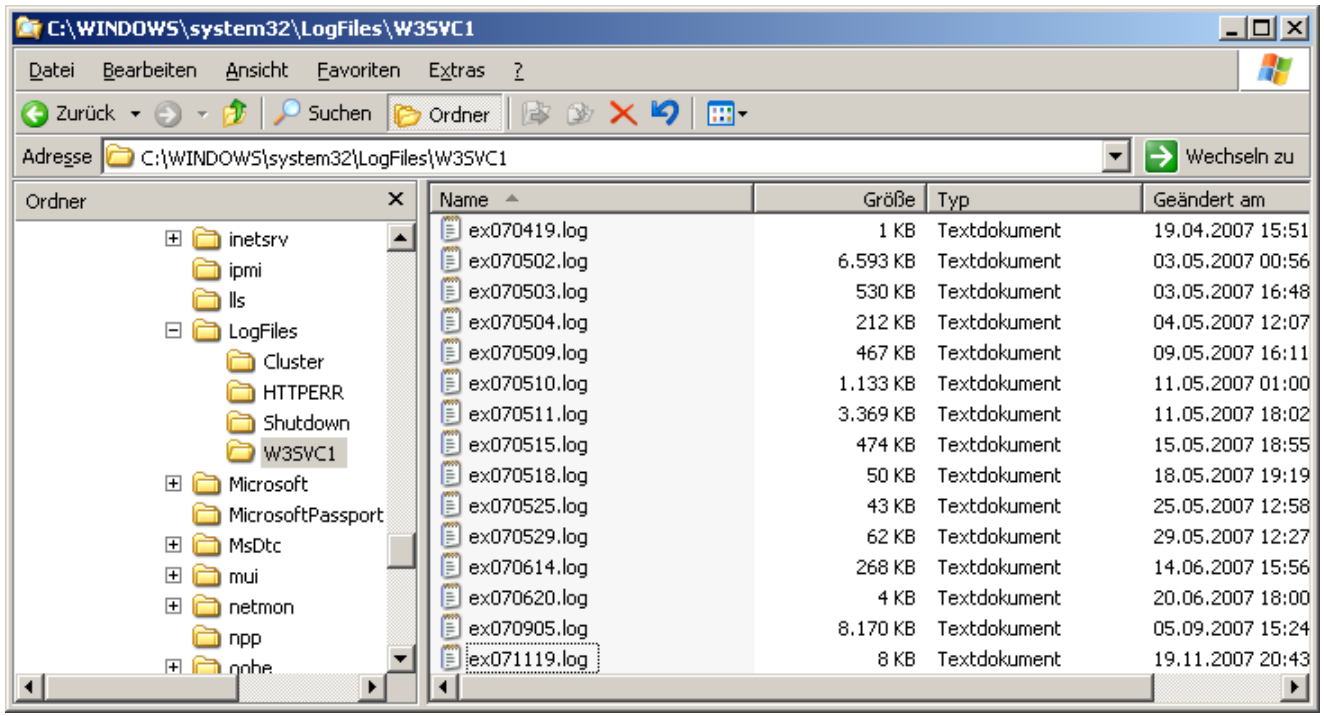


SSL

SSL erzwingen, Clientzertifkatbehandlung



Logging



W3C-Format der Quasi-Standard,
Logging sehr weitreichend konfigurierbar

R|R|Z|N

Absicherung

- Microsofts Best-Practise wenig hilfreich
- Nutzerkonfiguration, NTFS-Rechte
- Gruppenrichtlinien
- Standard-Tools zu Absicherung & Prüfung
  - Microsoft Baseline Security Analyzer (MSBA)
  - Security Configuration Wizard (SCW)
- evt. einige ISAPI-Filter

IIS-Lockdown-Tool & URLScan in IIS $\geq$ 6.0 überflüssig

Einschätzung/Empfehlung

Benutzen Sie lieber ein Unix-System mit Apache, es sei denn

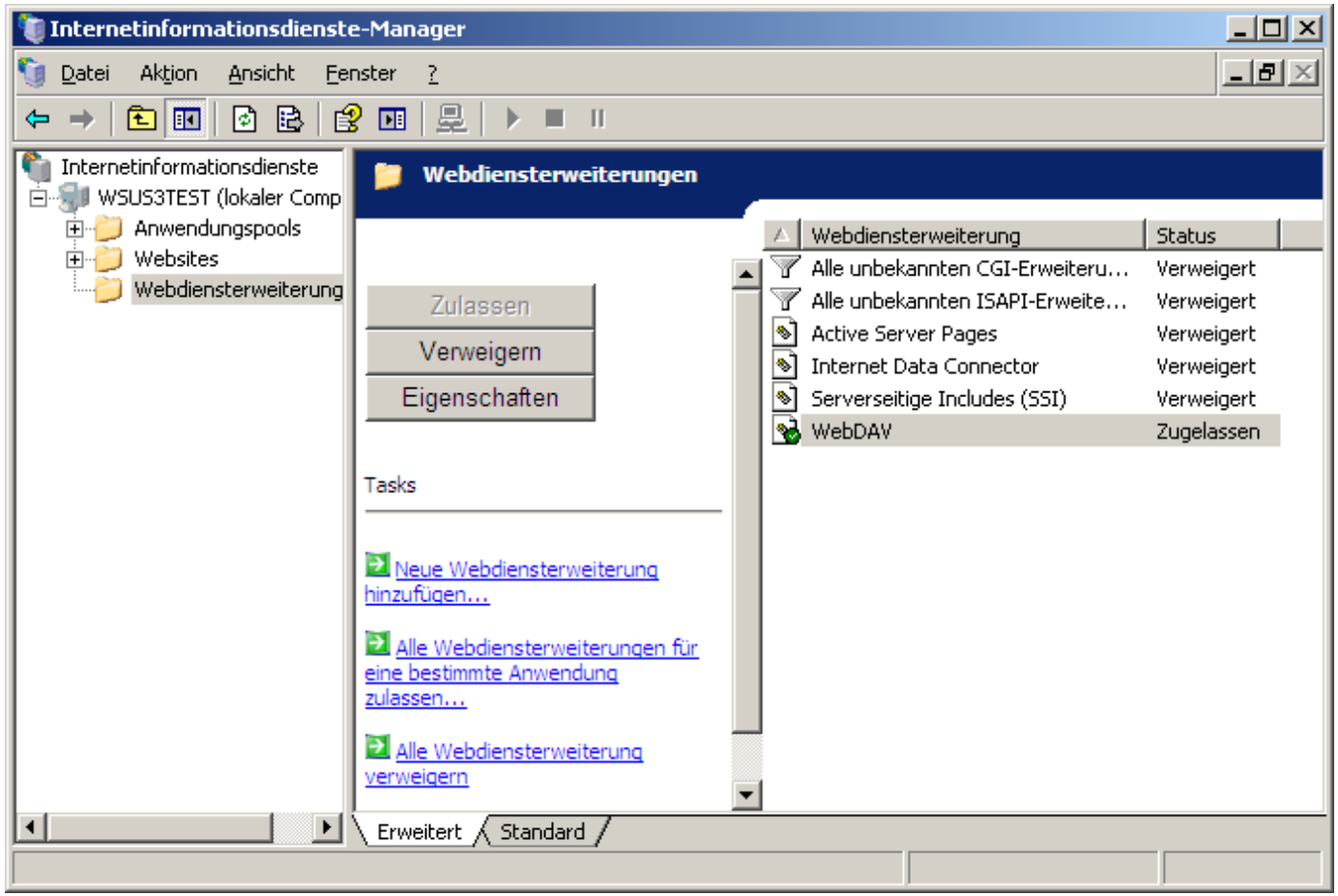
- Sie brauchen IIS für ein MS-Produkt (z.B. WSUS)
- Sie nutzen eine fertige ASP.Net-Applikation
- Sie haben Windows-Fileservices und wollen WebDAV nutzen

Begründung:

- schlechte Erfahrungen mit alten IIS-Versionen ≤ 5.1
- HTTP-Nutzer = (evt. reglementierter) Windows-Nutzer, keine zusätzliche Nutzerverwaltung
- unübersichtliche Konfiguration
- Verwundbarkeit des Betriebssystems selbst, viele Dienste & GUI haben auf Server nichts zu suchen[1]
- persönliche Meinung

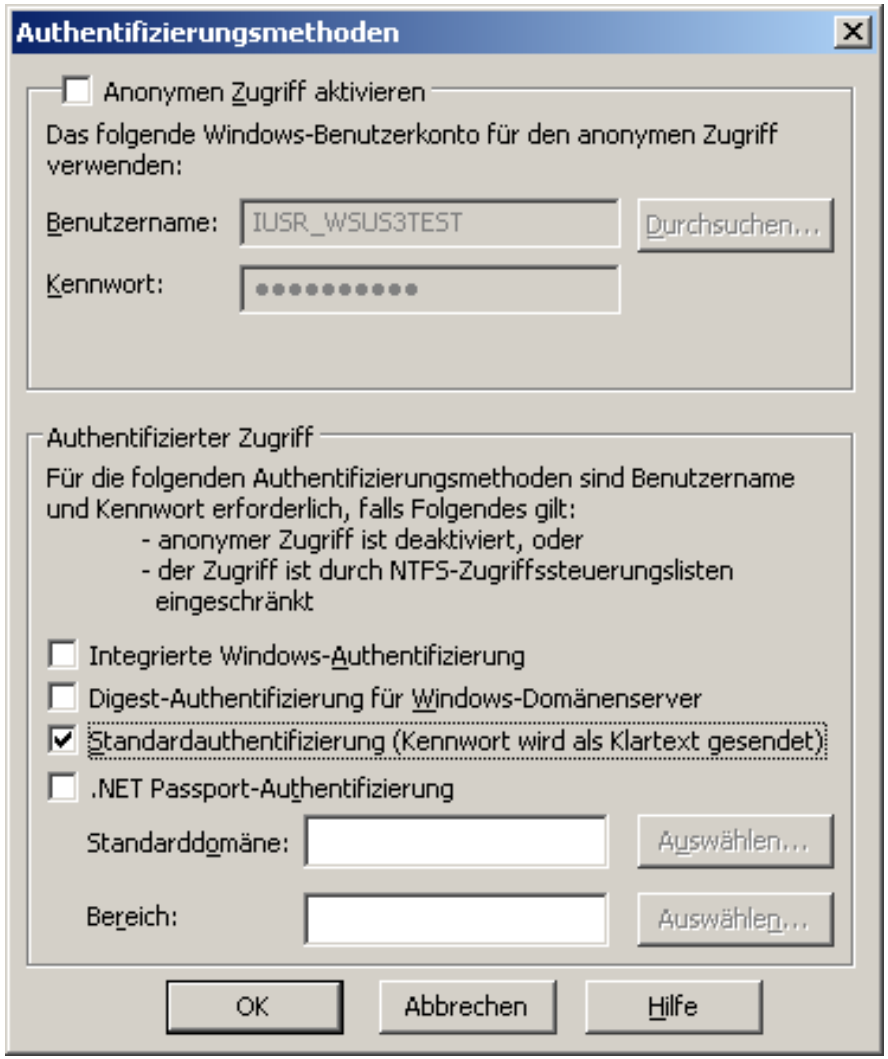
[1] Soll in Server 2008 besser werden

WebDAV-Dienst aktivieren

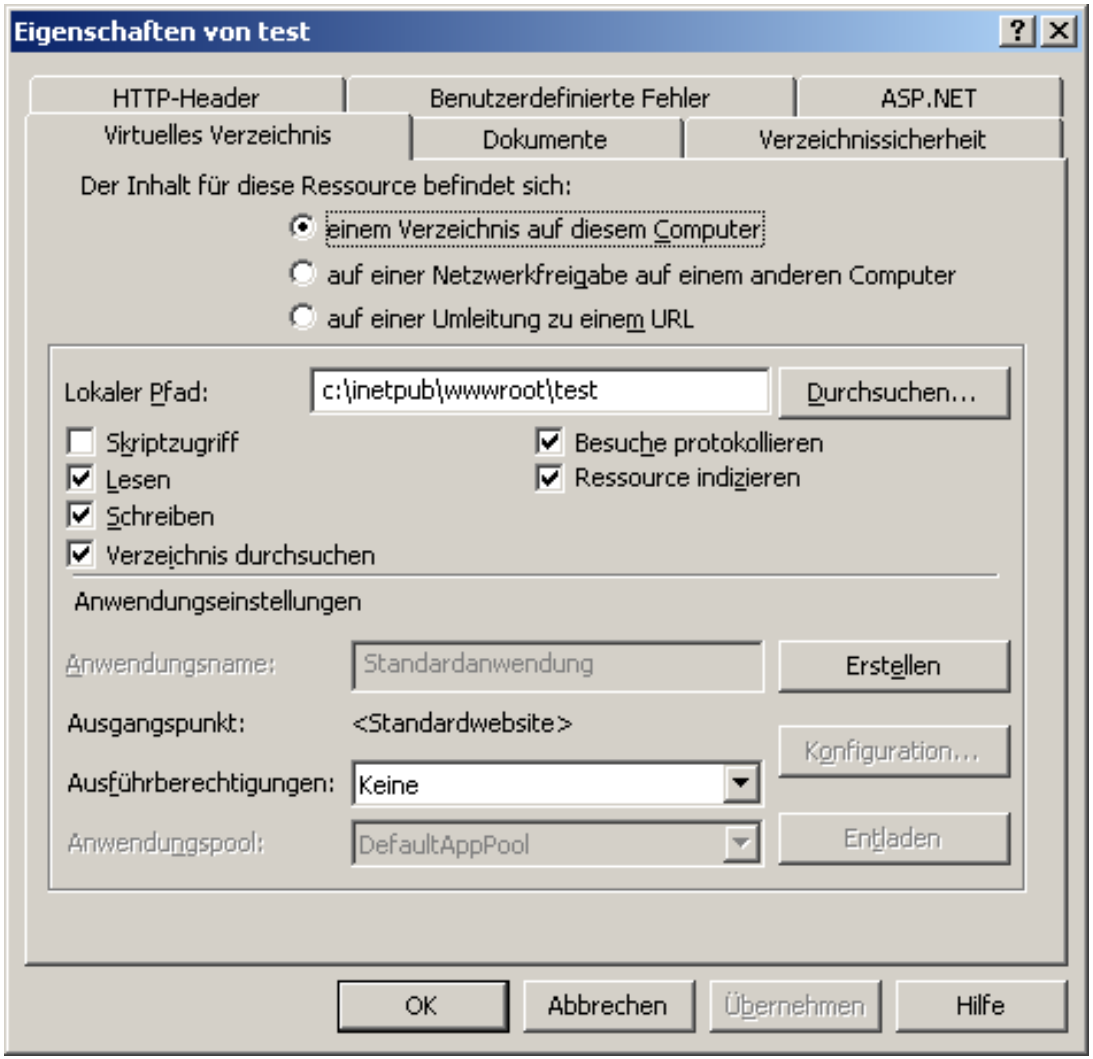


. . . und „verknüpftes Verzeichnis“ anlegen

HTTP-User=Windows-User ausnahmsweise sinnvoll



Mehr als Lesen notwendig



WebDAV-Erfahrung

. . . aber funktioniert hat es bei mir nicht auf Anhieb:

- habe es local auf dem Rechner versucht (http://localhost/test)
- auf Windows Server 2003 muss man als WebDAV-Client erst noch WebClient-Dienst starten
- Zwar funktionierte das Verbinden danach,
- aber eine Authentisierung war nicht möglich.