Microsoft | Managing Microsoft School Infrastructures

Skriptum
Managing Microsoft School Infrastructures

bm:bwk

it in Schulen GmbH

Microsoft

© 2004, Microsoft Österreich GmbH

Managing Microsoft School Infrastructures Skriptum – Version 1.1 im Jänner 2005

Microsoft Österreich GmbH
Am Euro Platz 3
1120 Wien

http://www.microsoft.com/austria/education

Dieses Werk ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Microsoft Österreich GmbH unzulässig und strafbar. Das gilt insbesondere für kommerzielle Nutzung dieses Skriptums.

Vorwort

Unsere Welt wird in zunehmendem Maße vernetzt. Auch an Österreichs Schulen sind Internetzugang und interne Vernetzung heute selbstverständlich, die IT-Infrastruktur wird weiter ausgebaut. Mit der zunehmenden Zahl von Computern, Benutzern und Netzwerkkomponenten stiegen die Anforderungen an das Kustodiat, damit alle dazu berechtigten Personen Daten zur richtigen Zeit und am richtigen Ort erreichen können.

Mit Abschluss des Microsoft College und High School Agreement (MS-ACH) im Juni 2003 ermöglichte das Bundesministerium für Bildung, Wissenschaft und Kultur allen höher bildenden Schulen Österreichs unter anderem die Nutzung der wichtigsten Server-Produkte von Microsoft. Von Anfang an war sowohl dem Ministerium als auch Microsoft bewusst, dass es nicht ausreicht, den Schulen Lizenzen zu geben. Sie müssen auch in der Lage sein, ein Schulnetzwerk zu installieren, zu konfigurieren und zu administrieren. Deshalb stellte Microsoft Österreich drei High School Advisors für die Betreuung der höheren Schulen bereit, die sich der Sorgen und Nöte der Kustoden annahmen.

Es zeigte sich schnell, dass die drei High School Advisors nicht alle Schulen direkt betreuen konnten, und so entwickelten sie gemeinsam mit Mag. Robert Beron, Mag. Franz Furtschegger und Otmar Haring einfache Step-by-Step-Anleitungen für den Microsoft Windows Server 2003. Seit September 2003 sind diese praktischen Anleitungen auf http://www.microsoft.com/austria/education verfügbar. Mehr als 10 000 Downloads im ersten halben Jahr und viel positives Feedback weit über die Grenzen Österreichs hinaus zeigen eindrucksvoll den enormen Bedarf an derartigen Schulungsmaterialien.

Einen Aspekt, den die Step-by-Step-Anleitungen nicht abdecken, ist das notwendige Basiswissen über Netzwerk- und Servertechnologien. So entstand der Wunsch nach einer speziellen Kustodenschulung, die dieses Wissen vermitteln sollte. Die Idee zum „Managing Microsoft School Infrastuctures"-Zertifikat (MMSI) war geboren.

Das eingespielte Team um die drei High School Advisors Mag. Georg Steingruber, Mag. Ulrike Müller und Thomas Kattinger entwickelte zusammen mit Mag. Robert Beron, Mag. Franz Furtschegger und Otmar Haring MMSI-Schulungsunterlagen, die Sie nun in Ihren Händen halten. Zusätzlich zu dem Skriptum entstand ein eigener Übungsteil, bestehend aus Labs und DVD.

Die vorliegenden Unterlagen sind in erster Linie zum Selbststudium gedacht und wie die Step-by-Step-Anleitungen unter obigem Link frei verfügbar. Darüber hinaus veranstaltet die IT an Schulen GmbH MMSI-Schulungen und bietet Prüfungen zum Erwerb des MMSI-Zertifikats an. Damit gibt es erstmals ein Zertifikat, das auf die speziellen Anforderungen der Kustoden abgestimmt ist und Ihnen und Ihrer Umwelt bescheinigt, dass Sie die Fachkompetenz zur Administration der IT-Infrastruktur an Schulen auf der Basis von Windows Server 2003 besitzen.

Ein Werk wie dieses entsteht mit Hilfe vieler Personen. Ich möchte an dieser Stelle allen danken, die zum Gelingen dieser Arbeit beigetragen haben: MR Dr. Christian Dorninger und Dr. Ernst Karner für ihr engagiertes Feedback bei der Konzeption des MMSI-Zertifikats, den zuvor genannten Autoren der MMSI-Unterlagen, sowie Wolfgang Hofmann für die Zusammenstellung der DVD und Mag. Yuri Goldfuß für die Gesamtkoordination. Danken möchte ich auch den Schülern des BG Mössingerstrasse und der HLW Biedermannsdorf für ihr fleißiges Korrekturlesen und ihre wertvollen Verbesserungsvorschläge.

Ich wünsche allen Lesern viel Erfolg beim Erwerb des MMSI-Zertifikats und lehrreiche Stunden mit diesen Unterlagen.

Dr. Ralph Zeller
Education Manager, Microsoft Österreich GmbH

Wien, November 2004

© 2005, Microsoft Österreich GmbH

Inhaltsverzeichnis

© 2005, Microsoft Österreich GmbH

© 2005, Microsoft Österreich GmbH

© 2005, Microsoft Österreich GmbH

© 2005, Microsoft Österreich GmbH

© 2005, Microsoft Österreich GmbH

© 2005, Microsoft Österreich GmbH

© 2005, Microsoft Österreich GmbH

1 Was Sie erwarten dürfen

Dieses Kapitel erläutert den allgemeinen Aufbau dieses Skriptums sowie die verwendeten Konventionen.

1.1 Überblick – Definition

Die Schulungsunterlagen sind in mehrere Teile gegliedert, die es ermöglichen, den Windows Server 2003 von der Installation bis zur Detailkonfiguration der einzelnen Dienste und Anwendungen kennen zu lernen.

Sie können dieses Werk aber auch als praktische Referenz nutzen, in dem Sie Anleitungen zur Lösung spezifischer Probleme finden.

Innerhalb eines Kapitels erhalten Sie allgemeine Informationen und Erklärungen über die einzelnen Installations- und Verwaltungsvorgänge des Windows Server 2003. Dazu gehören auch allgemein gehaltene Kurzanleitungen, die Ihnen helfen sollen, sich rasch einen Überblick über die jeweiligen Funktionen zu verschaffen.

Parallel zu jedem Kapitel finden Sie in den MMSI-Labs praktische Übungen, welche Ihnen die wichtigsten Arbeitsschritte und Vorgänge noch einmal in einer wesentlich spezifischeren Art erläutern. Dabei gehen diese Schulungsunterlagen von einem angenommenen Standardszenario aus. Die Definition dieses Szenarios finden Sie im nachfolgenden Kapitel 2 - *Planung*.

Die Kapitel behandeln folgende Inhalte und Themen:

Kapitel 1 gibt einen kurzen Überblick über die Inhalte, die Sie in diesen Schulungsunterlagen erwarten. Wir werden uns in den darauf folgenden Kapiteln detailliert mit den einzelnen Punkten beschäftigen und diese genau erläutern.

Kapitel 2 beschäftigt sich mit den Installationsvorbereitungen und der Planung einer Windows Server 2003-Installation. Wir werden über das Netzwerklayout und das Domänencontroller-Konzept nachdenken und diese anhand von Fallbeispielen erörtern.

Kapitel 3 behandelt die Installation bis zum ersten Start von Windows Server 2003. Unter anderem werden in diesem Kapitel die Hardwarevoraussetzungen behandelt und die verschiedenen Versionen des Betriebssystems vorgestellt.

In **Kapitel 4** werden wir die Konfiguration der einzelnen Netzwerkdienste vornehmen. Es gibt einen Überblick über das Active Directory, DHCP, WINS und DNS.

In **Kapitel 5** werden Sie sich mit der Verwaltung von Benutzern und Gruppen in einer Arbeitsgruppe beschäftigen.

In **Kapitel 6** wird näher auf die Benutzerverwaltung in einer Domäne eingegangen. Sie lernen, wie Sie Benutzer und Gruppen anlegen und wie die Benutzerverwaltung im Active Directory aussieht.

Kapitel 7 beschäftigt sich mit Gruppenrichtlinien in einer Domäne.

Kapitel 8 beschäftigt sich neben der Freigabe von Ordnern auch mit der Vergabe von Berechtigungen auf diese.

Kapitel 9 zeigt Ihnen die Installation von Clientrechnern. Sie erfahren, wie Sie Einstellungen von anderen Rechnern übertragen und die entsprechenden Netzwerkeinstellungen konfigurieren.

Kapitel 10 nimmt die Druck-Server-Funktionalität von Windows Server 2003 unter die Lupe. Sie werden Drucker und Druckaufträge sowohl lokal als auch im Netzwerk verwalten können.

Kapitel 11 widmet sich der Datensicherung. Sie werden Datensicherungen vornehmen und bestehende Sicherungen wiederherstellen. Außerdem lernen Sie die automatische Systemwiederherstellung und die Wiederherstellungskonsole kennen.

© 2005, Microsoft Österreich GmbH

Kapitel 12 beschäftigt sich mit Microsoft Software Update Services (SUS). Ziel von SUS ist es, den Zugang zu den neuesten Updates, Sicherheitsupdates und Service Packs zu erleichtern bzw. zu beschleunigen. Sie werden lernen, wie Sie in ihrem Schulnetz einen SUS-Server installieren und für den Einsatz im Schulalltag sinnvoll konfigurieren.

Als Abschluss dieses Skriptes finden Sie im Anhang noch drei zusätzliche Kapitel, die sich mit den Internet Information Services (IIS), der Kontingentverwaltung, sowie den Remote Installation Services (RIS) beschäftigen.

1.2 Vorausgesetzte Kenntnisse

Um die vorliegenden Unterlagen und die damit verbundenen Schulungen in einem vernünftigen Rahmen zu halten, sind die Autoren beim Erstellen des MMSI Skriptums und Labs von folgender Prämisse ausgegangen:

Die Leser der Unterlagen sind keine absoluten Neulinge im Bereich der Netzwerk-Administration. Insbesondere haben sich diese Personen bereits grundlegende Kenntnisse zu folgenden Themen angeeignet:

- Umgang mit einem Windows-Betriebssystems
- Netzwerktopologien und Technologien
- Einführende Kenntnisse über Netzwerkprotokolle
- Grundlagen von TCP/IP inklusive Konfiguration und Troubleshooting
- Darstellung von TCP/IP Adressen mit Hilfe von CIDR

1.3 Konventionen

Um die Lesbarkeit und das Verständnis zu erleichtern, werden verschiedene Schriftformate verwendet, um die unterschiedlichen Arten von Informationen hervorzuheben. So werden die Menübefehle in Versalien geschrieben, wie z. B.: Wählen Sie aus dem Menü DATEI den Befehl EIGENSCHAFTEN.

Schrittweise Anleitungen werden als nummerierte Aufzählungen dargestellt:

So erstellen Sie ein XYZ:

1. Wählen Sie die Option ALLE ANZEIGEN aus.
2. So werden die NAMEN von Menübefehlen dargestellt.

Hilfreich werden Sie vor allem die Tipps finden. Diese weisen auf Besonderheiten hin.

Wichtige Informationen sind folgendermaßen hervorgehoben:

Knifflige Details werden Sie häufig in einer solchen Hinweisbox lesen.

1.4 Gedanken zum Thema Sicherheit

Obwohl diese Schulungsunterlagen mehr als 350 Seiten umfassen, erheben sie weder Anspruch auf Vollständigkeit noch darauf, eine allgemein gültige Universalanleitung für die „perfekte" Planung und Implementierung einer Windows Server 2003-Infrastruktur zu sein.

Vor allem im Bereich der IT-Sicherheit mit all ihren Facetten, Stolpersteinen und Eigenheiten sollte man immer beachten, dass speziell in produktiven Systemen, also auch in einem Schulnetzwerk, individuelle und an die jeweilige Situation angepasste Vorkehrungen und Maßnahmen zu treffen sind.

Sowohl in der Planungs-, Implementierungs-, Verwaltungs- als auch in der Wartungsphase ist es absolut notwendig, das System immer auf dem neuesten Stand und möglichst sicher zu halten. Die Seiten der einzelnen Hard- und Softwarehersteller, allen voran Microsoft als Lieferant des Windows Server 2003, bieten dazu stets aktuelle Informationen.

In Zeiten der Mailviren und „RPC-Würmer" macht die Sicherung und Verwaltung eines Netzwerks einen nicht unerheblichen Teil des Verwaltungsaufwandes aus, der auf keinen Fall unterschätzt werden sollte. Ein Virus kann innerhalb einer Organisation schnell die wichtigsten Kommunikationsmittel und Wege lahm legen und einen nicht unbeträchtlichen wirtschaftlichen und immateriellen Schaden anrichten. Die Sicherheit kann und darf nicht außer Acht gelassen werden.

Es sei hiermit nochmals ausdrücklich auf die Dringlichkeit dieses Themas hingewiesen, jedoch auch auf den Umstand, dass es nicht möglich ist, in Schulungsunterlagen wie den vorliegenden alle sicherheitsrelevanten Informationen und Anweisungen unterzubringen. Dies würde nicht nur die Lesbarkeit und Handhabung erheblich stören, sondern auch den gegebenen Rahmen sprengen.

Mit den richtigen Informationen und dem entsprechenden Wissen lassen sich jedoch die meisten der heute vorhandenen Sicherheitsrisiken minimieren, wenn nicht sogar neutralisieren.

© 2005, Microsoft Österreich GmbH

2 Planung

Dieses Kapitel erläutert die Grundsätze der Planung vor einer Implementierung von Windows Server 2003.

2.1 Überblick - Definition

Jeder Aufbau eines Netzwerks, aber auch die Erweiterung oder Umkonfigurierung einer bestehenden Netzwerkinfrastruktur, bedarf einer guten Planung.

In der heutigen Zeit gibt es viele Möglichkeiten, Netzwerke aufzubauen und Geräte miteinander zu verbinden, wobei nicht nur der Kostenfaktor einen wichtigen Entscheidungspunkt darstellt.

2.2 Aufbau und Planung

Die grundlegende Vorgehensweise sollte in folgende Phasen aufgeteilt werden:

Analyse

Während dieser Phase legen Sie die IT-Ziele fest.

Sie müssen sich Gedanken über die nötige Bandbreite machen, Sicherheitsanforderungen festlegen und das Kosten/Nutzenverhältnis berücksichtigen.

Entwurf

In dieser Phase bewerten Sie das Infrastrukturkonzept. Sie wägen ab, welche Funktionen Ihr Netzwerk bereitstellen muss. Die Entwurfphase basiert auf der Analyse. Zu den Funktionen zählen unter anderem DNS, DHCP und die verwendeten Netzwerkprotokolle.

Test

Sie sollten ein Pilotprojekt in einer produktiven Umgebung mit einer geringen Zahl von Benutzern starten. Die Ergebnisse dieses Projekts zeigen Ihnen, ob Korrekturen am Netzwerkentwurf nötig sind, um eine stabile Netzwerkumgebung zu erreichen.

Produktion

In der letzten Phase können Sie das Pilot-Netzwerk auf die gesamte Umgebung ausweiten. Zusätzlich sollten Sie Notfallpläne erstellen, damit – falls wider Erwarten Probleme auftreten sollten – die zuständigen Personen das System wiederherstellen bzw. funktional halten können.

Bei der Planung eines Netzwerks sind auch die folgenden Begriffe und Techniken von Bedeutung: Domänencontroller, Domänenhierarchie, Netzwerktopologien.

2.3 Standardkonfiguration für die Schule

2.3.1 Allgemein

Die in diesem Kurs verwendete Konfiguration beruht auf der Annahme, dass pro Schule zwei Domänencontroller verwendet werden. Als Clientrechner stehen mindestens 100 Desktop PCs bereit, zuzüglich eventueller Notebook-Klassen. Das System sollte für etwa 500 bis 1000 Benutzer ausgelegt sein und die anfallende Arbeitslast tragen können.

© 2005, Microsoft Österreich GmbH

Grundsätzlich sollten die notwendigen Dienste und die damit verbundenen Lasten auf mehrere Serverinstanzen verteilt werden.

2.3.2 Konfiguration

Folgende Konfiguration besteht aus zwei Servern, auf denen die folgenden Dienste verteilt werden:

Server 1 (SRV01):

Normal

- Domänencontroller (Active Directory)
- DNS
- DHCP
- Internet Security & Acceleration Server (ISA Server)
  - Installation/Konfiguration ist nicht Teil dieser Schulungsunterlagen
- Dateiserver
- Applikationsserver

Server 2 (SRV02):

- Domänencontroller (Active Directory)
- DNS
- Druckserver
- RRAS (falls Segmentierung gewünscht ist)
- Exchange Server
  - Installation/Konfiguration ist nicht Teil dieser Schulungsunterlagen

© 2005, Microsoft Österreich GmbH

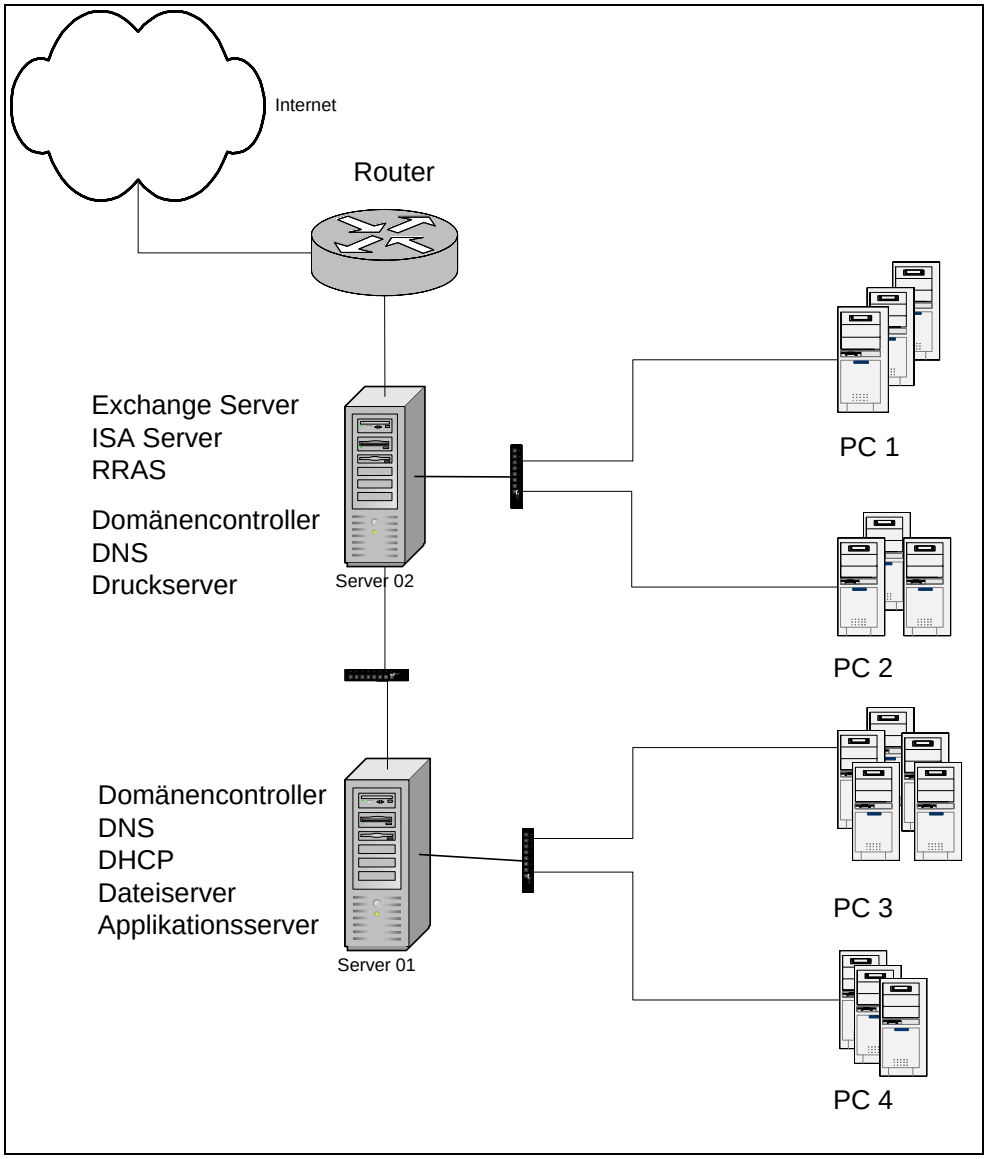


Abb. 1: Server-Konfiguration

2.3.3 IP-Adressen-Schema

Folgendes IP-Adressen-Schema wird für die Konfiguration einer Standardschule angenommen:

Element	IP-Adresse
Domänencontroller	192.168.1.1 und 192.168.1.2
Subnetzmaske	255.255.255.0

DNS-Server	192.168.1.1 und 192.168.1.2
DHCP-Server	192.168.1.1
Standardgateway	192.168.1.1
Exchange Server	192.168.1.2
Externes Web	192.168.1.2

2.4 Domänencontroller

Ein Domänencontroller ist der Server-Computer in Microsoft-Netzwerken, der die Anmeldungen an einer Domäne verifiziert. Des Weiteren verwaltet er die Sicherheitsrichtlinien und die Datenbank, in der die Benutzer, Benutzergruppen und Computer einer Domäne enthalten sind.

Domäne

Eine Domäne hingegen ist nichts anderes als eine Sammlung von Computern und Benutzern, die eine gemeinsame Datenbank- und Sicherheitsrichtlinie verwenden. Verschiedene Domänen können auch hierarchisch miteinander verbunden sein.

Domänencontroller (Domain Controller, DC)

Jede Domäne muss mindestens einen Domänencontroller haben. Dieser Server verwaltet die Benutzerdatenbank der Domäne und überprüft die Anmeldungen. Aus Gründen der Fehlertoleranz werden in der Praxis meist zusätzliche Domänencontroller eingesetzt.

Dafür sprechen mehrere Gründe, fällt z. B. ein DC aus, so kann der andere die Validierung der Benutzer übernehmen. Des Weiteren wird die Anmeldelast auf mehrere Domänencontroller aufgeteilt.

Damit im Falle des Ausfalles des ersten DC eine Benutzeranmeldung am zweiten DC möglich ist, ist dort ebenfalls die Global Catalog Funktion zu aktivieren.

2.5 Netzwerklayout

Die Wahl des Netzwerklayouts betrifft auf der einen Seite die verwendete Hardware und auf der anderen Seite die Konfigurationsmöglichkeiten, die durch die Verwendung der Serversoftware gegeben sind.

© 2005, Microsoft Österreich GmbH

Sternförmiges Netzwerk

Diese Form der Netzwerke ist die am weitesten verbreitete Topologie. Die Computer sind mittels Kabel sternförmig an ein Gerät gebunden, das die Weiterleitung des Netzwerkverkehrs übernimmt.

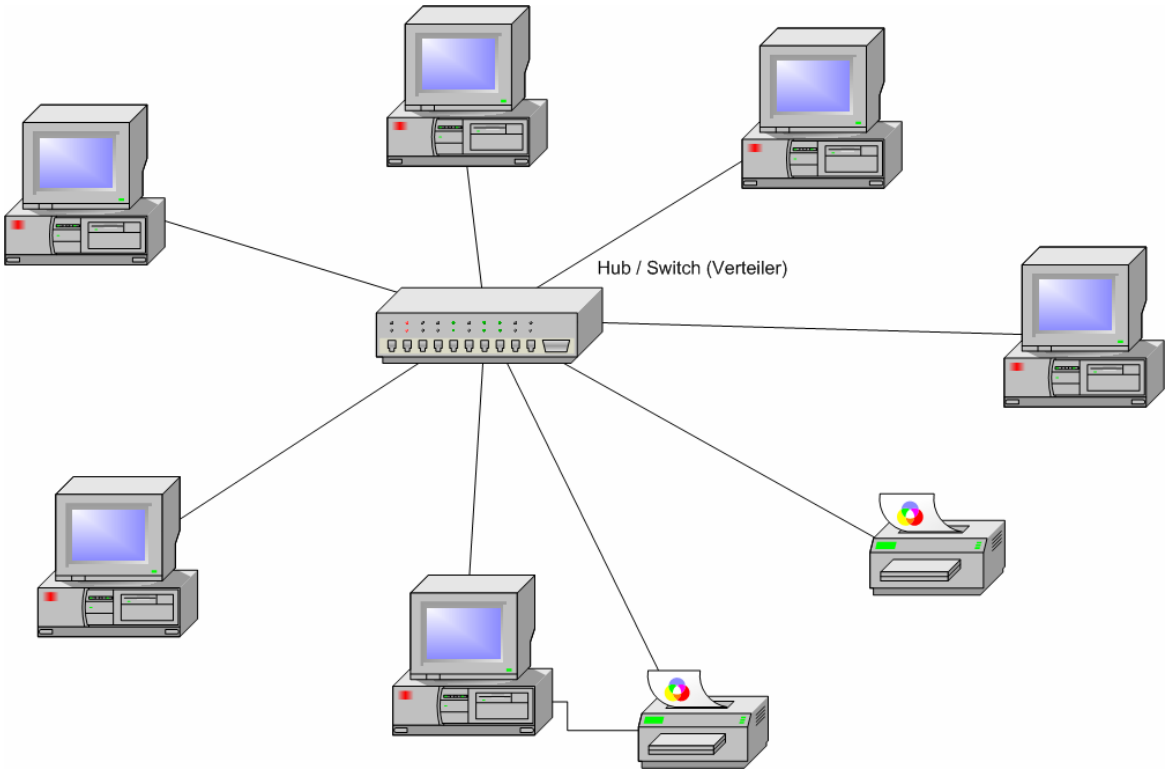


Abb. 2: Sternförmiges Netzwerklayout

Folgende Geräte kommen hierbei zum Einsatz:

Hubs (Verteiler), **Switches** oder **Router**. Diese Geräte unterscheiden sich vor allem darin, wie sie den Verkehr weiterleiten.

So schicken Hubs die ankommenden Datenpakete an jeden Anschluss im Gerät, wohingegen Switches genau wissen, hinter welchem Anschluss welcher Client hängt und die Datenpakete entsprechend abliefern. Normalerweise sind die Geräte, die an Hubs bzw. Switches hängen, immer im selben Netzwerksegment.

Router haben den Vorteil, dass diese hoch konfigurierbar sind und den Netzwerkverkehr auch zwischen verschiedenen Netzwerksegmenten weiterleiten können.

In der heutigen Zeit ist diese Form der Vernetzung die am weitesten verbreitete.

(Derzeitige) Geschwindigkeit: 100 Mbps bis 1 Gbps

Andere Topologien

Weitere Netzwerktopologien sind busförmige Netzwerke und Ringnetzwerke. Die Namen weisen schon auf die Art und Weise der Verkabelung hin. Diese Netzwerke bieten aber keine hohe Ausfallsicherheit, weswegen sie heutzutage nur noch in Spezialfällen angewandt werden.

Ringstruktur

Bei einem Netzwerk mit Ring-Topologie sind die Geräte über eine einzige – vorstellbar als ringförmig verlaufende – Leitung gleichberechtigt miteinander verbunden. In Wirklichkeit werden die einzelnen Rechner über ein hin- und rückführendes Kabel an einer so genannten MAU (Medium Attachement Unit) angeschlossen. Es gibt keinen zentralen Rechner. Jedes

© 2005, Microsoft Österreich GmbH

Gerät verfügt über einen eigenen Netzanschluss und ist über diesen mit seinem linken und rechten "Nachbarn" verbunden. Die Übertragung der Informationen erfolgt immer in einer Richtung von Station zu Station. Jede Station untersucht bei einer empfangenen Nachricht die darin enthaltene Zieladresse und nimmt die Nachricht entgegen, wenn diese Adresse mit der eigenen übereinstimmt. Andernfalls regeneriert sie das Signal und leitet die Nachricht, wie ein Repeater, zur nächsten Station im Ring weiter. Der Ausfall eines Computers hat bei der Ringstruktur also Einfluss auf das gesamte Netzwerk.

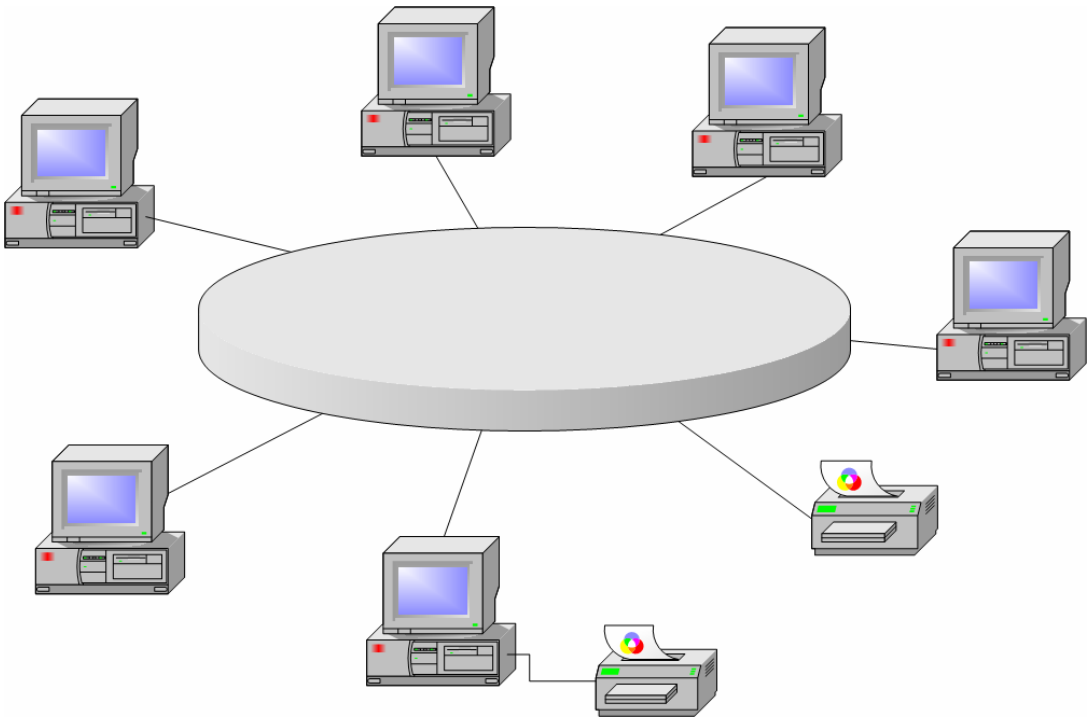


Abb. 3: Ringförmiges Netzwerk

Busstruktur

Die Bus-Topologie ist die einfachste und in der Vergangenheit am häufigsten verwendete Struktur für die Verkabelung. Auch hier gibt es keine Zentrale, die Verbindung aller Geräte erfolgt über eine gemeinsame Hauptkommunikationsleitung (Backbone). Die einzelnen Stationen verstärken die Signale bei dieser Topologie nicht, dadurch kommt es zu einer Dämpfung und Abschwächung. Die Länge der Bus-Topologie ist somit auf ca. 185 Meter begrenzt. Durch den Einsatz von Repeatern kann sie jedoch verlängert werden. An den beiden Kabelenden benötigen Bus-Netze einen Abschlusswiderstand, damit keine Echos auftreten, die zu Empfangsfehlern führen.

In einem Bus-Netzwerk beobachtet jede Station die Aktivitäten auf der Leitung. Nachrichten werden von allen Stationen erkannt, aber nur von den Stationen angenommen, für die eine Nachricht bestimmt ist.

Zu einem Zeitpunkt kann immer nur eine Nachricht über den Bus transportiert werden. Daher hängt die Leistung des Netzwerks davon ab, wie viele Geräte angeschlossen sind und in welchem Umfang die angeschlossenen Rechner das Netzwerk nutzen. Falls ein Rechner ausfällt, kann er zwar nicht mehr mit dem Netzwerk kommunizieren, die Funktionsfähigkeit des Netzwerks wird jedoch nicht beeinträchtigt. Die Unterbrechung des Kabels an einer Stelle führt jedoch zur Unterbrechung des gesamten Netzbetriebs.

© 2005, Microsoft Österreich GmbH

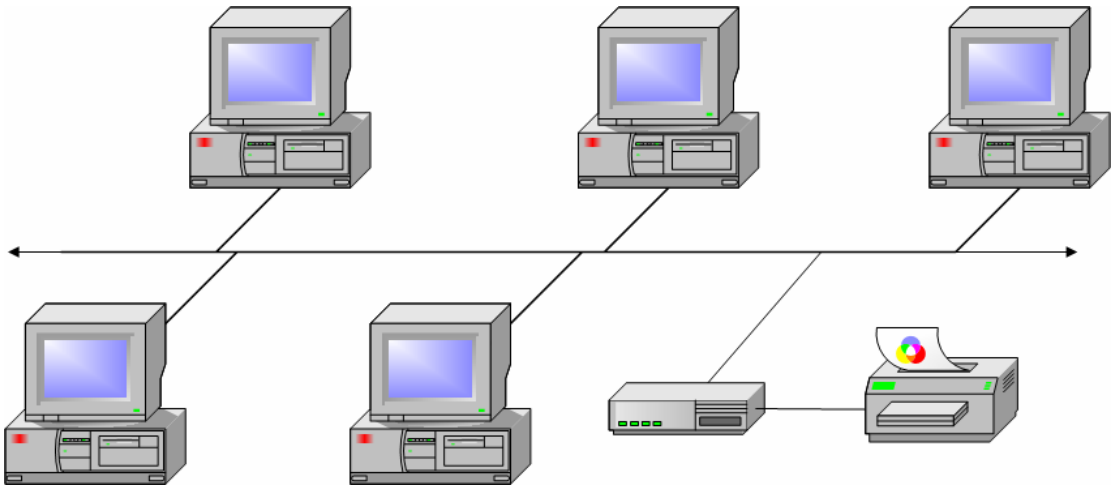


Abb. 4: Busförmiges Netzwerk

Speziell bei der Wahl der Netzwerktopologie sollten Sie auch zukünftige Entwicklungen und Anforderungen an Ihr Netzwerk im Auge behalten, da ein Topologiewechsel häufig mit sehr hohen Kosten einhergeht.

Empfehlung für Schulen: Strukturierte Verkabelung

Die Vergangenheit hat gezeigt, dass lokale Netze immer größer werden. Die oben beschriebenen Topologien können nur mit erheblichem Aufwand erweitert werden. Die strukturierte Verkabelung beschreibt eine hierarchische Baumstruktur. Von einem zentralen Kabelstrang, gewissermaßen dem »Stamm« des Baumes, gehen nach beliebigen Richtungen einzelne Verästelungen ab, an denen entweder eine einzelne Station oder ein ganzes sternförmiges Netz hängt. Diese kann sehr leicht erweitert werden und gilt deshalb als einzig zukunftssichere Topologie.

2.6 Aussicht Exchange, SQL

In einem Netzwerk übernehmen bestimmte Server festgesetzte Aufgaben. Windows Server 2003 stellt die grundlegenden Netzwerkfunktionen zur Verfügung. Es kann in weiterer Folge aber durchaus auch wünschenswert sein, bestimmte Funktionalitäten auf eigene, dedizierte Server auszulagern, um die Arbeitslast der einzelnen Server zu minimieren:

Exchange Server 2003

Dazu zählen unter anderem die E-Mail-Funktionen. Windows Server 2003 verfügt über einen integrierten SMTP (Simple Mail Transfer Protocol) und POP3 (Post Office Protocol 3) Server. Viel leistungsfähiger, speziell im Zusammenwirken mit Microsoft Office, ist der Exchange Server 2003. Mit Microsoft Exchange Server 2003 können Sie nicht nur jederzeit, orts- und clientunabhängig auf Ihre Emails zugreifen, sondern auch Aufgabenlisten, Kalender, Notizen, Kontakte, Dokumente und vieles mehr mit den unterschiedlichsten Geräten über das Internet verwalten.

SQL Server

Im Windows Server 2003 ist kein Datenbank Management System inkludiert. Wollen oder müssen Sie eine Datenbank in Ihrem Netzwerk betreiben – z. B. wenn Sie den Microsoft Class Server als Learning Management System verwenden – müssen Sie auf andere Anwendungen zurückgreifen.

Der Microsoft SQL Server ist ein leistungsfähiges relationales Datenbank-Management-System, mit dem Sie große Mengen an Daten verarbeiten und bereitstellen können.

© 2005, Microsoft Österreich GmbH

ISA (Internet Security and Acceleration) Server

Der ISA Server stellt grundlegende Firewall- und Proxyserver-Funktionalitäten zur Verfügung.

Über die Firewall-Funktionen des ISA Servers haben Sie die Möglichkeit, den Verkehr von Ihrem Schulnetz ins Internet bzw. vom Internet in Ihr Schulnetz zu kontrollieren. Diese Kontrolle geht sogar so weit, dass Sie Beschränkungen auf Benutzerebene (und nicht nur auf Protokollebene) festlegen können.

Die Proxyserver-Funktionen werden benötigt, damit der externe Internetverkehr ins lokale Netzwerk weitergeleitet wird. Außerdem können auf einem Proxyserver viele Regeln erstellt werden, die den Administratoren erlauben, bestimmte Anwendungen und Dienste im Internet für ihre User frei zu schalten oder zu sperren.

Wichtig in diesem Zusammenhang ist auch die Protokollierungsfähigkeit. Mit Hilfe eines Proxyservers überblicken Administratoren jederzeit, welche Benutzer auf welchen Internetseiten surfen und wie viel Verkehr letztendlich generiert wurde. Des Weiteren wird bei aktivierter Cachefunktion der Internetverkehr minimiert, da die angesurften Seiten auf dem Proxyserver zwischengespeichert werden und so nur einmal vom Internet herunter geladen werden.

© 2005, Microsoft Österreich GmbH

3 Installation

Dieses Kapitel erläutert die Installation von Windows Server 2003 sowie das erstmalige Einrichten eines Domänencontrollers.

3.1 Überblick – Definition

Dieses Kapitel wird Ihnen einen Überblick über die Installation des Betriebssystems Windows Server 2003 geben.

Dieses Kapitel kann jedoch nur einen allgemeinen Einblick in die Standardkonfiguration des Systems liefern, detailliertere Informationen über die Planung und Installation von Windows Server 2003 erhalten Sie online unter http://www.microsoft.com/windows/reskits (Resourcekits) bzw. unter http://www.microsoft.com/windowsserver2003/proddoc (Produktdokumentationen).

Nachdem Sie dieses Kapitel durchgearbeitet haben, beherrschen Sie Folgendes:

- Abklärung der Hardwarevoraussetzungen
- Wahl der geeigneten Betriebssystem-Edition
- Vorarbeiten (Installation spezieller Hardware)
- Partitionierung des Festplattensystems
- Basisneuinstallation
- Starten des neu installierten Systems
- Erstinstallation eines Domänencontrollers (DC)

3.2 Vorüberlegungen

3.2.1 Allgemeines

Grundsätzlich gibt es mehrere Möglichkeiten, ein Produkt der Windows Server 2003-Familie zu installieren. Zum einen können Sie Windows Server 2003 vollständig neu installieren, zum anderen können Sie eine bestehende Windows 2000- oder NT 4.0-Installation upgraden.

In diesem Skriptum wird nur die Neuinstallation eines Windows Servers 2003 besprochen, da für ein Upgrade zusätzliche Überlegungen im Umfeld anzustellen sind bzw. ein Upgrade auf ein Produkt der Windows Server 2003-Familie mehr Probleme aufwerfen kann als eine Neuinstallation.

© 2005, Microsoft Österreich GmbH

3.3 Hardware-Voraussetzungen

Der folgenden Tabelle können Sie die von Microsoft empfohlenen Systemvoraussetzungen für die verschiedenen Betriebsystemeditionen entnehmen:

Voraussetzungen	Standard Edition	Enterprise Edition	Web Edition
Minimale CPU-Geschwindigkeit	133 MHz	133 MHz für auf x86 basierende Computer	133 MHz
Empfohlene CPU-Geschwindigkeit	550 MHz	733 MHz	550 MHz
Minimaler Arbeitsspeicher	128 MB	128 MB	128 MB
Empfohlener Arbeitsspeicher	256 MB	256 MB	256 MB
Maximaler Arbeitsspeicher	4 GB	32 GB für auf x86 basierende Computer	2 GB
Multi-Prozessor-Unterstützung	*	Bis zu 8	Bis zu 2
Benötigter Speicherplatz	1,5 GB	1,5 GB für auf x86 basierende Computer	1,5 GB

** Die Standardedition von Windows Server 2003 unterstützt unter Umständen keine Multi-Prozessor-Systeme, die Pentium Pro oder Pentium II verwenden. Nähere Informationen dazu finden Sie in Microsoft Knowledge Base im Artikel:*
319091 Windows Server 2003 May Not Use Multiple Processors with Some Pentium Pro or Pentium II Processors

3.3.1 Angenommene Mindestkonfiguration

Die bisherigen Erfahrungswerte zeigen, dass die vorgeschlagenen Werte nur bedingt zutreffen. Vielmehr ist die Auslegung der eingesetzten Hardware je nach Einsatzszenario unterschiedlich. Daher nehmen wir für die Demonstration der einzelnen Übungen und Beispiele in diesem Skriptum folgende Mindestkonfiguration an:

Arbeitsspeicher	256MB RAM oder höher
CPU	x86-kompatibler Prozessor
Taktfrequenz	1GHz oder höher
Festplatte	Mindestens eine IDE Platte 40GB oder höher

In Bezug auf das verwendete Speichersystem ist keine allgemeingültige Aussage möglich. Aus Kostengründen und der mittlerweile geringeren Performanceunterschiede zwischen normalen die- und SCSI-Speichersystemen wäre es durchaus praktikabel, einen IDE RAID-Verbund einzusetzen. Nehmen Skalierbarkeit und Ausfallssicherheit einen höheren Stellenwert ein, empfiehlt sich der Einsatz eines SCSI-RAID-Speichersystems.

3.3.2 Hardware-Kompatibilität

Einer der wichtigsten Schritte vor einer Installation von Windows Server 2003 ist, zu überprüfen, ob die verwendete Hardware kompatibel zur geplanten Betriebssystem-Edition ist. Diese Überprüfung kann durch Ausführen des so genannten „Preinstallation Compatibility Check" (infolge eines Windows-Upgrades) erfolgen oder durch den Vergleich mit den Angaben auf der Windows-Katalog-Website. Vor allem ist eine aktuelle Version des „Basic Input Output Systems" (BIOS) sowie aller verwendeten Hardwaretreiber bereitzuhalten. Eine entsprechende aktuelle Version erhalten Sie von Ihrem Hardwarehersteller.

3.3.3 Wahl der Betriebssystem-Edition

Die Windows Server 2003-Familie besteht derzeit aus vier unterschiedlichen Versionen. Diese Editionen, wie Microsoft sie gern nennt, haben jeweils einen eigenen, streng abgesteckten Einsatzbereich. Daher sollte man sich vor einer Installation natürlich ausführlich mit den jeweiligen Spezialitäten der einzelnen Editionen auseinandersetzen.

Dieser Abschnitt versteht sich nicht als komplette Darlegung aller Features der einzelnen Produkte, vielmehr soll ein kurzer und prägnanter Überblick gewährt werden.

Eine komplette Vergleichsaufstellung der Features der einzelnen Produkte kann unter diesem Link aufgerufen werden: http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx?

Windows Server 2003 Standard Edition

ist die passende Server-Plattform für Abteilungen und kleinere Unternehmen. Diese Edition ermöglicht Datei- und Drucker-Sharing, sichere Internet-Anbindung und eine zentrale Applikationsverteilung.

Windows Server 2003 Enterprise Edition

ist die grundsätzliche Antwort auf die Anforderungen von Unternehmen aller Größenordnungen. Sie ist die optimale Plattform für Applikationen, Web Services und Infrastruktur mit einem exzellenten Maß an Hochverfügbarkeit.

Sie unterstützt bei auf x86 basierenden Computern bis zu 8 Prozessoren, bis zu 32 GB Arbeitsspeicher und 8fach Clustering.

Windows Server 2003 Datacenter Edition

wurde entworfen, um den Ansprüchen an höchste Verfügbarkeit, Skalierbarkeit und Sicherheit gerecht zu werden. Sie unterstützt bei auf x86 basierenden Computern bis zu 32 symmetrische Prozessoren und bis zu 64 GB Arbeitsspeicher. Ebenso sind 8fach Clustering und Load-Balancing möglich.

Windows Server 2003 Web Edition

ist eine Neuerung in der Familie der Microsoft Windows Server. Sie ist speziell auf den Einsatz als Web Applikation Server optimiert und damit für alle Formen des Hostings von Webanwendungen, Websites und XML Web Services geeignet. Damit wird eine spezielle Version für die Unterstützung von ASP.NET-Seiten geliefert, die einen Schlüsselbereich der .NET-Strategie von Microsoft darstellen. Der Einsatz als Domänencontroller ist nicht möglich, wohl aber die Integrierbarkeit in einer Active-Directory-Domäne.

3.3.4 Wahl des Lizenzmodells

Die Produkte der Windows Server 2003-Familie unterstützen zweierlei Lizenzmodelle. Zum einen die Lizenzierung pro Anwender beziehungsweise pro Clientrechner (per Device/per User Mode) und zum anderen die Lizenzierung pro Server (per Server Mode).

„Pro Gerät"- oder „Pro Benutzer"-Modell

Bei Anwendung des „Pro Gerät"- oder „Pro Benutzer"-Modells benötigt jeder Clientrechner beziehungsweise jeder Benutzer eine eigene so genannte „Client Access Licence", kurz (CAL).

Mit einer CAL kann ein einzelner Rechner oder Benutzer sich zu einer beliebigen Zahl von Servern verbinden, auf denen Windows Server 2003 als Betriebssystem läuft. Dies ist das wohl am häufigsten eingesetzte Modell und gleichzeitig die empfohlene Variante, wenn innerhalb eines Unternehmens oder einer Abteilung mehrere Server betrieben werden.

„Pro Server"-Modell

Im Gegensatz dazu steht die Anwendung des „Pro Server"-Modells, bei dem jede separat bestehende Verbindung zu einem Server eine eigene CAL benötigt. Dies bedeutet, dass jeder Server nur eine gewisse, zuvor definierte Anzahl an gleichzeitigen Verbindungen akzeptiert. Würde man einen Server nach diesem Modell mit fünf Lizenzen betreiben, bedeutete dies, dass der Server gleichzeitig maximal fünf Zugriffe von einzelnen Clientrechnern erlaubt.

Der Server kann den Versuch, mit ihm eine Verbindung herzustellen, abweisen, sofern das Maximum an Verbindungen erreicht ist.

Bei der Installation von Windows Server 2003 im Rahmen der Vereinbarung mit dem bm:bwk innerhalb einer Schule ist das **„Pro Gerät"- oder „Pro Benutzer"-Modell** zu wählen.

3.3.5 Wahl des Dateisystems

Prinzipiell stehen drei mögliche Dateisysteme für die Installation eines Produkts aus der Windows Server 2003-Familie zur Verfügung:

- NTFS
- FAT
- FAT32

Das zu wählende Dateisystem ist NTFS, da mit Hilfe dieses Systems die größten Leistungsreserven der verschiedenen Editionen freigesetzt werden.

3.3.6 Dateisystem-Kompatibilität

Die Änderung des Dateisystems auf einem Computer, der mehrere Betriebssysteme enthält, stellt sich als weitaus komplexer dar, als auf einem System mit nur einem durchgängigen Dateisystem.

NTFS ist das empfohlene Dateisystem, da dieses – im Vergleich mit FAT oder FAT32 – spezielle und erweiterte Funktionen bietet. Speziell Windows 2000, Windows XP und Windows Server 2003 bieten gänzlich neue Paradigmen und Features als Windows NT. Dateien, die diese neuen Funktionen nutzen, sind unter Windows NT nicht mehr verwend- und lesbar.

© 2005, Microsoft Österreich GmbH

3.3.7 Anwendungsszenarios

Folgende Auflistung stellt verschiedene Anwendungsszenarios und die jeweils empfohlene Wahl des Datei-Systems dar:

Szenario	Wahl - Dateisystem
Das aktuelle Dateisystem auf dem Zielrechner ist bereits NTFS (kein FAT oder FAT32 System).	Sie können dieses Dateiformat weiterverwenden, es ist keine Änderung notwendig.
Das aktuelle Dateisystem auf dem Zielrechner besteht aus FAT- oder FAT32-Partitionen. Das Betriebs-system ist Windows 2000, Windows XP oder ein Produkt aus der Windows Server 2003-Familie.	Sie sollten eine Formatierung oder Konvertierung des bestehenden Dateisystems auf NTFS in Erwägung ziehen. "CONVERT *LW*: /FS:NTFS"

ACHTUNG: Die Konvertierung von FAT oder FAT32 auf NTFS ist unter Beibehaltung der Daten möglich. Eine Rückkonvertierung von NTFS auf das vorhergehende Format ist nicht vorgesehen und daher NICHT möglich (kann nur über eine Neuformatierung erreicht werden)!

3.3.8 Spezielle Hardwaretreiber für die Installation

Wenn Sie von Ihrem Hardwarehersteller spezielle Treiber für Massenspeichergeräte wie etwa Raid-Controller, Fibre-Channel Controller oder ähnliches erhalten und diese anstelle der Standardtreiber während der Installation verwenden möchten, müssen Sie die entsprechenden Daten auf einer Diskette bereithalten.

So installieren Sie einen speziellen Treiber für Massenspeichergeräte:

1. Starten Sie das Setup.
2. Während der frühen Phase der Installationsroutine erscheint im unteren Bereich des Bildschirms eine Aufforderung, die Taste F6 zu drücken.
3. Betätigen Sie die Taste F6.
4. Folgen Sie den Anweisungen am Bildschirm, um Ihren eigenen Treiber zu installieren.

Wenn Sie nicht sicher sind, ob Sie die speziellen Treiber des Herstellers benötigen, versuchen Sie, die Installationsroutine ohne diese laufen zu lassen. Wenn das Setupfile die verwendete Hardware nicht mit den Standardtreibern installieren kann, erscheint eine Fehlermeldung und die Installation wird abgebrochen. Organisieren Sie die entsprechenden Treiber, starten Sie das Setup erneut und folgen Sie den Anweisungen weiter oben in diesem Absatz.

© 2005, Microsoft Österreich GmbH

3.3.9 Partitionierung

Unter Partitionieren versteht man das Unterteilen des physikalischen Festplattenspeichers in kleinere logische Einheiten. Jede dieser Einheiten erhält üblicherweise einen eigenen Festplatten-Buchstaben. Jede Einheit kann mit einem eigenen Dateisystem formatiert werden, also NTFS, FAT oder FAT32.

Der Grund für die Notwendigkeit einer Partitionierung hat einen historischen Hintergrund. Ältere Systeme konnten mit Festplattenspeichern, die eine gewisse Größe überschritten, nicht richtig oder gar nicht umgehen. Daher musste man Speicher mit einer größeren Kapazität in kleinere logische Bereiche aufteilen.

Da speziell beim Einrichten, Ändern und Löschen von Partitionen ein nicht unerhebliches Risiko von Datenverlust besteht, sollte man die Daten vorher sichern.

Selbst wenn Sie beabsichtigen, bestehende Partitionen nicht zu verändern, sollten Sie das potenzielle Risiko bedenken!

Weiter unterscheidet man zwischen Basis-Laufwerken (Basic Disks) und so genannten dynamischen Laufwerken (Dynamic Disks).

Basic Disks

Basic Disks können in bis zu vier primäre Partitionen oder in drei primäre Partitionen und eine erweiterte Partition unterteilt werden. Eine erweiterte Partition kann wiederum in weitere logische Laufwerke unterteilt werden, eine primäre Partition hingegen nicht.

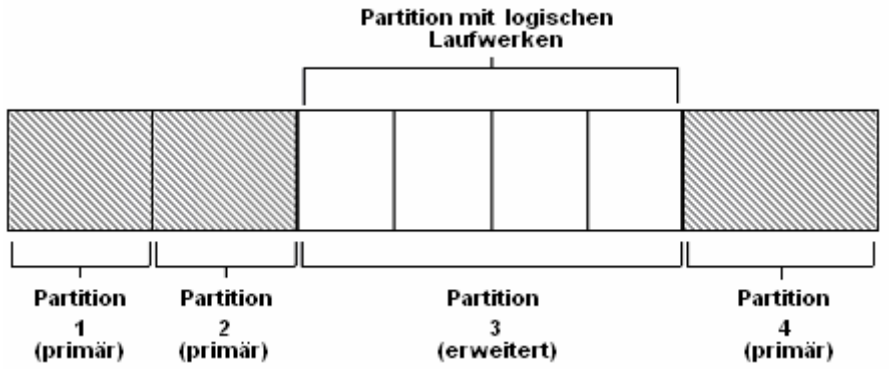


Abb. 5: Basic Disk Schema

Dynamic Disks

Dynamic Disks nutzen ein neues Speicherverfahren, das erstmals mit Windows 2000 eingeführt wurde. Dynamic Disks sind normale Basic Disks, die jedoch mit Hilfe von Windows 2000, Windows XP oder eines Produkts aus der Windows Server 2003-Familie in eben solche dynamische Laufwerke konvertiert wurden.

Dynamic Disks können von einem kompatiblen Betriebssystem aus vergrößert werden, ohne Datenverlust oder Performanceeinbußen befürchten zu müssen. Es ist auch keine neuerliche Installation nötig. Eine Vergrößerung von Basic Disks hingegen ist nur unter bestimmten Umständen möglich (siehe http://support.microsoft.com/kb/325590/de). Erst unter Verwendung von Dynamic Disks ist ein Disk Mirroring unter Windows Server 2003 möglich.

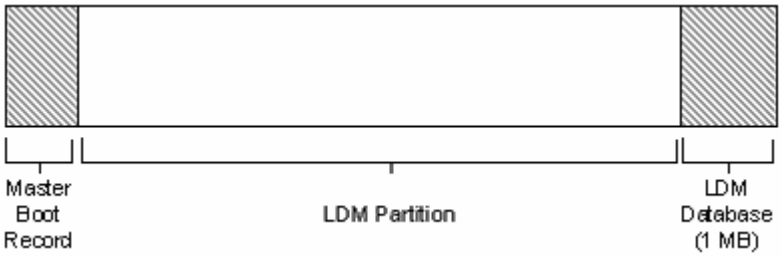


Abb. 6: Dynamic-Disk-Schema

Eine Änderung der Zusammensetzung und Größe ist jedoch nur aus dem laufenden Betriebssystem heraus möglich. Wenn Sie eine Neuinstallation auf einer bestehenden Dynamic Disk beabsichtigen, sind folgende Punkte zu beachten:

- Wenn Sie Windows 2000 oder Windows XP benutzt haben, um eine Dynamic Disk zu erstellen, müssen Sie diese zuerst in eine Basic Disk zurück konvertieren. Dabei gehen jedoch sämtliche Daten verloren. Es ist daher eine Datensicherung erforderlich.
- Sie können für diese Konvertierung Windows 2000 oder Windows XP benutzen. Hinweise und Anleitungen finden Sie in der Hilfe des Betriebssystems.
- Die Konvertierung von einer Dynamic Disk in eine Basic Disk ist außerdem mit Hilfe des Setups für Windows Server 2003 möglich. Dazu wählen Sie im entsprechenden Bildschirm des Setups von Windows Server 2003 aus der Gruppe der verfügbaren Partitionen das dynamische Laufwerk aus. Sie werden aufgefordert, die Umwandlung zu bestätigen. Auch hierbei gehen sämtliche gespeicherten Daten verloren.
- Wenn Sie eine Neuinstallation auf einem Computer beabsichtigen, auf dem bereits ein Produkt der Windows Server 2003-Familie installiert wurde, und der Datenträger des Zielrechners bereits Dynamic Disks enthält, sind ebenfalls spezielle Gegebenheiten zu beachten. Diesbezüglich verweisen wir auf die Informationen über eventuelle Einschränkungen innerhalb des `Hilfe- und Supportcenters`.

Partitionierung während des Setups

Während der Setup-Routine können Sie bestehende Partitionen verändern oder neue Partitionen erstellen, jedoch nur bei einer Neuinstallation. Bei einem Upgrade besteht diese Möglichkeit nicht. Jedoch können Sie die Einteilung der Festplatte nach Abschluss des Setups mit Hilfe des Dienstprogramms DATENTRÄGERVERWALTUNG aus dem Menü VERWALTUNG – COMPUTERVERWALTUNG nachträglich verändern.

ACHTUNG: Während der Setup-Routine sollte bei einer Neuinstallation nur die Systempartition erstellt und mit NTFS formatiert werden. Die Erstellung weiterer Partitionen bzw. die Konvertierung in dynamische Datenträger sollte nach erfolgreicher Installation über das Dienstprogramm **DATENTRÄGERVERWALTUNG** in der MMC-**COMPUTERVERWALTUNG** vorgenommen werden

3.3.10 Dynamische Datenträger

Die im Folgenden beschriebenen Möglichkeiten (RAID-Systeme) sind ausschließlich Softwarelösungen, die mit Windows Server 2003 realisierbar sind. Für diese Softwarelösungen müssen die Festplatten in dynamische Datenträger konvertiert werden. Sollten Hardware-RAID-Systeme verwendet werden, ist diese Konvertierung nicht notwendig

Einfache Datenträger

Einfache Datenträger entsprechen den Partitionen in den älteren Betriebssystemen (Windows NT 4.0, Windows 95, ...). Einfache Datenträger können jederzeit vergrößert werden, wenn sie unter Windows Server 2003 (oder Windows 2000) erstellt wurden. Wenn sie von Basisfestplatten konvertiert wurden, ist diese Vergrößerung jedoch nicht möglich.

Übergreifende Datenträger

Ein übergreifender Datenträger kann Speicherplatz von bis zu 32 physischen Festplatten verwalten. Dieser Datenträgertyp kann jederzeit vergrößert werden, muss jedoch mit NTFS formatiert sein. Nach der Erweiterung eines übergreifenden Datenträgers kann keiner der Bereiche gelöscht werden.

Diese Datenträgerart bietet absolut keine Fehlertoleranz, da sie weder gespiegelt (RAID 1) noch Teil eines RAID 5-Verbunds sein kann.

Stripesetdatenträger – Striped Volume (RAID Level 0)

Diese Datenträger bestehen aus gleich großen Datenstripes, die sich über 32 Festplatten erstrecken können und auf die gleichzeitig geschrieben wird. Mit Stripesetdatenträgern wird daher die größte Schreibgeschwindigkeit erreicht. Ein Stripesetdatenträger kann nach seiner Erstellung nicht mehr in der Größe verändert werden. Er beinhaltet auch keine redundanten Informationen, d. h. wenn eine Festplatte ausfällt, gehen alle Informationen dieses Datenträgers verloren. Diese Variante wurde bisher als „Stripe Set" bezeichnet. In Windows Server 2003 wird diese Variante nun „Striped Volume" genannt.

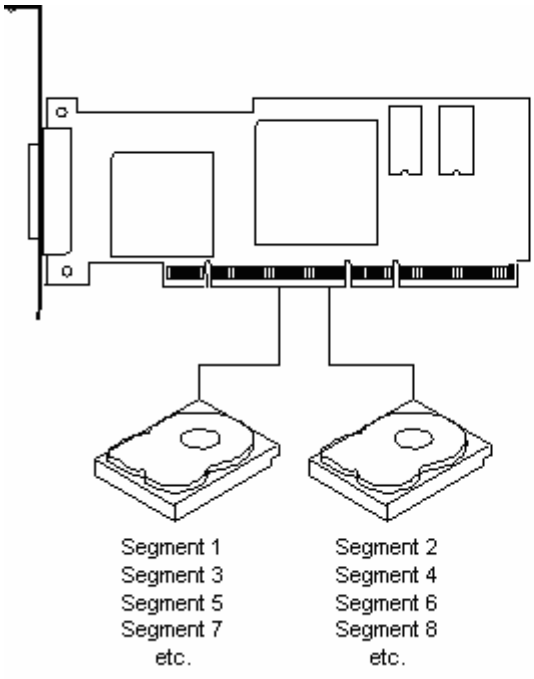


Abb. 7: RAID Level 0 Speicherverbund

Gespiegelte Datenträger (RAID Level 1)

Unter dieser Bezeichnung versteht man die redundante Speicherung von Daten mit Hilfe zweier Festplatten. Dabei werden die Daten auf zwei Festplatten gleichzeitig gespeichert, wodurch ein sehr kostengünstiges redundantes System realisierbar ist.

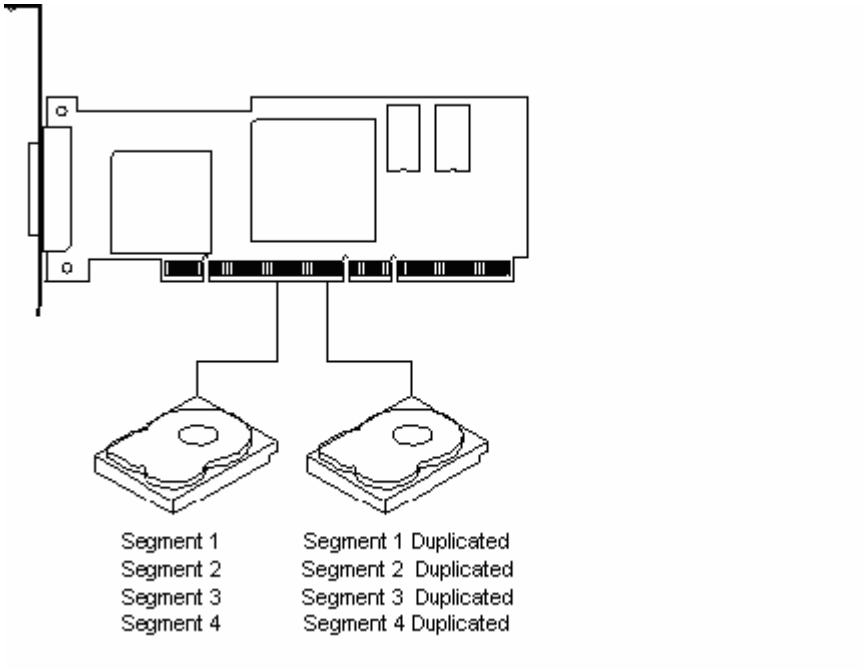


Abb. 8: RAID Level 1 Speicherverbund

Da jedoch die Daten jeweils doppelt gehalten werden, steigt auch der Preis pro Megabyte auf mindestens das Doppelte. Allerdings führt der Defekt oder Ausfall eines Datenträgers zu keinem Datenverlust, da die gespeicherten Daten vom anderen Datenträger wiederhergestellt werden können.

Diese Variante wurde bisher auch als „Mirror Set" bezeichnet. In Windows Server 2003 wird diese Variante nun „Mirrored Volume" genannt.

RAID Level 5 Datenträger:

Bei einem RAID Level 5 System werden die Paritätsdaten auf alle Laufwerke verteilt. Dies vermeidet den Flaschenhals, der bei anderen RAID Level Systemen entstehen kann, da nicht auf ein einziges gemeinsames Laufwerk Korrekturdaten gespeichert werden. Da jedoch bei Lesezugriffen auf ein Laufwerk die Speicherung der Parität auf eben dieses Laufwerk ausgelassen bzw. verschoben wird, sinkt die Gesamtperformance geringfügig unter die Performance anderer RAID-Level-Systeme.

© 2005, Microsoft Österreich GmbH

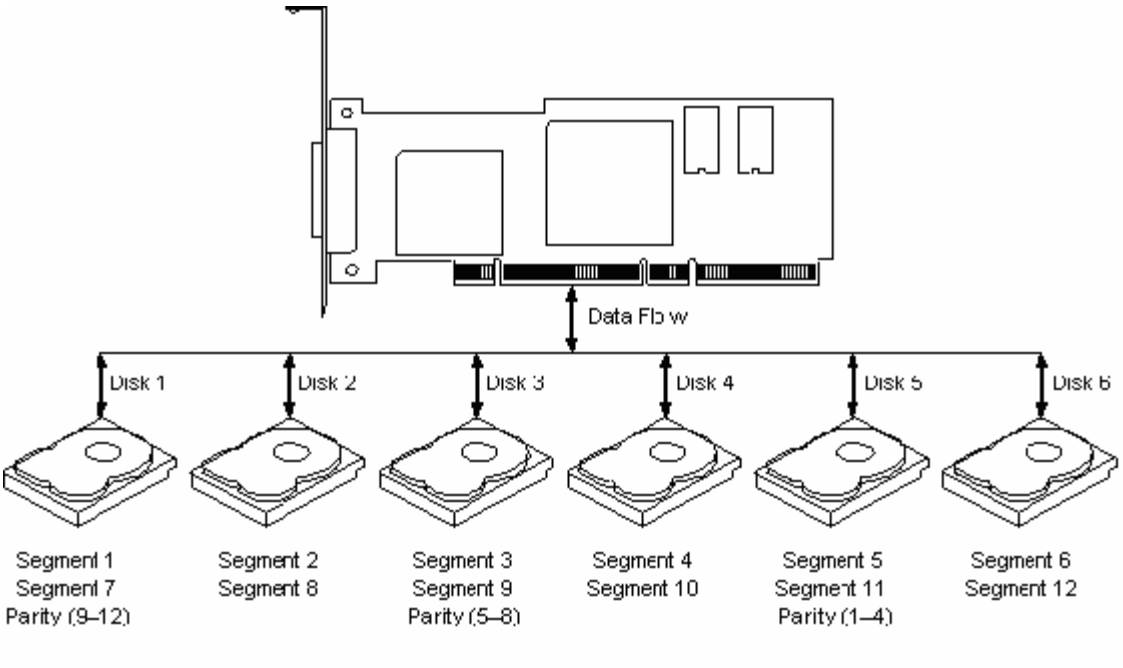


Abb. 9: RAID Level 5 Speicherverbund

RAID Level 10:

Ein RAID Level 10 System ist eine spezielle Kombination der Vorteile eines RAID Level 0 Systems und denen eines RAID Level 1 Systems.

Dabei werden vereinfacht ausgedrückt zwei RAID Level 1 Systeme als einzelne Datenträger angenommen und diese zu einem gemeinsamen RAID Level 0 System zusammengefügt.

Die Vorteile sind eine bestmögliche Fehlertoleranz sowie die enorme Performance eines solchen Systems.

Die Nachteile liegen in den relativ hohen Kosten, da man vom verfügbaren physischen Speicherplatz lediglich die Hälfte effektiv nutzen kann. Der Rest wird zur Spiegelung verwendet.

© 2005, Microsoft Österreich GmbH

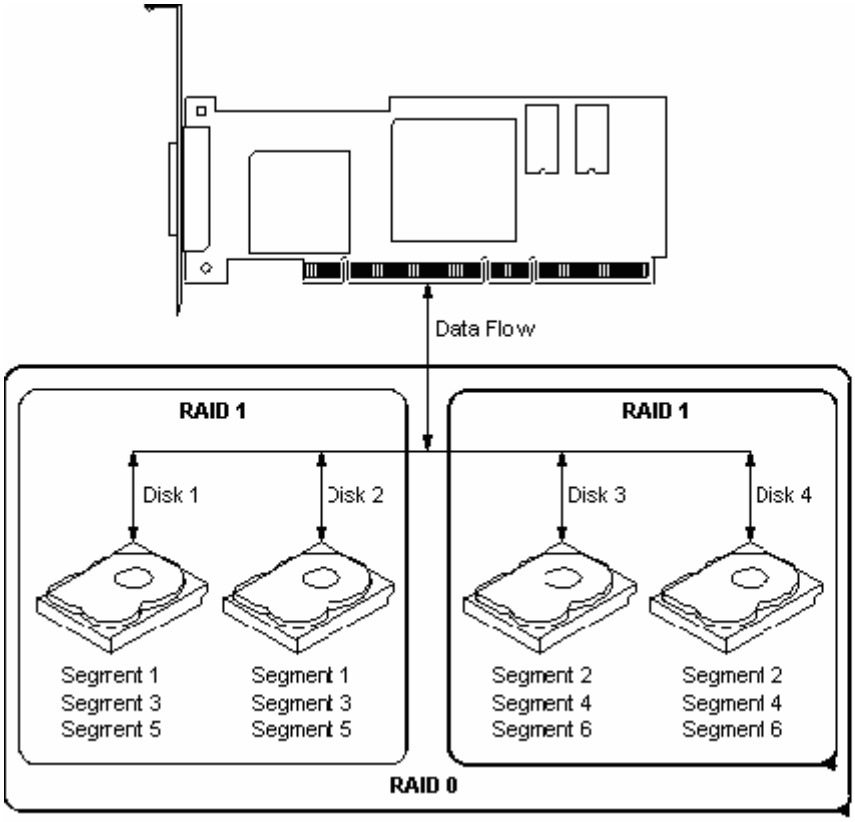


Abb. 10: RAID Level 10 Speicherverbund

3.3.11 Partitionierung für den Schulbetrieb

Empfohlene Aufteilung der Serverplatte für den Schulbetrieb:

Partition 1:

- Zweck: Betriebssystem inkl. der Serveranwendungen
- Dateisystem: NTFS
- Größe: 10 GB

Partition 2:

- Zweck: Homeverzeichnisse
- Dateisystem: NTFS
- Größe: 50 MB pro User; plus einmalig 30 % der Partitionsgröße als Reserve
- Besonderheit: Kontingente aktivieren

Partition 3:

- Zweck: Verzeichnisse für Datenaustausch, Workstation-Images
- Dateisystem: NTFS
- Größe: Verwendung des restlichen Platzes auf der HD
- Besonderheit: Kontingente können aktiviert werden

© 2005, Microsoft Österreich GmbH

Um allerdings auch gegen Datenverlust im Schulbetrieb möglichst gesichert zu sein, ist es empfehlenswert, mindestens zwei Festplatten im Server eingebaut zu haben. Damit ist es möglich, die Spiegelung (RAID 1) zu aktivieren, wie sie in Abbildung 8 dargestellt ist.

Dazu ist es notwendig, dass nach der Installation des Betriebssystems die Basisfestplatten in dynamische Laufwerke konvertiert werden. Anschließend kann die Spiegelung eingerichtet werden.

© 2005, Microsoft Österreich GmbH

4 Netzwerkdienste

In diesem Kapitel erfahren Sie, was eine Domäne ist, wie man sie einrichtet und verwaltet. Dazu gehören auch detaillierte Informationen zu den verwendeten Netzwerkdiensten sowie zur Konfiguration.

4.1 Domänen

4.1.1 Allgemeines

Computernetzwerke sind entwickelt worden, um Ressourcen wie z. B. einen Datenaustausch zwischen den einzelnen Clients zu ermöglichen bzw. gewisse Aufgaben einem leistungsfähigeren Computer – einem Server – zu überlassen.

Dieser Entwicklung gingen verschiedene Netzwerkmodelle voran, über die Sie schon in Kapitel 2 einiges erfahren haben.

4.1.2 Vergleich zwischen Domäne und Arbeitsgruppe

Arbeitsgruppen

Arbeitsgruppe nennen wir eine kleine Anzahl von Rechnern, die in einem Netzwerk ohne einen dedizierten Server zusammengeschlossen sind. Diese können untereinander kommunizieren, Serverfunktionalitäten können von jedem teilnehmenden Rechner übernommen werden.

In einer Arbeitsgruppe ist jeder Nutzer/Teilnehmer gleichberechtigt, da die einzelnen Rechner lokal einzeln verwaltet werden müssen. Eine echte zentrale Steuerung ist nur in einem Domänenmodell vorhanden. Ohne Domäne müssten Benutzer und Kennwörter auf jedem Rechner extra verwaltet werden. Das würde bei einem Kennwortwechsel in einem Netzwerk mit 20 Rechnern etwa bedeuten, dass das Kennwort an 20 Rechnern verändert werden müsste.

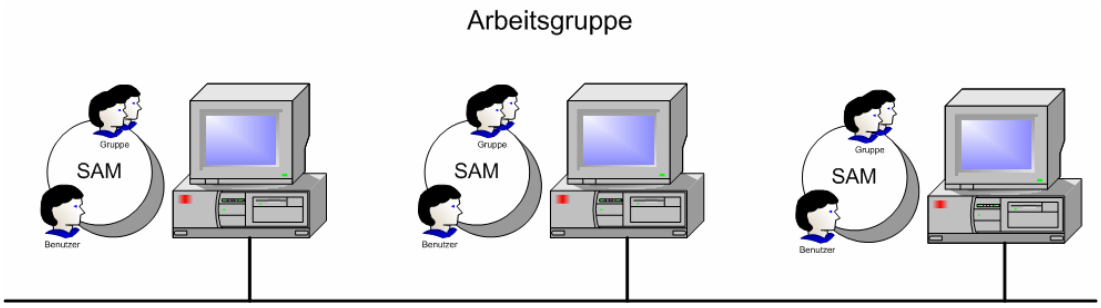


Abb. 11: Arbeitsgruppen

In heterogenen Netzwerken sind mehrere verschiedene Betriebssysteme in einem Netzwerk vorhanden. Dabei kann sich die Implementierung von Arbeitsgruppen jedoch als schwierig erweisen, da der Verwaltungsaufwand um ein Vielfaches gesteigert wird.

Computer, die in Arbeitsgruppen zusammengefasst sind, können zwar gemeinsame Ressourcen teilen, die Administration und Implementierung von Sicherheit gestaltet sich aber relativ schwierig, da jeder einzelne Rechner konfiguriert werden muss.

Arbeitsgruppen eignen sich in den meisten Fällen nur für kleine Heimnetzwerke, da die Rechner hauptsächlich mit Workstationbetriebssystemen (Windows XP Professional, Windows 2000 Professional) betrieben werden.

Vergleichbar sind die Arbeitsgruppen-Netzwerke mit Peer-To-Peer-Netzwerken. In dieser Art von Netzwerk übernimmt jeder Computer gleichzeitig die Rolle des Servers und eines Clients.

Im Normalfall sollten die einzelnen Rechner ein wenig leistungsfähiger sein als normale Desktop-PCs, da die zusätzlichen Serverfunktionalitäten Ressourcen verbrauchen, die normalerweise den Benutzern zur Verfügung stehen.

Ein weiterer Nachteil ist die eingeschränkte Möglichkeit der gleichzeitigen Verbindungen. Damit nicht übermäßig viele Ressourcen des Rechners verbraucht werden, ist bei Windows XP Professional die Zahl der gleichzeitigen Verbindungen auf zehn beschränkt worden.

Windows Server 2003 als Domäne

Mit Hilfe einer Domäne kann ein klassisches Client-Server-Netzwerk eingerichtet werden.

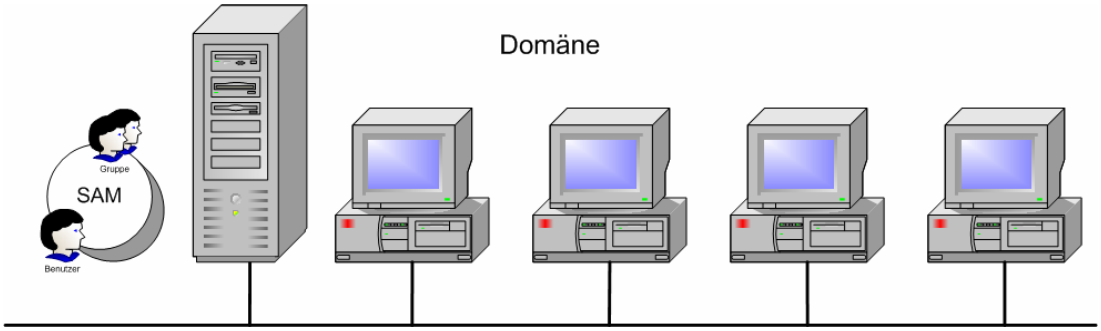


Abb. 12: Windows Server 2003 als Domäne

Domänen übernehmen in einem Windows-Netzwerk bestimmte Rollen und Aufgaben. Sie sind jedoch für folgende primäre Aufgaben konzipiert:

Benutzerauthentifizierung

Ein Benutzerkonto ermöglicht es bestimmten Benutzern, sich in der Domäne anzumelden. Diese Benutzerkonten können entweder an jedem einzelnen Rechner konfiguriert werden (siehe Arbeitsgruppe) oder zentral auf einem speziell konfigurierten Server, der schließlich die Benutzer authentifiziert.

Zugriff auf Ressourcen gewähren bzw. verweigern

Sobald ein Benutzer authentifiziert ist, kann er Ressourcen des Netzwerks nutzen: den Speicherplatz auf einem Server, eine Anwendung oder einen Drucker. Auf der Basis einer Windows Server 2003-Domäne kann der Zugriff für einen Benutzer oder eine Gruppe gewährt oder verweigert werden.

Durch die Einrichtung von Benutzergruppen unter Windows Server 2003 wird die Steuerung des Zugriffs auf Netzwerkressourcen wesentlich erleichtert.

Überwachungsfunktionen

Zusätzlich kann man in einer Domäne bestimmte Überwachungsfunktionen ausführen, damit die Sicherheit in einem Netzwerk gewährleistet wird. So werden im Hintergrund laufend Protokolle mitgeführt, die Informationen über den Netzwerkbetrieb und die installierte Software liefern. Die Konfiguration dieser Dienste kann sogar soweit gehen, dass die Administratoren automatisch benachrichtigt werden, sobald Fehlfunktionen auftreten.

Zusätzliche Serverfunktionen

Die Möglichkeiten, die Windows Server 2003 anbietet, gehen weit über die oben genannten Punkte hinaus. So kann er im Serverbetrieb die Funktion als

- Datei- und Druckserver
- Mailserver

© 2005, Microsoft Österreich GmbH

- Anwendungsserver
- Streaming Media Server
- Web- und FTP-Server
- und viele andere Aufgaben übernehmen.

4.2 Active Directory (AD)

Mit dem Einrichten des Active Directory wird eine zentrale Benutzerverwaltung für Schüler und Lehrer ermöglicht. Seit Windows 2000 hat jeder Active-Directory-Server einer Domäne die gleichen Berechtigungen, so dass es nur noch geringe Unterschiede zwischen den verschiedenen Domänencontrollern gibt. Ein Benutzer, der auf einem Domänencontroller angelegt wird, wird automatisch auf den anderen repliziert und umgekehrt. Dabei wird z. B. ein Kennwort, das ein Schüler auf einem Domänencontroller ändert, auf jeden anderen Domänencontroller übertragen.

Aus den Informationen des Active Directory können für alle Systemressourcen eines Windows Server 2003-Systems Rechte vergeben werden. Benutzern aus dem Active Directory können Administratoren den Zugriff auf Ordner und Dateien erlauben und verweigern, sie können ihnen das Drucken oder sogar die Druckerverwaltung erlauben. Aus den AD-Infos können Exchange-Rechte auf öffentliche Termine, auf Kontakte und vieles mehr abgeleitet werden, sie können die Zugangsrechte für Datenbanken oder über den ISA Server auch den Internetzugang steuern, usw.

In einer Schule sollten zumindest zwei Domänencontroller existieren, damit beim Ausfall eines Domänencontrollers (z. B. durch einen Hardwaredefekt) die Informationen des AD erhalten bleiben.

Die Möglichkeiten des AD sind äußerst umfangreich im Hinblick auf das Zusammenfassen mehrerer Domänen zu Forests, im Schulbereich werden wir im Normalfall mit dem einfachsten Domänenmodell auskommen, einer Domäne mit zwei Domänencontrollern.

Installation einer Domäne mit zwei Domänencontrollern:

- Installieren Sie vorerst 2 Windows Server 2003.
- Anschließend installieren Sie auf dem 1. Server das Active Directory.
- Daraufhin konfigurieren Sie den 2. Server als 2. Domänencontroller in der bestehenden Domäne.

4.2.1 Planungsschritte vor der Installation

Bevor Sie mit der Installation beginnen, müssen Sie sich über Folgendes Gedanken machen:

DNS-Name Ihrer Domäne

z. B. meineschule.at

NetBios-Name Ihrer Domäne

z. B. meineschule

Servernamen

z. B. srv01 und srv02

Der DNS-Name der Domäne sollte mit dem Internet-Domänennamen Ihrer Schule übereinstimmen.

Während der Installation benötigen Sie folgende Informationen:

- IP-Adresse eines externen DNS-Servers (erhältlich beim Internetp-Provider)

© 2005, Microsoft Österreich GmbH

4.2.2 Die Funktion des DNS-Servers im Active Directory

Ein Windows 2000/XP/2003-System bezieht viele Informationen über das Active Directory aus dem DNS Server. Aus diesem Grund ist es zwingend erforderlich, dass in einer Windows 2000/2003-Domäne ein eigener Windows 2000/2003-DNS-Server eingerichtet wird. Ein Domänencontroller ist der Server-Computer

Viele Fehlfunktionen (keine Anwendung von Gruppenrichtlinien, lange Anmeldezeiten) resultieren aus der Fehlkonfiguration, dass der DNS-Eintrag eines Clients nicht auf die IP-Adresse unseres Windows 2000/2003-DNS-Servers zeigt, oder dass kein Windows 2000/2003-DNS-Server implementiert ist.

Windows Server 2003 hilft bei der Installation des Active Directory mit dem „Manage Your Server"-Assistenten, um die unter Windows 2000 häufigsten Fehler zu vermeiden. Trotzdem sollten Sie vor der Installation den DNS-Client-Eintrag überprüfen:

- Wählen Sie START - SYSTEMSTEUERUNG - NETZWERKVERBINDUNGEN
- Rechtsklicken Sie die Netzwerkverbindung
- Wählen Sie EIGENSCHAFTEN

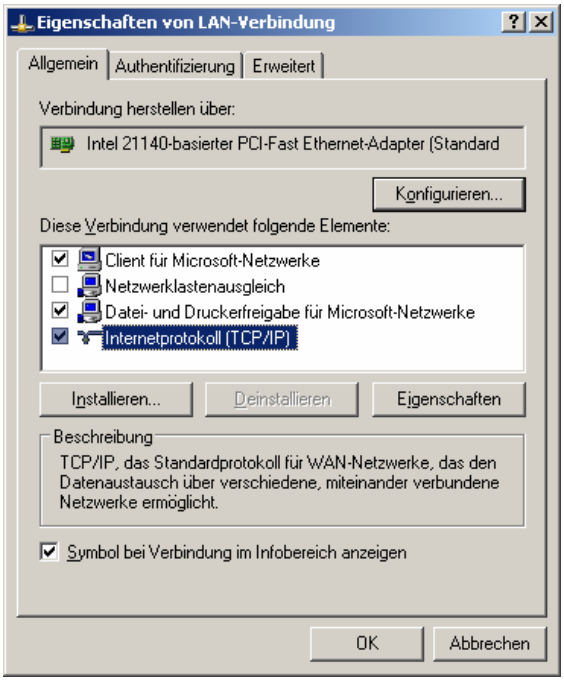


Abb. 13: Eigenschaften von LAN-Verbindungen

- Markieren Sie INTERNETPROTOKOLL
- Wählen Sie EIGENSCHAFTEN

4.2.3 DNS-Eintrag für den 1. Domänencontroller

Für die Installation des 1. Domänencontrollers muss die IP-Adresse unter BEVORZUGTER DNS SERVER mit der IP-Adresse des eigenen Servers übereinstimmen, damit der Active-Directory-Installationsassistent (dcpromo) die Installation und Konfiguration des DNS-Servers automatisch übernimmt.

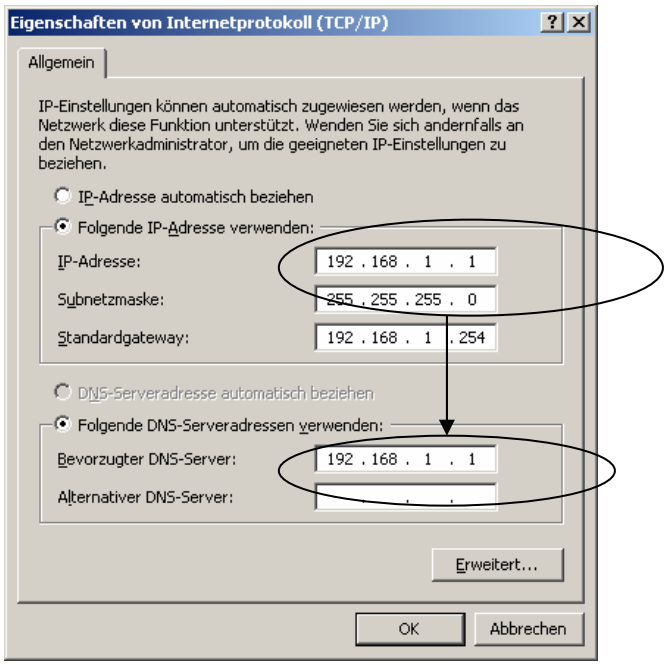


Abb. 14: DNS Eintrag für den 1. Domänencontroller

4.2.4 DNS-Eintrag für den 2. Domänencontroller in einer bestehenden Domäne

Für die Installation des 2. Domänencontrollers muss die IP-Adresse unter BEVORZUGTER DNS SERVER mit der IP-Adresse des 1. Domänencontrollers übereinstimmen, da sich die Informationen über die Domäne und die Domänencontroller im bereits existierenden DNS-Server auf dem 1. Domänencontroller befinden.

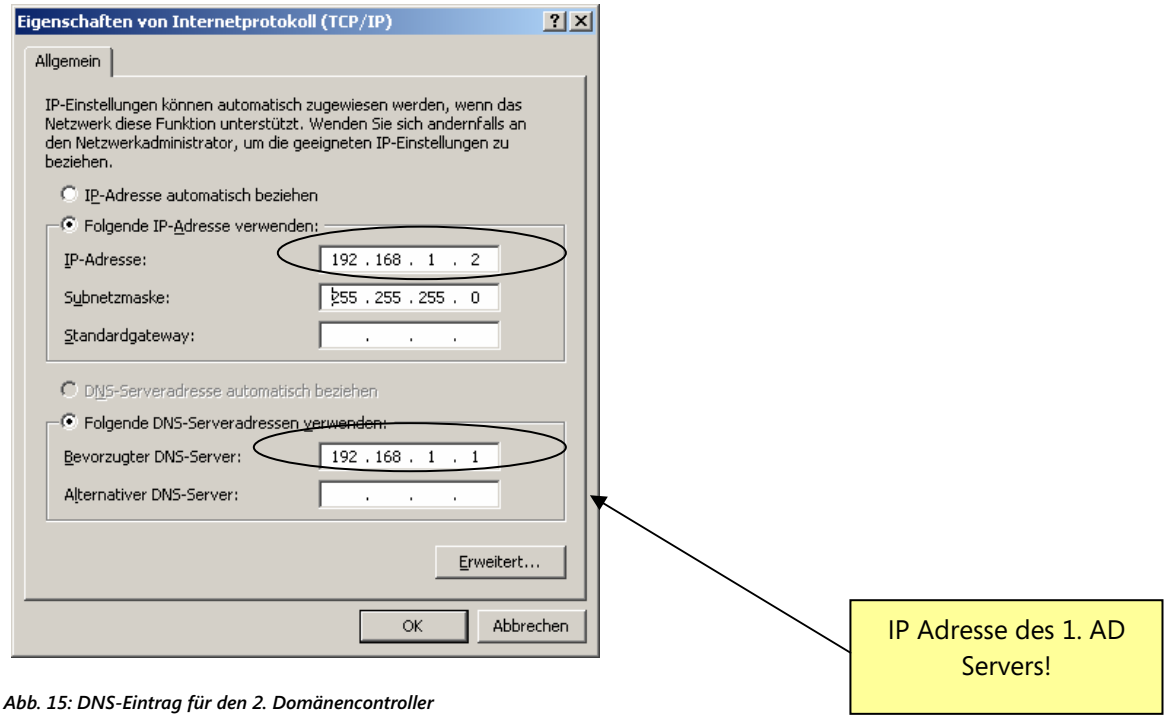


Abb. 15: DNS-Eintrag für den 2. Domänencontroller

4.2.5 Installation des 1. Domänencontrollers der Domäne

- Installieren Sie eine Basisversion von Windows Server 2003 wie im Step by Step Dokument „Schritt 2 Grundinstallation Windows 2003“ beschrieben (downloadbar unter http://www.microsoft.com/austria/education).
- Nachdem Sie Windows Server 2003 installiert haben, melden Sie sich als Administrator an ihrem Server an.
- Falls Sie nach dem Neustart nach der neuen Bildschirmauflösung gefragt werden, stellen Sie diese bitte um.
- Überprüfen Sie den DNS-Client-Eintrag des Servers (DNS-Client = eigene IP-Adresse) wie unter „Wichtige Informationen“ beschrieben.
- Starten Sie DCPromo.
- Wählen Sie START – AUSFÜHREN.
- Tippen Sie ***dcpromo*** ein.
- Klicken Sie auf OK.

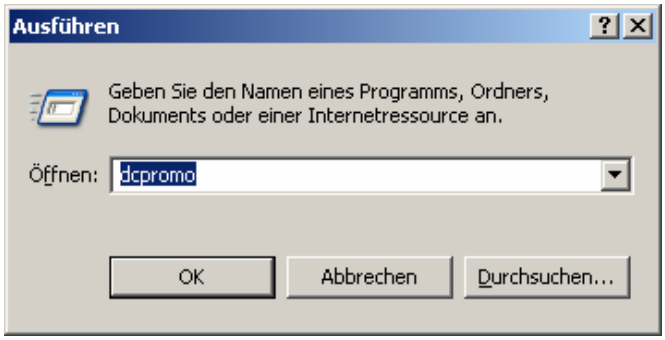


Abb. 16: Aufruf von DCPromo

Abb. 17: Typ des Domänencontrollers

- Klicken Sie auf DOMÄNENCONTROLLER FÜR EINE NEUE DOMÄNE.
- Klicken Sie auf WEITER.

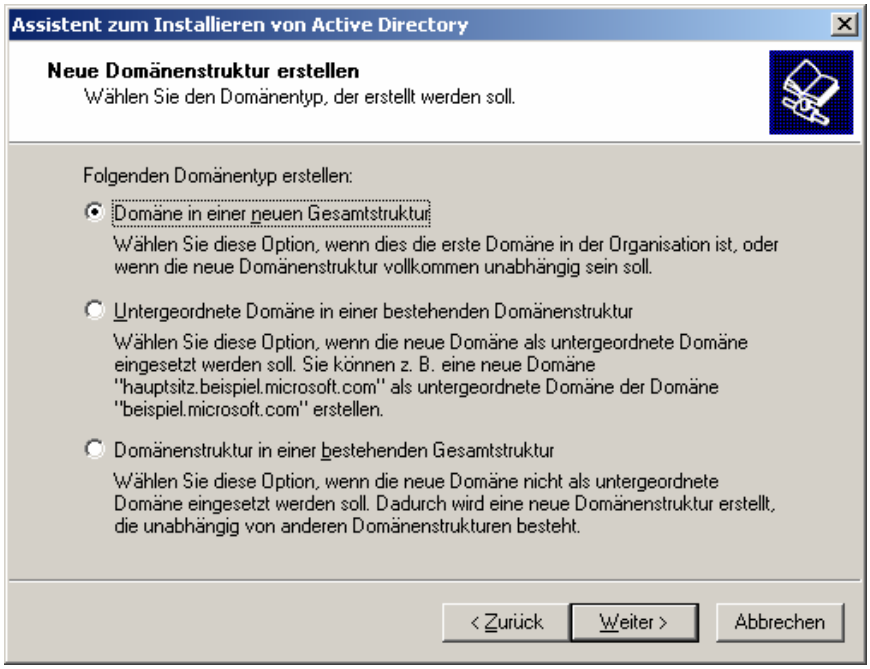


Abb. 18: Erstellung einer neuen Domänenstruktur

- Wählen Sie DOMÄNE IN EINER NEUEN GESAMTSTRUKTUR.
- Klicken Sie auf WEITER.

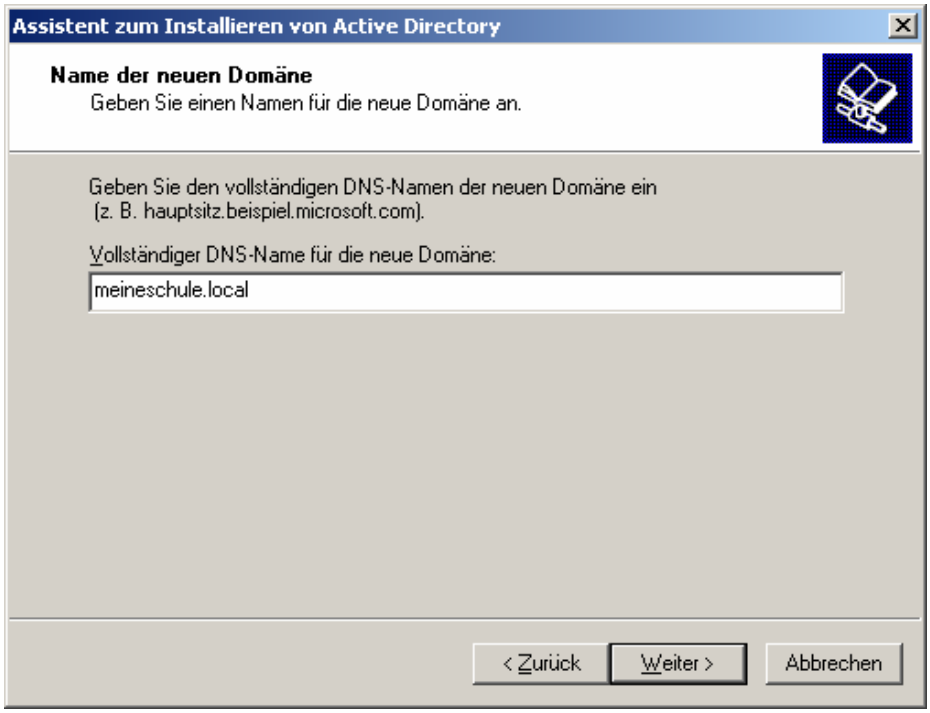


Abb. 19: Benennung der neuen Domäne mit DNS-Namen

- Geben Sie den DNS-Namen Ihrer neuen Domäne (z. B. meineschule.local) ein.

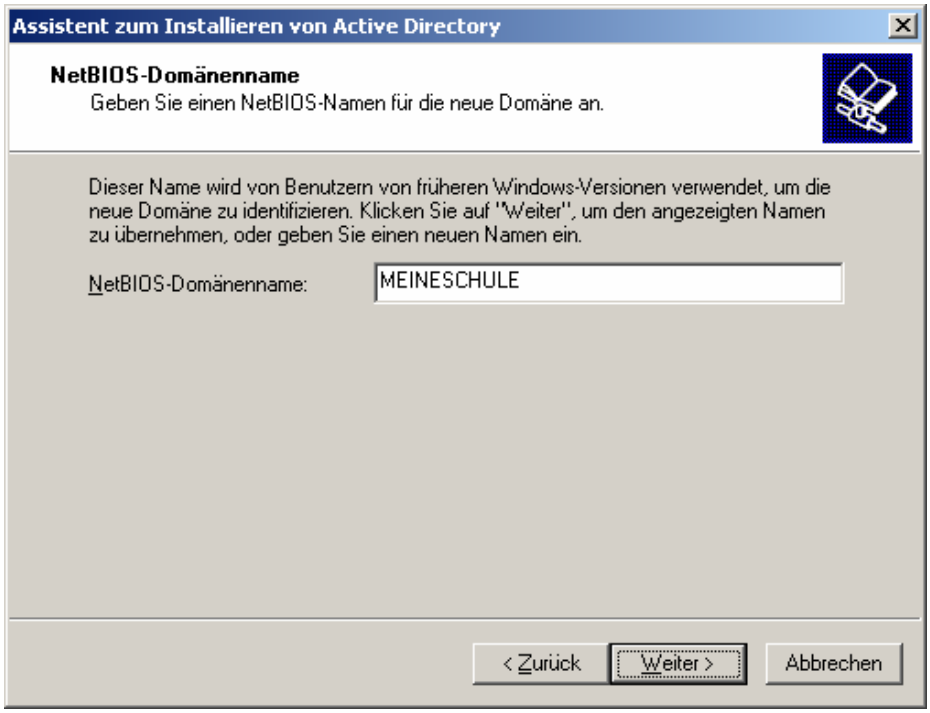


Abb. 20: Benennung der neuen Domäne mit NetBIOS Domänenname

- Nur in begründeten Fällen ändern Sie den NETBIOS-DOMÄNENNAMEN.

- Klicken Sie auf WEITER.

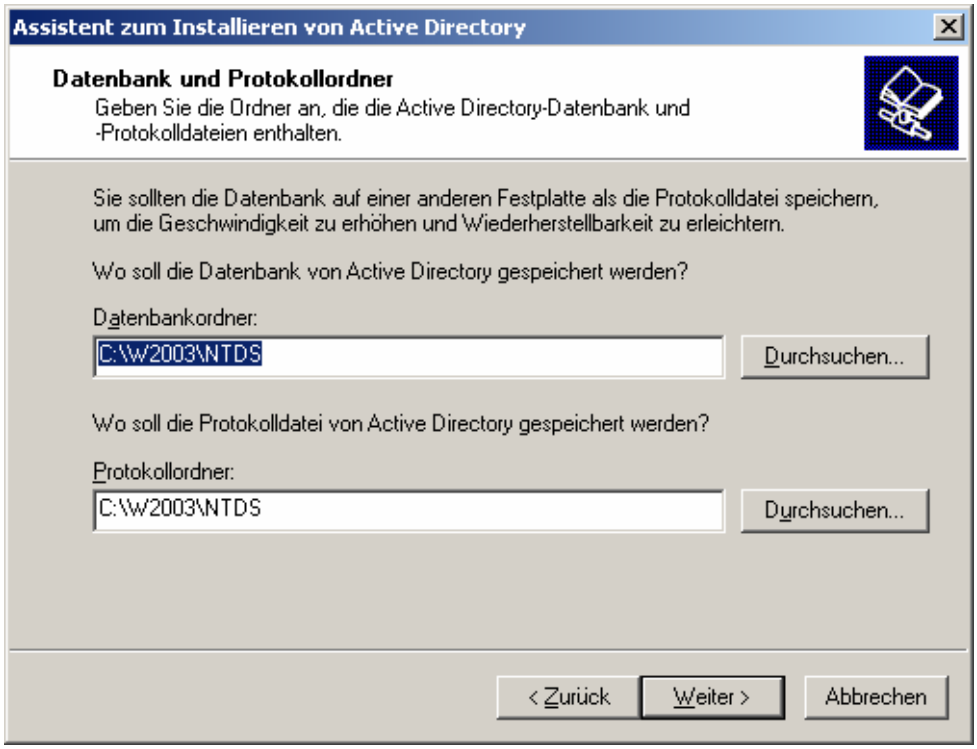


Abb. 21: Angabe des Datenbank- und Protokollordner

- Übernehmen Sie den Vorschlag.
- Klicken Sie auf WEITER.

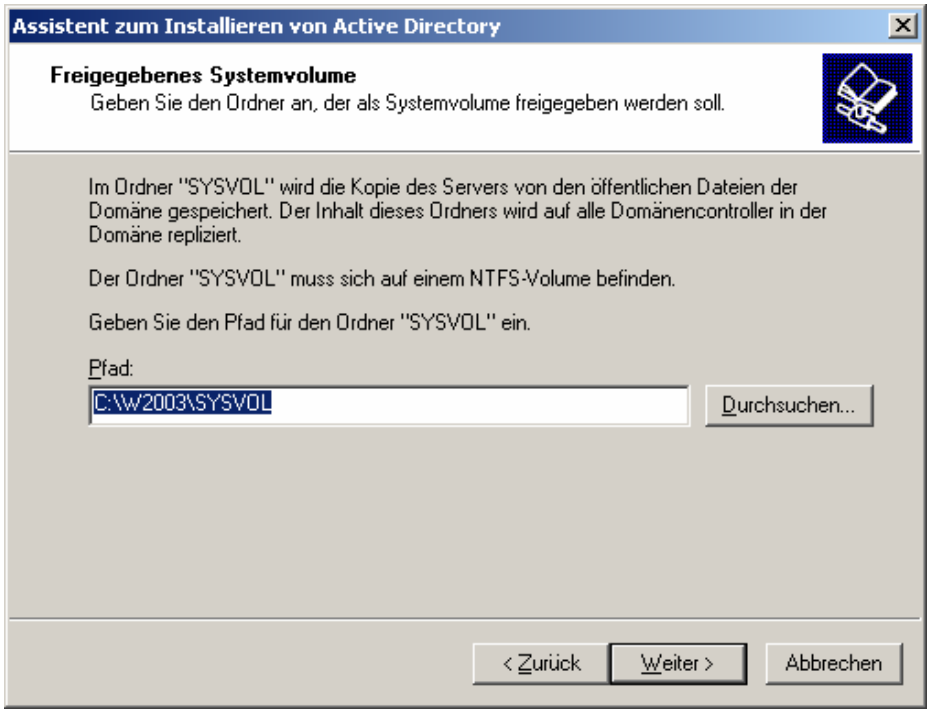


Abb. 22: Angabe des freigegebenen Systemvolumes

- Übernehmen Sie den Vorschlag.
- Klicken Sie auf WEITER.

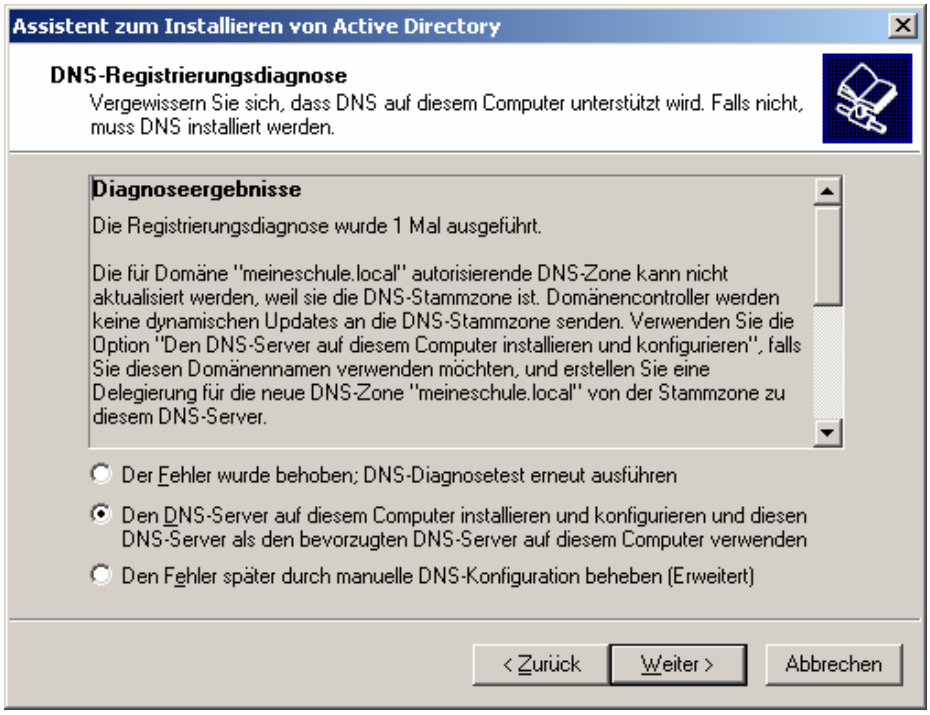


Abb. 23: DNS-Registrierungsdiagnose

- Klicken Sie auf WEITER.

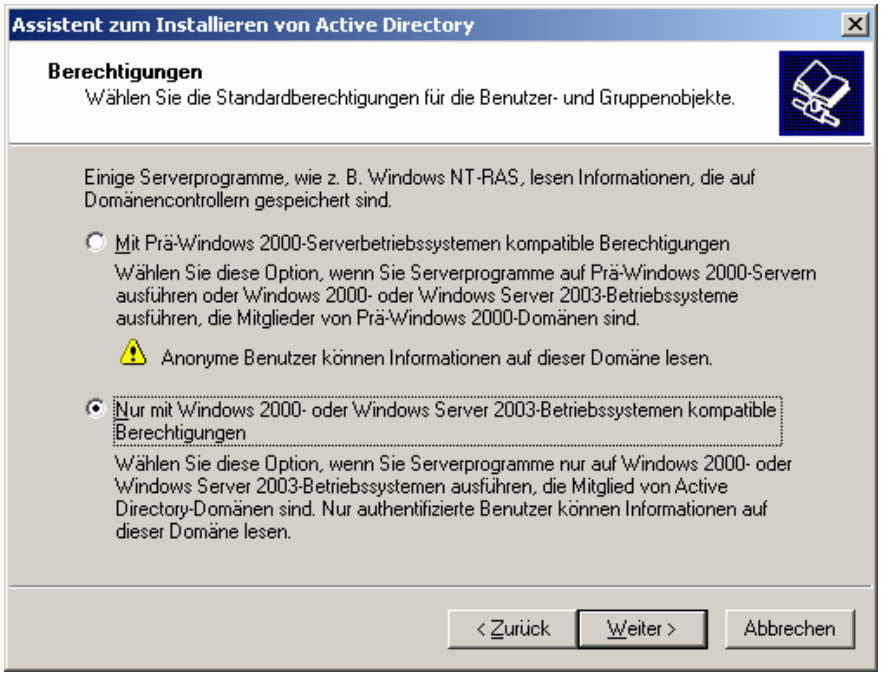


Abb. 24: Vergabe der Berechtigungen

- Da im Schulbereich keine Serveranwendungen verwendet werden, die speziell auf Windows NT4 LanMan Security aufsetzen, wählen Sie NUR MIT WINDOWS 2000- ODER....

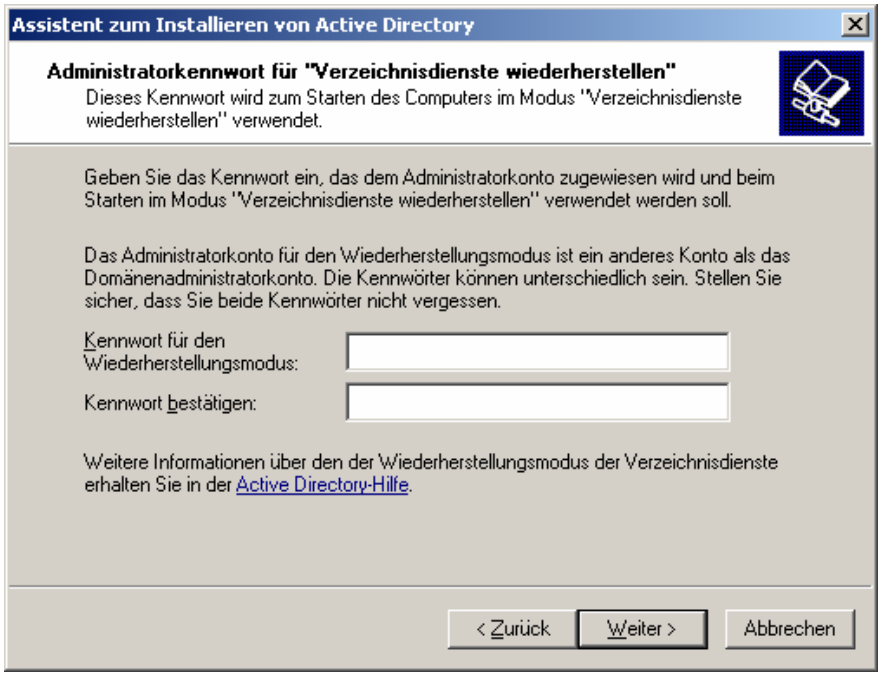


Abb. 25: Vergabe des Administratorkennworts

- Das Kennwort für die Verzeichnisdienstwiederherstellung dient zur Reparatur des Active Directory nach einem Hardwareausfall.
- Wählen Sie ein sicheres Kennwort und bewahren Sie es an einem sicheren Ort auf.
- Klicken Sie auf WEITER.

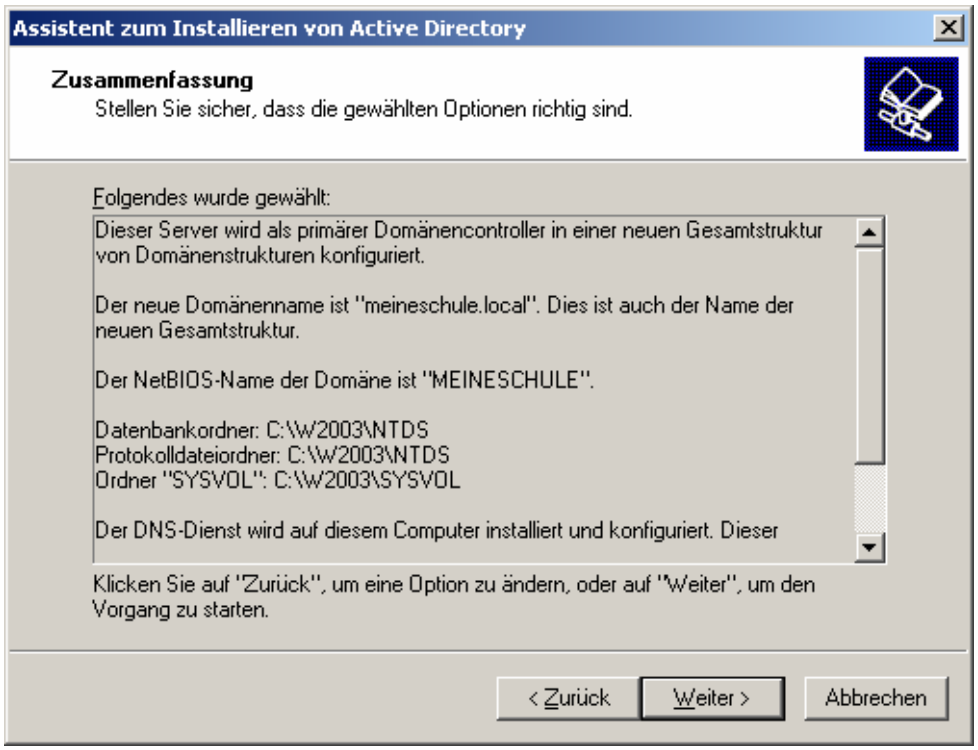


Abb. 26: Abschließende Zusammenfassung

- Die Konfiguration des Active Directory kann einige Minuten dauern.
- Nach dem Neustart ist Ihr 1. Domänencontroller eingerichtet.

4.2.6 Zeitsynchronisation einrichten

Damit die Uhren Ihrer Rechner immer richtig gehen, müssen Sie die Zeit Ihres 1. Domänencontrollers (=PDC Emulator) mit einer Zeitquelle (Zeitserver) übers Internet synchronisieren. Die Synchronisation der Uhren aller anderen Server und Workstations erfolgt dann automatisch.

- Am 1. Domänencontroller wählen Sie START – AUSFÜHREN.
- Geben Sie ***cmd*** ein.
- Klicken Sie auf OK.

Auf der Kommandozeile geben Sie folgenden Befehl ein:

- ***net time /setsntp:time.windows.com***

Abb. 27: Abgleichen der Uhrzeit des Domänencontrollers mit einem Zeitserver

4.2.7 Installation des 2. Domänencontrollers der Domäne

Nachdem Sie Windows Server 2003 installiert haben, melden Sie sich als Administrator an ihrem Server an.

Falls Sie nach dem Neustart nach der neuen Bildschirmauflösung gefragt werden, stellen Sie diese bitte um.

- Überprüfen Sie den DNS-Client-Eintrag des Servers (DNS-Client = IP-Adresse des 1. DNS-Servers) wie unter "Wichtige Informationen" beschrieben.
- Starten Sie DCPromo.
- Wählen Sie START – AUSFÜHREN.
- Tippen Sie ***dcpromo*** ein.
- Klicken Sie auf OK.

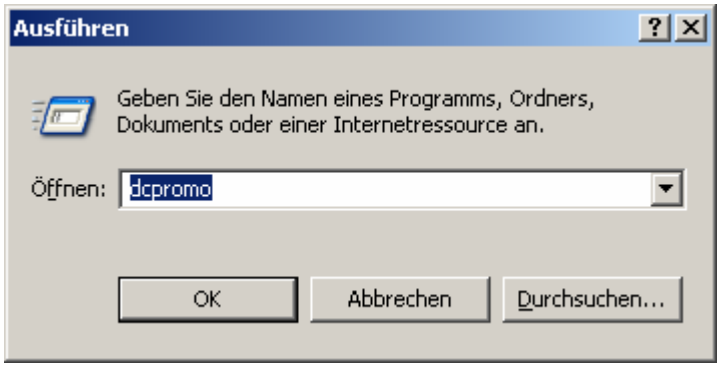


Abb. 28: Aufruf von DCPromo

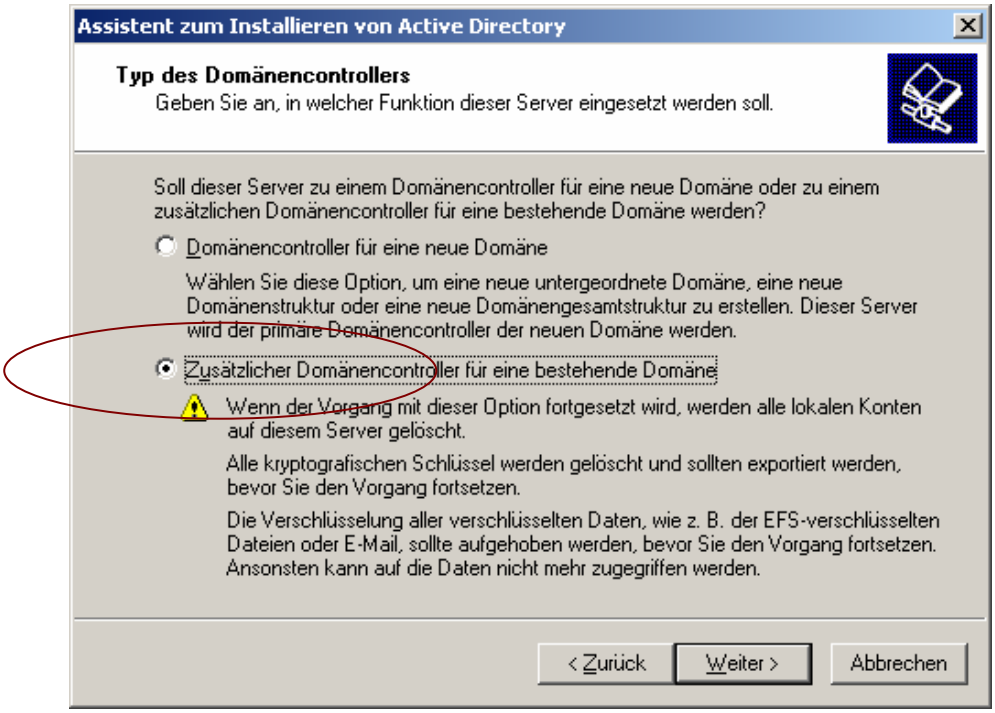


Abb. 29: Auswahl eines zusätzlichen Domänencontrollers für eine bestehende Domäne

- Wählen Sie ZUSÄTZLICHER DOMÄNENCONTROLLER....
- Klicken Sie auf WEITER.

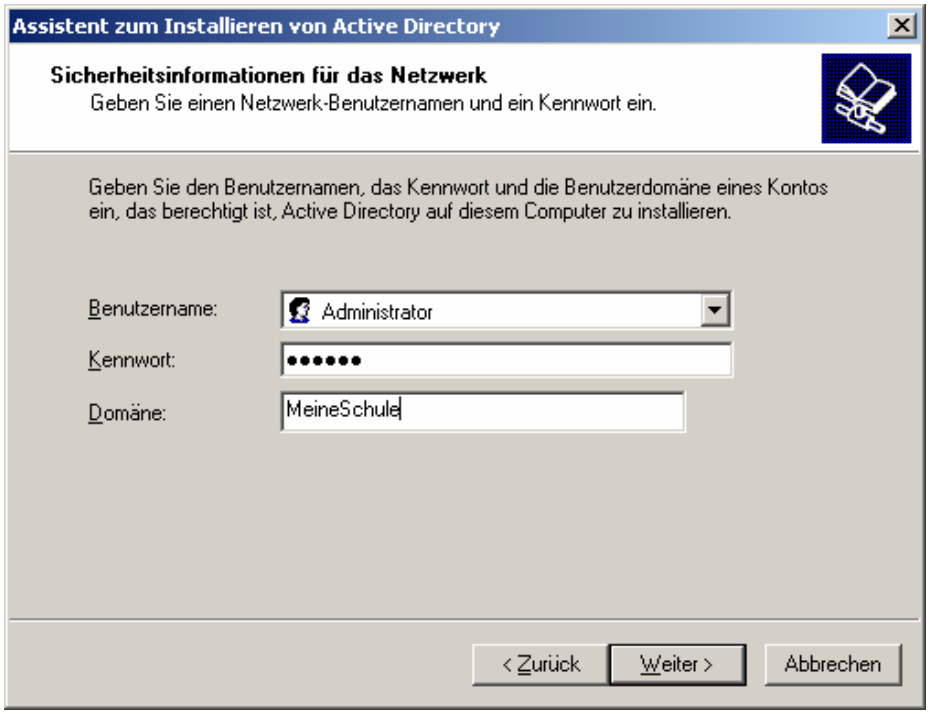


Abb. 30: Eingabe der Sicherheitsinformationen für das Netzwerk

- Geben Sie ein Benutzerkonto mit Administratorenrechten in der bestehenden Domäne ein.

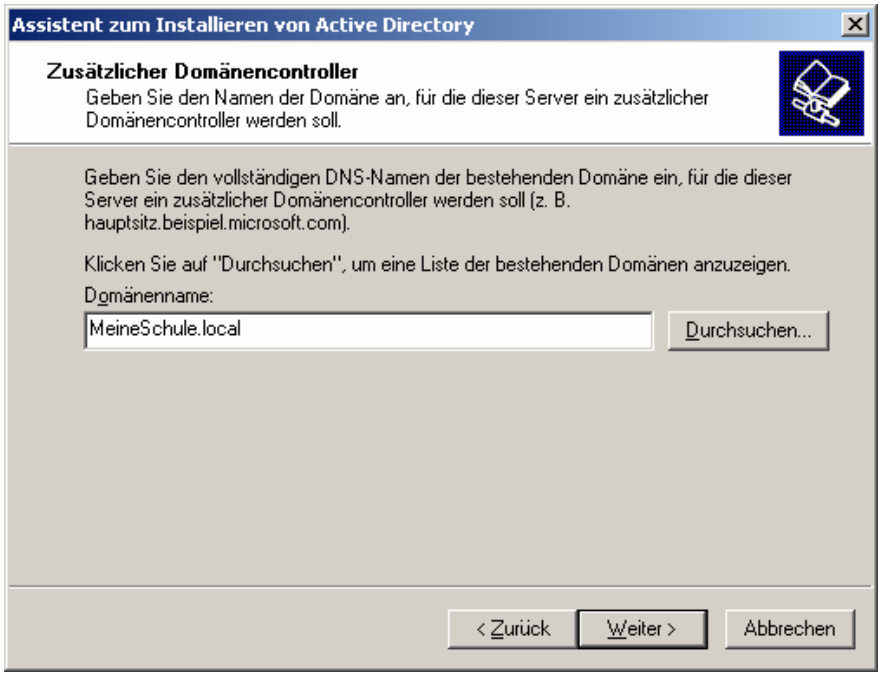


Abb. 31: Erstellung eines zusätzlichen Domänencontrollers

- Geben Sie den DNS-Namen der bestehenden Domäne an.

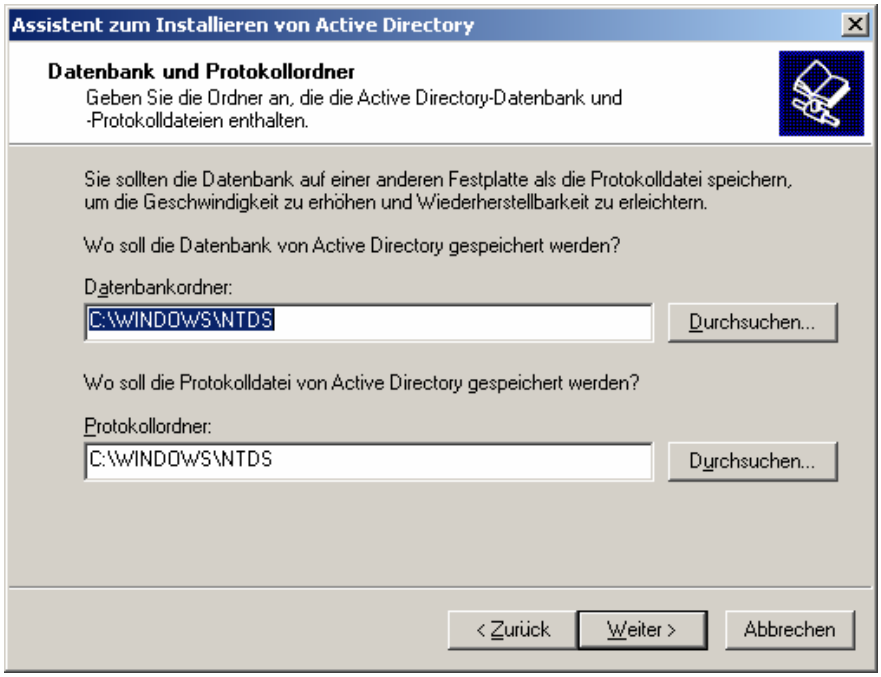


Abb. 32: Angabe des Datenbank- und Protokollordner

- Klicken Sie auf WEITER.

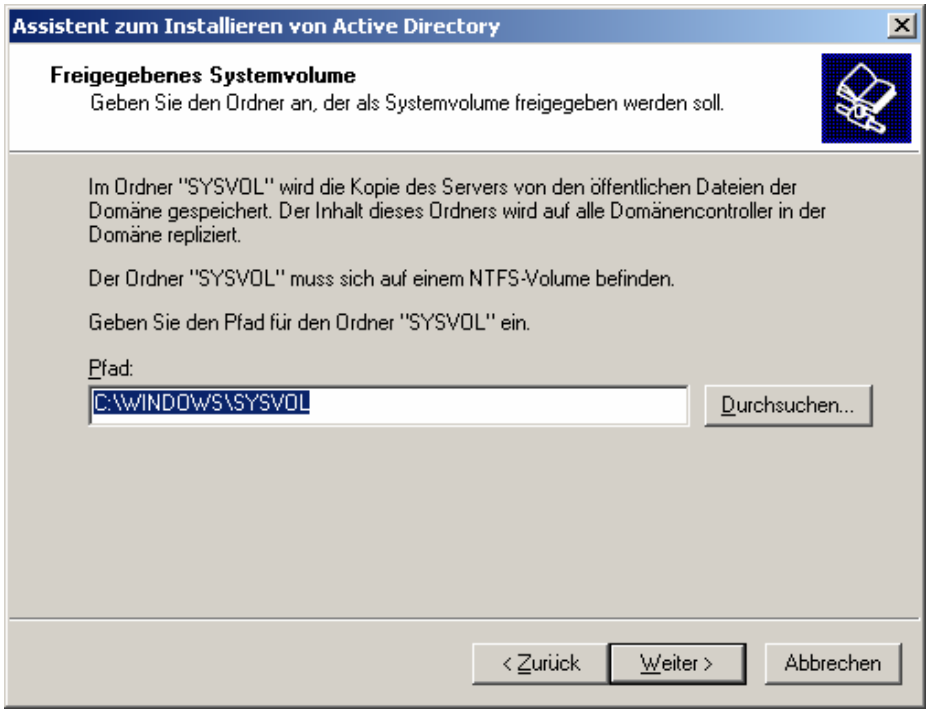


Abb. 33: Angabe des freigegebenen Systemvolumes

- Klicken Sie auf WEITER.

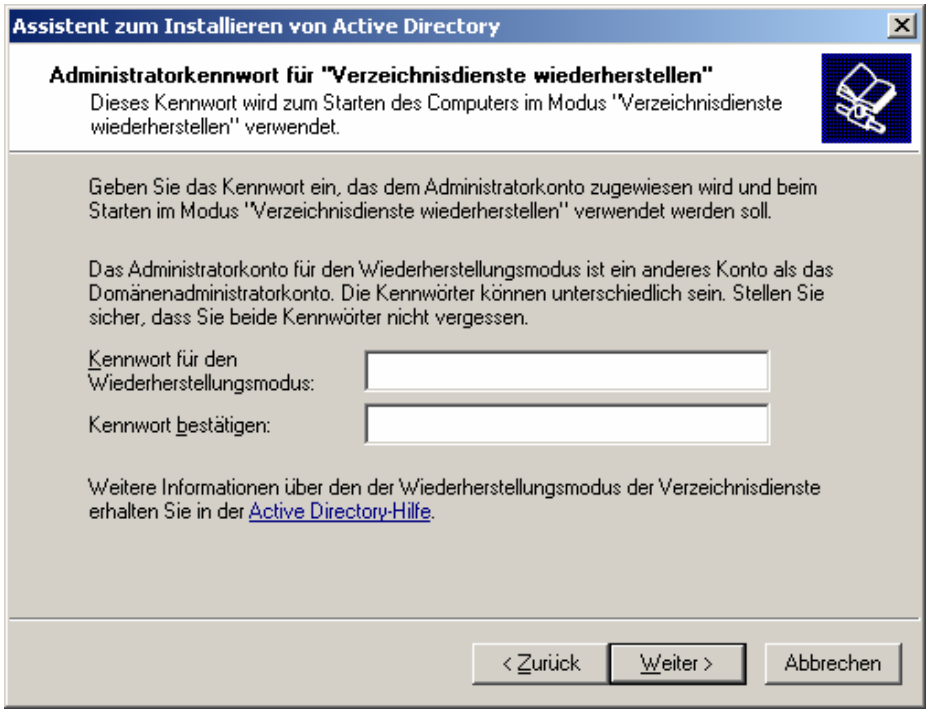


Abb. 34: Vergabe des Administratorkennworts

- Nach dem Neustart ist der 2. Domänencontroller fertig konfiguriert.

4.2.8 Weiterleitungen einrichten

Die Windows 2003-Domäne erfordert einen Windows 2003 DNS-Server. Damit DNS-Anfragen für externe DNS-Namen (z. B. www.microsoft.com) beantwortet werden können, müssen Sie auf allen Windows 2003-DNS-Servern die Weiterleitung einrichten.

- Wählen Sie START - ALLE PROGRAMME – VERWALTUNG - DNS.

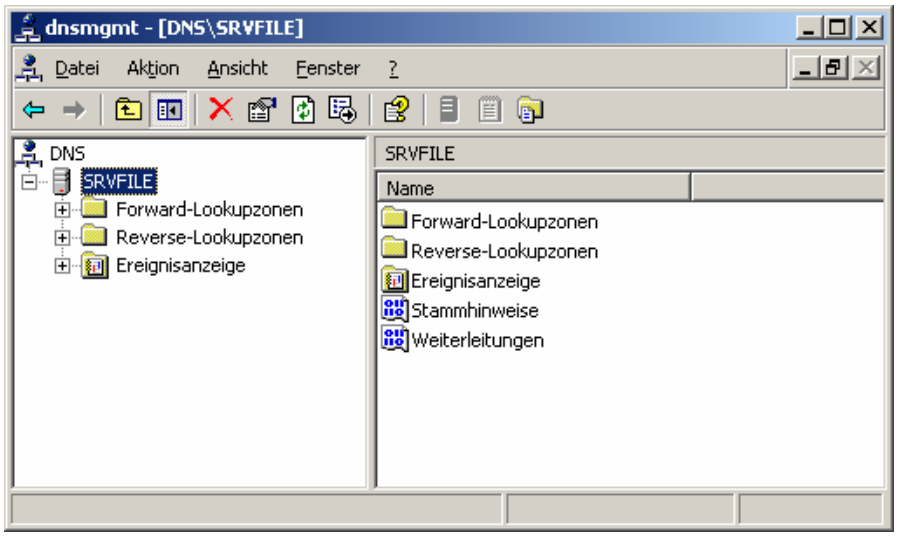


Abb. 35: DNS Management Konsole

- Klicken Sie mit der rechten Maustaste auf den Servernamen.
- Wählen Sie EIGENSCHAFTEN.

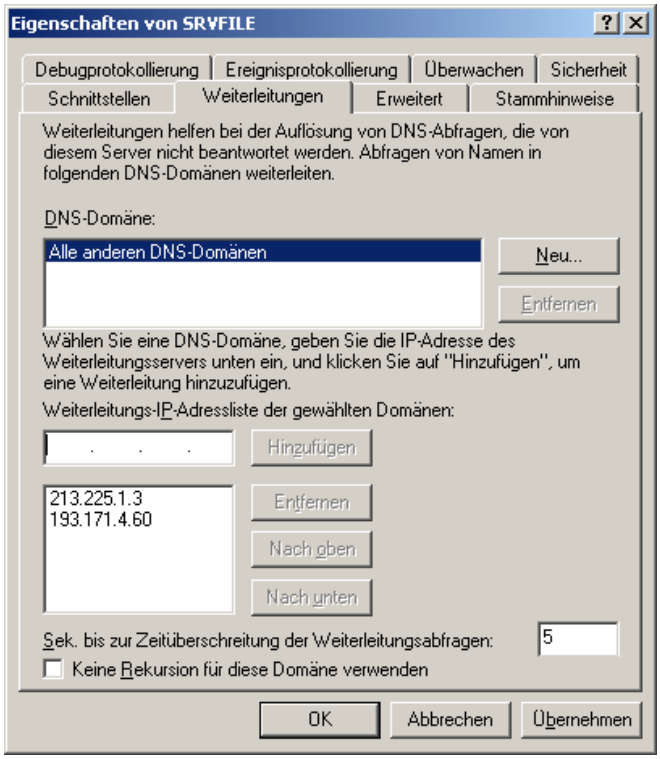


Abb. 36: Eigenschaften des Servers

- Klicken Sie auf die Registerkarte WEITERLEITUNGEN.
- Geben Sie externe DNS-Server ihres ISP ein.

Damit ist die Windows 2000/2003-Domäne richtig konfiguriert und die Clients können die DNS-Namen externer Adressen über die Weiterleitung richtig auflösen.

In einem Netzwerk kommunizieren die Computer über ein Netzwerkprotokoll (TCP/IP) miteinander. Damit die Kommunikation funktioniert, muss jeder Computer eine einzigartige Adresse (IP-Adresse) erhalten. Diese IP-Adresse kann entweder manuell auf jedem Rechner eingegeben oder per DHCP-Server zentral zugewiesen werden.

Die Zuweisung der IP-Adressen per DHCP bringt den Vorteil, dass Änderungen in der IP-Konfiguration (anderer Router, 2. DNS-Server, andere IP-Adressierungsschemas etc.) zentral erledigt werden können.

Ein DHCP-Server verwaltet Pools von IP-Adressen (z. B. 192.168.100.10 bis 192.168.100.200). In einem Netzwerk darf es nur einen einzigen DHCP-Server geben, der diesen Pool verwaltet. Sollte ein zweiter DHCP-Server im Netzwerk auftauchen, so kann es dazu kommen, dass dieselbe IP-Adresse zweimal vergeben wird.

In einem Schulnetzwerk werden im Standardfall folgende IP Konfigurationen zentral verwaltet:

- IP-Adresse
- Subnet Mask
- Default Gateway
- DNS Server
- DNS Domäne

4.3 TCP/IP im Überblick

4.3.1 IP-Adresse

Jeder Computer, der via TCP/IP kommunizieren soll, braucht eine eindeutige IP-Adresse. Diese IP-Adresse besteht aus 4 Bytes (= 4 x 8 Bits, 1 Bit = 0 oder 1). Jedes dieser Bytes kann daher nur Werte zwischen 0 und 255 annehmen.

Beispiele:

192.168.100.210

10.1.1.254

193.171.4.10

4.3.2 Subnetzmaske

Zu jeder IP-Adresse gehört eine Subnetzmaske. Die Subnetzmaske dient lediglich der Teilung der IP-Adresse in zwei Teile.

Beispiel:

IP-Adresse: 192.168.100.210

Subnetzmaske: 255.255.255.0

Wenn wir die Subnetzmaske als Binärzahl umrechnen, so erhalten wir:

Subnetzmaske dezimal	255	255	255	0
Subnetzmaske binär	11111111	11111111	11111111	0

Rechnen wir die IP-Adresse in eine Binärzahl, so erhalten wir:

IP-Adresse dezimal	192	168	100	210
Subnetzmaske binär	11000000	10101000	1100100	11010010

Die Subnetzmaske unterteilt nun die IP-Adresse in zwei Teile, den Netzanteil und den Hostanteil. Alle Bits der IP-Adresse, denen in der zugehörigen Subnetzmaske eine 1 zugeteilt ist, gehören zum Netzanteil. Alle Bits der IP-Adresse, denen eine 0 zugeteilt ist, gehören zum Hostanteil.

Damit Schulrechner in einem Subnetz, also ohne Router, miteinander kommunizieren können, muss der Netzanteil der IP-Adressen der Rechner gleich sein.

Da jede IP-Adresse in unserem Netzwerk eindeutig sein muss, muss daher der Hostanteil der IP-Adressen jedes Rechners unterschiedlich sein.

Beispiele für Subnetzmaske: 255.255.0.0:

die ersten beiden Bytes der IP-Adressen = Netzanteil

die letzten beiden Bytes der IP-Adressen = Hostanteil

Daraus ergibt sich, dass die ersten beiden Bytes der IP-Adressen unserer Rechner gleich sein müssen, die letzten beiden Bytes müssen sich unterscheiden.

→ Mögliche IP-Adressen: 172.1.x.y →

© 2005, Microsoft Österreich GmbH

PC1: **172.1**.1.1

PC2: **172.1**.2.1

PC3: **172.1**.2.2

PC4: **172.1**.3.4

Beispiele für Subnetzmaske: 255.255.255.0

→ Die ersten drei Bytes der IP-Adressen = Netzanteil

das letzte Byte der IP-Adressen = Hostanteil

Daraus ergibt sich, dass die ersten drei Bytes der IP-Adressen unserer Rechner gleich sein müssen, das letzte Byte muss sich unterscheiden.

→ Mögliche IP-Adressen: 192.168.1.x →

PC1: 192.168.1.1

PC2: 192.168.1.2

PC3: 192.168.1.3

PC4: 192.168.1.4

4.3.3 Das Default Gateway (Standardgateway oder Routeradresse)

Zur TCP/IP-Konfiguration eines Rechners gehören drei Parameter:

- IP-Adresse
- Subnetzmaske
- Default Gateway

Das Default Gateway gibt jene IP-Adresse an, an die Datenpakete gesendet werden, deren Ziel IP-Adresse nicht im gleichen IP-Netz liegt. Das bedeutet, dass ein Datenpaket, das von einem Rechner (PC1) an eine IP-Adresse gesendet werden soll, deren Netzanteil mit dem Netzanteil der eigenen IP-Adresse (PC1) nicht übereinstimmt, an den Rechner (oder Router) mit der IP-Adresse des Default Gateway gesendet wird. Der Rechner (oder Router) mit der Default-Gateway-Adresse muss über so genannte Routingtabellen wissen, wie das Datenpaket weitergeleitet werden kann.

Der Netzanteil des Default Gateway muss dem Netzanteil der IP-Adresse entsprechen.

Beispiele für eine konkrete Konfiguration:

IP-Adresse: **192.168.2**.10

Subnetzmaske: 255.255.255.0

Default Gateway: **192.168.2**.254

IP-Adresse: **172.16.**10.2

Subnetzmaske: 255.255.0.0

Default Gateway: **172.16.**22.254

Ein häufiger Fehler in den Konfigurationen liegt darin, dass der Netzanteil des Default Gateway nicht mit dem Netzanteil der IP-Adresse des Rechners übereinstimmt.

4.4 DHCP-Service

4.4.1 Allgemeines

Das Dynamic Host Configuration Protocol ist eine Erweiterung zum BOOTP (Boot Protocol). Das Boot-Protokoll erlaubt es datenträgerlosen Systemen, TCP/IP zu konfigurieren und zu starten.

Mit Hilfe von DHCP werden in einem Netzwerk automatisch Konfigurationsdaten an die Clients gesendet, die diese bei der Initialisierung von TCP/IP anfordern.

Grundsätzlich gibt es in einem Netzwerk zwei Möglichkeiten, TCP/IP auf Clients zu konfigurieren:

Entweder geschieht dies **manuell**, oder durch die **Konfigurationsdaten**, die ein DHCP-Server zur Verfügung stellt.

Bei der manuellen Konfiguration erhält jeder einzelne Client eine willkürliche IP-Adresse, was auf der einen Seite den administrativen Aufwand immens erhöht und auf der anderen Seite eine schwer zu findende Fehlerquelle im Netzwerk sein kann.

Wird z. B. versehentlich eine falsche Subnetzmaske eingegeben, führt dies zu Problemen bei der Kommunikation. Außerdem können IP-Adressen doppelt vergeben werden. Ein weiterer Nachteil ist, dass die Clientrechner jedes Mal manuell umkonfiguriert werden müssen, wenn diese in ein anderes Subnetz gestellt werden.

Die automatische Zuweisung der IP-Adresse durch einen DHCP-Server hingegen vereinfacht die administrative Tätigkeit.

4.4.2 Funktion der automatischen Clientkonfiguration

Die automatische Clientkonfiguration durch den DHCP-Server geschieht folgendermaßen:

Abb. 37: Ablauf der automatischen Clientkonfiguration

1. Leaseerkennung

Zu Beginn initialisiert der Client eine eingeschränkte Version von TCP/IP und sendet eine Rundmeldung (Broadcast), um die Position eines DHCP-Servers und IP-Adressinformationen anzufordern.

2. Leaseangebot

Sämtliche DHCP-Server, die über gültige Adressinformationen verfügen, senden ein Angebot an den Client.

3. Leaseanforderung

Die IP-Adressinformationen aus dem ersten eingehenden Angebot werden übernommen und eine Leaseanforderung an den DHCP-Server geschickt.

4. Leasebestätigung

Der entsprechende DHCP-Server bestätigt das Angebot und alle weiteren DHCP-Server ziehen ihre Angebote zurück.

Das Schicken und Empfangen von DHCP-Meldungen geschieht jeweils über die UDP-Ports 67 und 68.

Bevor Administratoren einen DHCP-Server installieren, sollte abgeklärt werden, ob alle Clients eine dynamische Konfiguration benötigen. Statische IP-Adressen müssen in weiterer Folge bei der Serverkonfiguration ausgeschlossen werden, damit diese nicht erneut zugewiesen werden.

Wenn ein DHCP-Server für mehrere Subnetze verwendet werden soll, dann bedarf es eines DHCP Relay Agents, der die Anforderungen in das andere Netzwerksegment weiterleitet. Ein DHCP Relay Agent nimmt die Leaseerkennung der Clients im Subnetz auf und sendet diese an einen DHCP-Server in einem anderen Subnetz, dieser bearbeitet dann die Anfrage der Clients. Der Relay Agent sollte jedoch auf einem anderen Computer installiert werden, da beide Dienste über dieselben Ports kommunizieren und dementsprechend auf demselben Rechner nicht zuverlässig arbeiten können.

Der DHCP-Server selbst darf nicht über DHCP konfiguriert werden. Er muss eine statische IP-Adresse besitzen und über eine Standard-Gatewayadresse und Subnetzmaske verfügen.

Mit Hilfe von DHCP lassen sich unter anderem folgende IP-Adressoptionen konfigurieren:

- DNS-Server
- Standardgateway
- NetBIOS über TCP/IP-Namensauflösung
- WINS-Server

4.4.3 Anzeige der TCP/IP-Daten eines Clients

So zeigen Sie die Konfigurationsdaten für TCP/IP an:

1. Öffnen Sie die Eingabeaufforderung über START – AUSFÜHREN – CMD.EXE
2. Geben Sie ***ipconfig /all*** ein, um die Konfigurationsdaten aller Schnittstellen anzuzeigen.

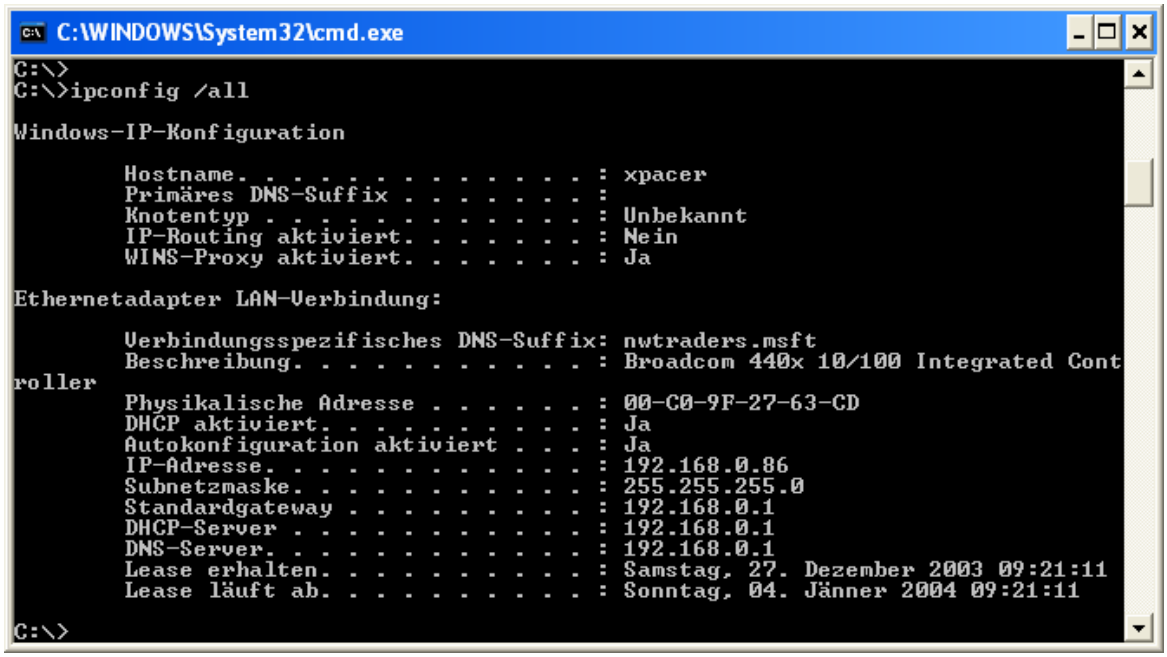


Abb. 38: Konfigurationsdaten der Schnittstellen

Auf DHCP-Clientrechnern können Sie die erneute Zuweisung des IP-Leases durch die Eingabe von `IPCONFIG /RENEW` an der Eingabeaufforderung erzwingen.

4.4.4 Installation eines DHCP-Servers

Ein DHCP-Server wird über die Windows-Komponenten in der Systemsteuerung unter Software installiert.

Wenn Sie die Active-Directory-Dienste in Anspruch nehmen, ist es wichtig, dass der erste DHCP-Server nicht als Einzelplatzserver installiert wird, da alle DHCP-Server Domänencontroller oder Mitgliedsserver sein müssen, bevor Sie im Active Directory autorisiert werden.

4.4.5 Erstellen eines neuen Bereichs

So erstellen Sie einen neuen Bereich:

1. Wählen Sie in der Konsolenstruktur den DHCP-Server aus.
2. Klicken Sie im Menü AKTION auf NEUER BEREICH...

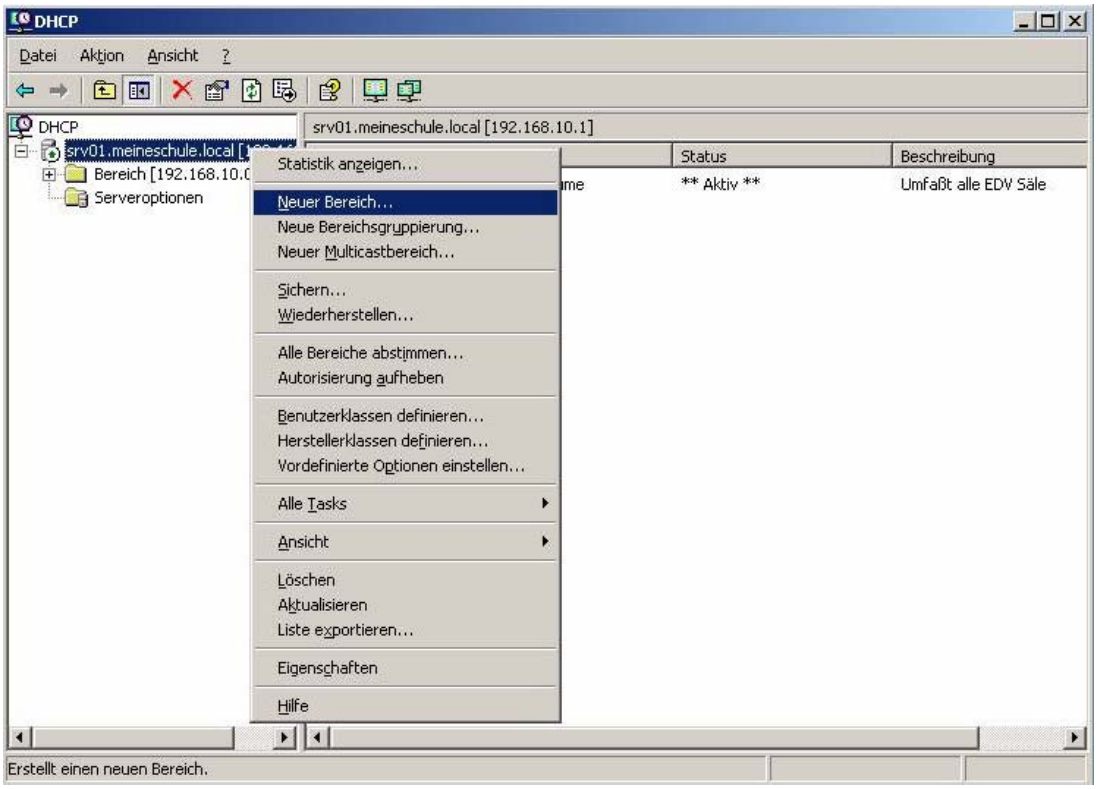


Abb. 39: Erstellen eines neuen DHCP-Bereichs

3. Klicken Sie auf WEITER.
4. Geben Sie einen Namen und eine Beschreibung für den Bereich an und klicken Sie auf WEITER.

Im nun folgen Dialogfenster haben Sie folgende Möglichkeiten:

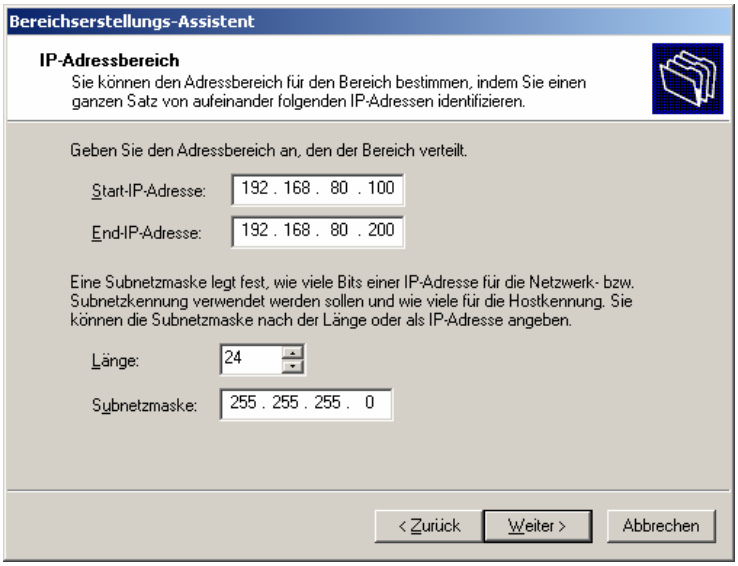


Abb. 40: Vergabe des IP-Adressbereichs

Start-IP-Adresse	Gibt den Anfang des Bereichs an
End-IP-Adresse	Gibt das Ende des Bereichs an
Länge	Hier können Sie Werte zwischen 1 und 31 angeben. Dieser Wert bezeichnet die Bits, die für die Netzwerk- bzw. Hostkennung verwendet werden. Geben Sie hier den Wert 24 für ein Subnetz der Klasse C ein. Letztendlich bestimmt dieser Wert, wie viele Clientcomputer sich in einem Netzwerksegment befinden können.
Subnetzmaske	Wird automatisch aktualisiert, wenn Sie einen Wert bei Länge eingeben.

5. Geben Sie die entsprechenden Werte ein und klicken Sie auf WEITER..
6. Hierauf können bestimmte Adressen angegeben werden, die bei der Vergabe ausgeschlossen sein sollen. Tragen Sie bei Start-IP-Adresse und End-IP-Adresse die entsprechenden Adressen ein und klicken Sie auf HINZUFÜGEN, wenn Sie keine Adressen ausschließen möchten, bzw. die auszuschließenden Bereiche konfiguriert haben.
   Klicken Sie auf WEITER.
7. Nun können Sie die Leasedauer bestimmen.
   Diese Dauer legt fest, wie lange eine vergebene IP-Adresse einem bestimmten Computer zugeordnet bleibt, nachdem dieser wieder vom Netzwerk getrennt wird. Für Netzwerke, die überwiegend aus mobilen Geräten bestehen, ist es sinnvoll, eine kürzere Dauer anzugeben.
   Konfigurieren Sie die Dauer und klicken Sie auf WEITER.
8. Wenn Sie erweiterte DHCP-Optionen konfigurieren möchten, wie zum Beispiel das Standardgateway, DNS-Server und WINS-Server, dann wählen Sie JA, DIESE OPTIONEN JETZT KONFIGURIEREN, und klicken Sie auf WEITER.
9. Geben Sie die Adressen der Standardgateways ein und fügen diese entsprechend mit HINZUFÜGEN zur Liste hinzu. Mit den Buttons NACH OBEN und NACH UNTEN können Sie die Verwendungsreihenfolge bestimmen.
   Klicken Sie auf WEITER.

10. Geben Sie die DNS-Server-Adressen bzw. wenn gewünscht den übergeordneten Domänennamen an, den die Clientcomputer für die Namensauflösung verwenden sollen.
    Klicken Sie auf WEITER.
11. Nun können Sie noch WINS-Server hinzufügen, die dafür verantwortlich sind, NetBIOS-Namen in IP-Adressen umzuwandeln.
    Klicken Sie auf WEITER.
12. Abschließend können Sie aussuchen, ob Sie den Bereich sofort oder später aktivieren möchten.
    Wählen Sie die gewünschte Option und klicken Sie auf WEITER und FERTIGSTELLEN.

Nachdem die Konfiguration mit dem Bereichs-Assistenten abgeschlossen ist, können Sie entweder neue Bereiche hinzufügen, bzw. Detaileinstellungen zu einem Bereich vornehmen.

In der Konsolenstruktur erscheint der nun konfigurierte Bereich unterhalb des DHCP-Servers.

Ein Bereich enthält folgende Punkte:

Adresspool	Enthält die konfigurierten IP-Adressbereiche und die ausgeschlossenen Bereiche.
Adressleases	Eine Liste der bereits an Clients vergebenen IP-Adressen
Reservierungen	Hier werden die Reservierungen für bestimmte Clients angezeigt
Bereichsoptionen	Konfigurieren Sie hier erweiterte Einstellungen, die der DHCP-Server den Clients zuweisen soll.

Mit Hilfe von Reservierungen können Sie sicherstellen, dass ein Client immer dieselbe IP-Adresse bekommt. Dies ist vor allem für Clients wichtig, die im Netzwerk eine Serverfunktion übernehmen.

4.4.6 Autorisierung eine DHCP-Servers im Active Directory

Damit nicht ein unabsichtlich installierter DHCP-Server in einem Netzwerk für Verwirrung sorgt, muss jeder DHCP-Server nach der Installation autorisiert werden.

So autorisieren Sie einen DHCP-Server im Active Directory:

1. Klicken Sie auf START – VERWALTUNG - DHCP.
2. Klicken Sie im Menü AKTIONEN auf AUTORISIERTE SERVER VERWALTEN.
3. Klicken Sie auf AUTORISIEREN.
4. Geben Sie den Namen bzw. die IP-Adresse des zu autorisierenden DHCP-Servers an, und klicken Sie anschließend auf OK.

Nach diesem Schritt wird sichergestellt, dass kein anderer DHCP-Server im Netzwerk eventuell falsche Konfigurationsdaten an die Clients schickt.

4.4.7 Reservierung hinzufügen

So fügen Sie eine Reservierung hinzu:

1. Wählen Sie den Punkt RESERVIERUNGEN.
2. Klicken Sie im Menü AKTION auf NEUE RESERVIERUNG.
3. Geben Sie die Daten für die Reservierung ein und klicken Sie auf HINZUFÜGEN.

© 2005, Microsoft Österreich GmbH

4. Wiederholen Sie die Schritte zwei und drei für jede Reservierung, die Sie vornehmen möchten und klicken abschließend auf SCHLIEßEN.

Die Informationen, die für eine Reservierung nötig sind:

Reservierungsname	Geben Sie hier einen Namen für die Reservierung an.
IP-Adresse	Die IP-Adresse, die für einen Client reserviert werden soll.
MAC-Adresse	Die eindeutige Kennung der Netzwerkschnittstellenkarte. Die MAC (Media Access Control)-Adresse ist eine hexadezimale Kennung im folgenden Format: xx-xx-xx-xx-xx-xx, wobei Sie die Bindestriche nicht eingeben müssen. Sie finden die MAC-Adresse eines Clientcomputers mittels des Befehls ***ipconfig /all*** bzw. ***getmac*** heraus.
Beschreibung	Eine Beschreibung für die Reservierung
Unterstützte Typen	Gibt an, ob nur DHCP- bzw. BOOTP-Clients für diese Reservierung erlaubt werden sollen oder auch beide.

4.4.8 Anzeige der DHCP-Server-Statistik

Damit Sie während des laufenden Betriebs des DHCP-Servers immer überblicken, wie viele Adressen in Verwendung und wie viele noch verfügbar sind, können Sie sich Statistiken anzeigen lassen.

Abb. 41: DHCP-Server-Statistiken

So zeigen Sie die Statistik für einen DHCP-Server an:

1. Wählen Sie den gewünschten DHCP-Server in der Konsolenstruktur.
2. Klicken Sie im Menü AKTION auf STATISTIKEN ANZEIGEN....

Im Kontextmenü eines Bereichs können Sie auch DEAKTIVIEREN wählen, damit die Adressvergabe für einen bestimmten Bereich gestoppt wird.

4.5 DNS (Domain Name System)-Server

4.5.1 Allgemeines

Das Domain Name System (DNS) bietet die Funktion der konventionellen Internet-Namensauflösung und dient in größeren Netzwerken als primärer Namensdienst.

DNS wurde entwickelt, da die Administration mittels der HOSTS-Datei im Laufe der Zeit nicht mehr möglich war, und um die Kommunikationsfähigkeit mit anderen Netzwerken zu gewährleisten. Es handelt sich dabei um eine hierarchische, verteilte und skalierbare Datenbank.

Die Server werden als Namensserver bezeichnet, wohingegen das System auf den Clients durch Auflösungsdienste implementiert wird.

4.5.2 Domänenarten

Die Hierarchie in der DNS-Struktur ist durch verschiedene Domänen – im Sinne von Wertigkeitsbereichen – gegeben:

Stammdomänen

Sie stehen an der obersten Stelle der Hierarchie und werden durch einen Punkt (.) dargestellt.

Topleveldomänen

Beispiele hierfür wären com, org, net, gov, arpa, Länderkürzel, u. v. a.

Topleveldomänen beinhalten entweder Domänen der zweiten Ebene (Second Level Domäne) oder Hosts.

Domänen der zweiten Ebene

Domänen dieser Ebene enthalten entweder weitere untergeordnete Domänen oder Hosts. So kann die Domäne **meineschule.at** weitere untergeordnete Domänen, wie z. B. **abteilung.meineschule.at** enthalten. Diese untergeordnete Domäne kann wiederum Hosts wie **ntserver.abteilung.meineschule.at** enthalten.

Hostnamen

Die Hostnamen werden mit den Domänennamen verwendet, um einen FQDN (Fully Qualified Domain Name) für einen Computer zu erstellen. Ein FQDN ist der Hostname, dem jeweils ein Punkt und der Domänenname nachgestellt wird.

Beispiel: **www.meineschule.at**

„www" stellt den Hostnamen dar, und „meineschule.at" die Domäne.

4.5.3 Zonen

Eine weitere Verwaltungseinheit im DNS-System ist eine Zone.

Die einzelnen Zonen werden separat verwaltet und können entweder aus einer einzigen Domäne oder einer Domäne mit untergeordneten Domänen bestehen. Die untergeordneten Domänen können wiederum in Zonen aufgeteilt sein.

Die Autoritätszonen (Zone of Authority) sind Teil des Domänennamespace, für die ein bestimmter Nameserver zuständig ist. Ein Nameserver speichert alle Adresszuordnungen für den Domänennamespace in einer Zone und beantwortet die Clientanfragen für diese Namen. Die Autoritätszone umfasst mindestens eine Domäne, welche die Stammdomäne der jeweiligen Zone ist.

Damit Datenbankredundanz und ein gewisser Grad an Fehlertoleranz gewährleistet sind, werden mindestens zwei Nameserver benötigt:

© 2005, Microsoft Österreich GmbH

Primärer Nameserver

Dabei handelt es sich um einen DNS-Server, der die Daten für seine Zone lokal abruft. Sämtliche Änderungen der Zonendaten müssen auf dem primären Server vorgenommen werden.

Sekundärer Nameserver

Dieser ruft die Daten mit den Zonendaten des primären DNS-Servers auf, der für diese Zone autorisiert ist. Wenn der primäre Nameserver eine Kopie seiner Zonendatei an den sekundären DNS-Server schickt, spricht man von Zonenübertragung.

Zusätzlich kann es in einem Netzwerk noch Server für die reine Zwischenspeicherung der Abfragen mit den jeweiligen Antworten geben. Prinzipiell wird dies auch von allen anderen DNS-Servern gemacht, jedoch enthalten die DNS-Server für die Zwischenspeicherung keine lokalen Zonendaten.

4.5.4 Die DNS-Namensauflösung

Die Namensauflösung selbst kann auf drei verschiedene Arten geschehen. Der Client-Auflösungsdienst kann auf einem DNS-Server rekursive, iterative und inverse Abfragen ausführen.

Rekursive Abfragen	In einer rekursiven Abfrage kann der Nameserver nicht auf einen anderen Nameserver verweisen. Er muss entweder die Daten oder eine Fehlermeldung zurückliefern, die besagt, dass der Domänenname nicht vorhanden ist.
Iterative Abfragen	Hierbei liefert der Nameserver die beste, momentan verfügbare Antwort zurück. Dies kann entweder der aufgelöste Name sein oder der Verweis auf einen anderen Nameserver, der die Anforderung möglicherweise beantworten kann.
Inverse Abfragen	Wenn es in der DNS-Namespace keinen Zusammenhang zwischen Hostname und IP-Adressen gibt, kann eine Auflösung nur stattfinden, wenn alle Domänen durchsucht werden. Um die Zeit zu verringern, die diese Suche in Anspruch nimmt, wurde eine spezielle Domäne eingeführt, die die Bezeichnung in-addr.arpa trägt. Domänennamen werden von rechts nach links spezifischer, IP-Adressen jedoch von links nach rechts. In der Domäne in-addr.arpa befinden sich spezielle Einträge, in denen die Reihenfolge der einzelnen Oktette einer IP-Adresse umgekehrt sind und die auf die entsprechenden Hostnamen verweisen (Zeigereinträge). Um beispielsweise einen Hostnamen für die IP-Adresse 159.56.202.50 zu ermitteln, fragt der Auflösedienst des Clients den DNS-Server nach dem PTR-Eintrag (Zeigereintrag) für 50.202.56.159.in-addr.arpa ab. Dieser Eintrag enthält den Hostnamen, sowie die IP-Adresse 159.56.202.50. Die Daten werden schließlich dem Auflösedienst zugesandt.

Beispiel für eine rekursive und iterative Abfrage:

1. Der Client-Auflösedienst sendet eine rekursive Abfrage an den lokalen DNS-Server. Dieser ist dafür verantwortlich dem Client eine Antwort zu liefern, darf also nicht auf einen anderen Nameserver verweisen.
2. Der lokale Server prüft seine Zonen, kann aber keine entsprechende Zone finden, die den angeforderten Domänennamen entsprechen. Der DNS-Server schickt schließlich eine iterative Anforderung an den Stammnameserver.

3. Dieser Stammnameserver ist für die Stammdomäne autorisiert und gibt die IP-Adresse eines Nameservers für die Topleveldomäne zurück.
4. Der lokale Nameserver schickt eine iterative Anforderung an den Nameserver der Topleveldomäne.
5. Der Nameserver der Topleveldomäne antwortet mit der Adresse des Nameservers für die untergeordnete Domäne.
6. Der lokale DNS-Server schickt eine iterative Abfrage an den Nameserver der untergeordneten Domäne.
7. Diese antwortet mit der IP-Adresse für die gewünschte Abfrage.
8. Der lokale DNS-Server sendet die IP-Adresse an den Auflösedienst des Clients zurück.

4.5.5 Installation eines DNS-Servers

Beachten Sie, dass beim Installieren von Active Directory der DNS-Server mitinstalliert wird. Die folgenden Schritte sind notwendig, falls Sie Active Directory nicht auf dem Server installieren, bzw. auf einem weiteren Server einen zusätzlichen DNS-Server benötigen.

So installieren Sie einen DNS-Server:

1. Klicken Sie auf START - SYSTEMSTEUERUNG.
2. Klicken Sie auf SOFTWARE und anschließend auf WINDOWS KOMPONENTEN HINZUFÜGEN/ENTFERNEN.
3. Wählen Sie die NETZWERKDIENSTE und klicken auf DETAILS.
4. Aktivieren Sie das Kontrollkästchen DNS-SERVER (DOMÄNE NAME SYSTEM) und klicken Sie auf OK.
5. Klicken Sie auf WEITER.

   Der DNS-Server wird nun installiert. Sie werden eventuell dazu aufgefordert die Windows Server 2003-CD einzulegen.
6. Klicken Sie auf FERTIGSTELLEN.

Es ist empfehlenswert, dass der Server, auf dem Sie einen DNS-Server installieren wollen, über eine statische IP-Adresse verfügt und dass Sie die entsprechenden TCP/IP-Konfigurationsdaten vor der Installation überprüfen, da der Serverdienst automatisch Einträge generiert, die auf den Hostnamen und auf den Domänennamen basieren.

Nachdem der DNS-Server installiert wurde, können Sie diesen konfigurieren.

Die Konfiguration kann sowohl manuell, als auch über eine Managementkonsole erfolgen, die über START – VERWALTUNG – DNS erreichbar ist (siehe weiter unten).

Standardmäßig fungiert ein neu installierter DNS-Server als reiner Cache-Server für das Internet, da er über keine Informationen seines Benutzernetzwerks verfügt.

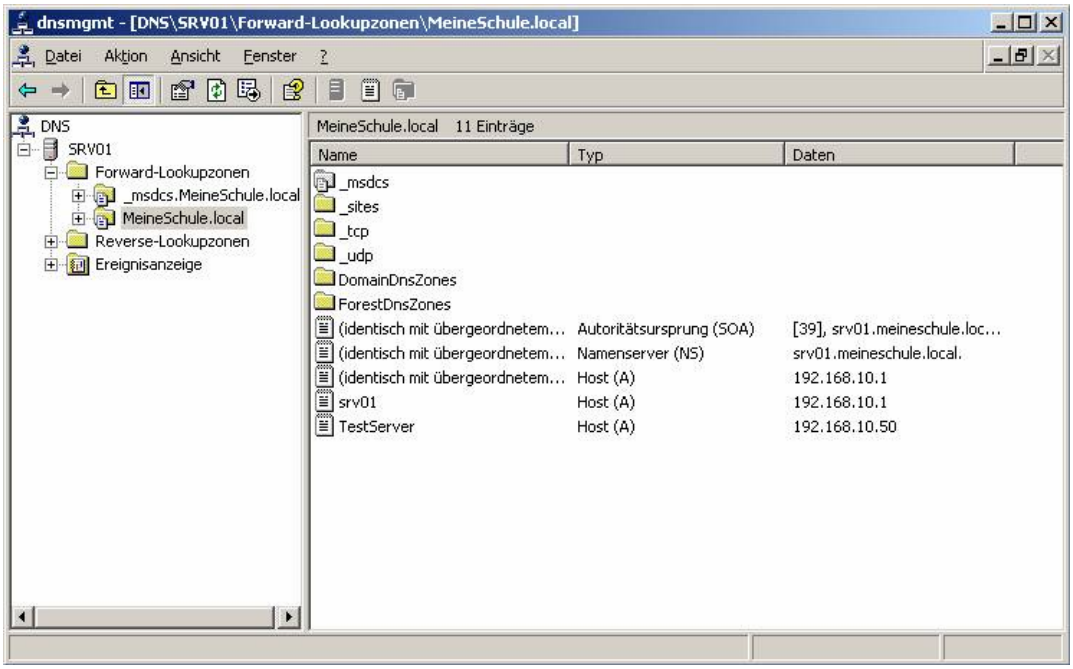


Abb. 42: DNS-Managementkonsole

So konfigurieren Sie einen DNS-Server:

1. Klicken Sie auf START – VERWALTUNG – DNS.
2. Markieren Sie den DNS-Server in der Konsolenstruktur und wählen Sie auf dem Menü AKTION den Punkt DNS-SERVER KONFIGURIEREN... .

   Sie werden auf die DNS-Prüflisten hingewiesen. Diese bieten Informationen aus der Hilfedatei.
3. Klicken Sie auf WEITER. Der Assistent zum Erstellen von Zonen wird aufgerufen.

   Sie können folgende Zonentypen erstellen:

   - FORWARD-LOOKUPZONE: Dies ist vor allem für kleinere Netzwerke empfehlenswert. Nicht-lokale Zuordnungen werden an andere DNS-Server im Internet oder ein anderes Netzwerk weitergeleitet. Es werden keine Reverselookupzonen konfiguriert.
   - FORWARD- UND REVERSE-LOOKUPZONE: Der Server ist für beide Zonen autorisierend, beantwortet rekursive Anfragen und leitet die Anfragen gegebenenfalls an andere DNS-Server weiter.
   - NUR STAMMHINWEISE KONFIGURIEREN: Speziell in einem Netzwerk ohne Internetanschluss müssen Sie die Hinweise auf dem Stammserver ändern, da die vordefinierten Internetstammserver nicht erreichbar sind. Sie können die einzelnen Zonen zu einem späteren Zeitpunkt konfigurieren.
4. Klicken Sie auf WEITER.

   Sie werden jetzt die gewählte Zone konfigurieren (siehe nächste Anleitung).
5. Klicken Sie abschließend auf FERTIGSTELLEN.

Bevor Sie die Zonen konfigurieren, müssen Sie die gewünschte Hierarchie ermitteln, die dann über die DNS-Konsole eingegeben wird.

4.5.6 Forward-Lookupzonen

So konfigurieren Sie eine Forward-Lookupzone:

1. Wählen Sie in der DNS-Konsole den Unterpunkt FORWARD-LOOKUPZONEN.
2. Klicken Sie im Menü AKTION auf NEUE ZONE... .

   Der Assistent zum Erstellen einer neuen Forward-Lookupzone wird gestartet.
3. Klicken Sie auf WEITER.
4. Sie können nun den Typ der Zone auswählen.

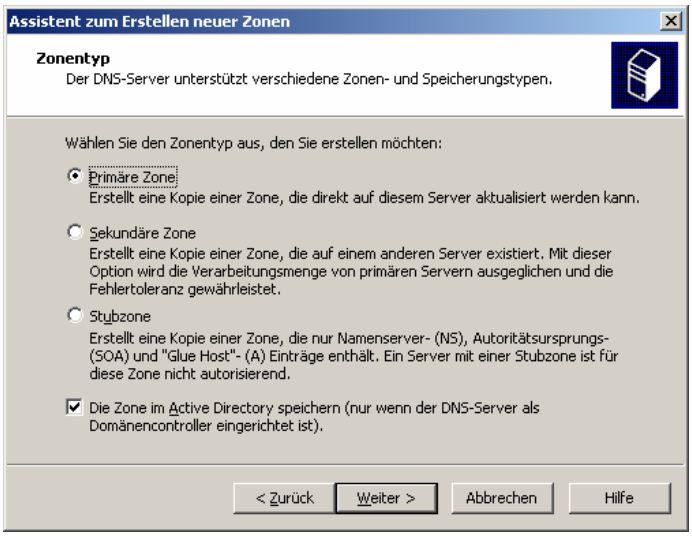


Abb. 43: Auswahl Zonentyp

Dabei gilt:

Primäre Zonen: Werden lokal auf dem Server gespeichert und können direkt aktualisiert werden.

Sekundäre Zonen: Dieser Punkt erstellt eine Kopie einer Zone, die sich auf einem anderen Server befindet. Mit dieser Option gewährleisten Sie einen Lastenausgleich und Fehlertoleranz. Wenn Sie diesen Punkt wählen, müssen Sie bei der Zonenkonfiguration einen Masterserver angeben, von welchem die Zonen kopiert werden.

Stubzone: Erstellt eine Kopie einer Zone, die nur NS- (Nameserver), SOA- (Autoritätsursprung) und A- (Ressourcen) Einträge enthält.

Optional können diese Zonen als Active-Directory-Objekte gespeichert werden. Diese Funktion veranlasst, dass die Zonendateien als Bestandteil der Domänenreplikation repliziert werden.

5. Wählen Sie PRIMÄRE ZONE und klicken auf WEITER.
6. Geben Sie in ZONENNAME den gewünschten Namen ein; z. B.: test.com.
7. Wählen Sie den Namen für eine Datei aus, in der die Einträge gespeichert werden sollen, oder wählen Sie eine vorhandene Datei aus. Diese sind im Verzeichnis %Systemroot%\System32\Dns gespeichert.

8. Wählen Sie DYNAMISCHE UPDATES NICHT ZULASSEN und klicken Sie auf WEITER.
9. Klicken Sie auf FERTIGSTELLEN.

   Unterhalb von Forward-Lookupzonen erscheint nun die neu erstellte Zone.

Die automatisch generierten Einträge in dieser Datei erscheinen in der Detailansicht auf der rechten Seite der Konsole. Dazu gehören ein SOA-Eintrag und ein Nameserver-Eintrag.

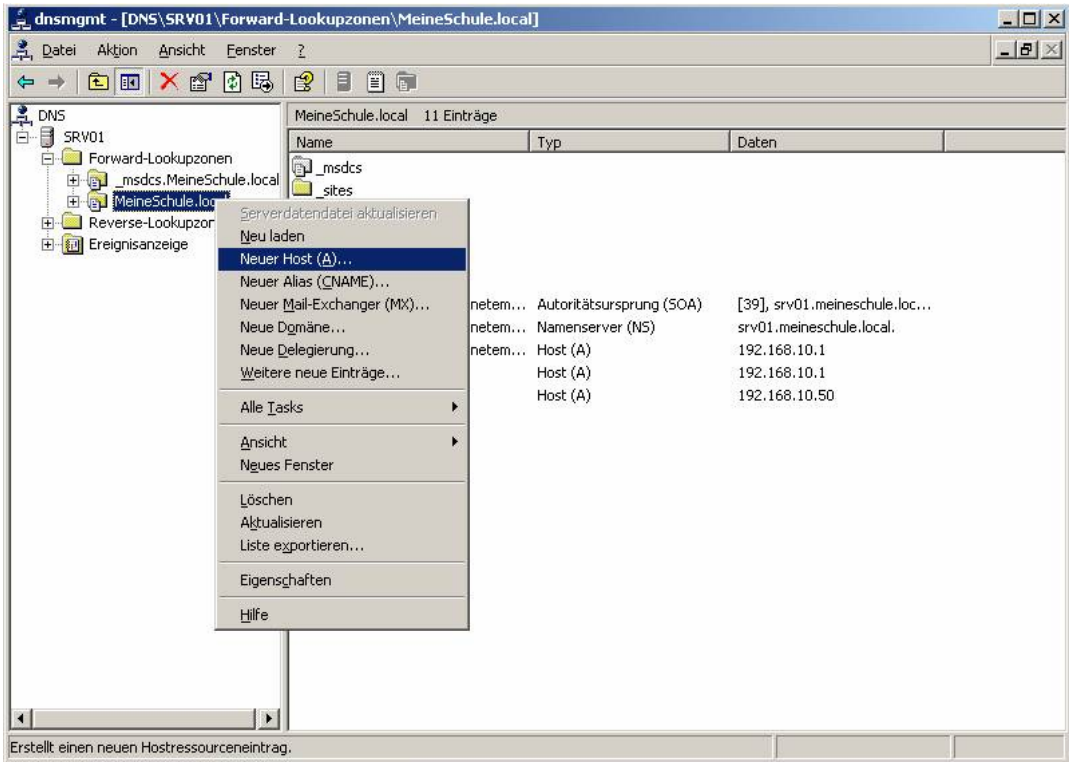


Abb. 44: Neue Einträge für eine Zone erstellen

Sie haben jetzt die Möglichkeit, der Liste Einträge hinzuzufügen:

- Neuen Host (A)
- Neuen Alias (CNAME)
- Neuen Mail-Exchanger (MX)
- Neue Domäne
- Neue Delegierung
- Weitere neue Einträge

Die Assistenten zum Hinzufügen der einzelnen Einträge rufen Sie entweder über das Kontextmenü der Zone oder über das Menü AKTION auf, nachdem Sie die entsprechende Zone ausgewählt haben.

Mit einem Doppelklick auf die Detaileinträge können die dazugehörigen Eigenschaften bearbeitet werden.

Wenn Sie Einträge manuell im Dateisystem ändern, sollten Sie die Ansicht über das Menü AKTION - AKTUALISIEREN bzw. NEU LADEN einstellen.

Um die Zoneneigenschaften zu bearbeiten, bzw. die Zonenübertragungen zu konfigurieren, wählen Sie die Zone aus und klicken im Menü AKTION auf EIGENSCHAFTEN.

4.5.7 Einen Host hinzufügen

So erstellen Sie einen neuen Host Eintrag:

1. Klicken Sie auf START – VERWALTUNG - DNS.
2. Wählen Sie die gewünschte Zone, in der Sie den Eintrag erstellen möchten, in der Konsolenstruktur.
3. Wählen Sie im Menü AKTION den Punkt NEUER HOST (A) . . . .
4. Geben Sie im Feld Name den gewünschten Namen ein (z. B.: www)
5. Schreiben Sie die dazugehörige IP-Adresse in das entsprechende Feld.
6. Die Option VERKNÜPFTEN PTR-EINTRAG ERSTELLEN wählen Sie, um einen solchen Eintrag zu generieren (genaue Beschreibung siehe Anleitung zum Konfigurieren von Reverse-Lookupzonen weiter unten).
7. Klicken Sie auf HOST HINZUFÜGEN.

4.5.8 Testen der DNS-Konfiguration

Hierauf können Sie die Konfiguration mit dem Kommandozeilentool NSLOOKUP überprüfen.

So testen Sie die DNS-Konfiguration mittels nslookup:

1. Klicken Sie auf START – AUSFÜHREN.
2. Geben Sie bei Öffnen den Befehl ***cmd*** ein.

   Hierauf wird die Eingabeaufforderung angezeigt.
3. Geben Sie den Befehl ***nslookup <gesuchter Computer>*** ein.
   z. B.: nslookup www.test.com
4. Schließen Sie die Eingabeaufforderung.

nslookup hat auch einen interaktiven Modus integriert. Geben Sie hierfür in der Eingabeaufforderung nur ***nslookup*** ein. Der interaktive Modus bietet mehr Informationen zum DNS-Server an. Beenden Sie diesen Modus mit dem Befehl ***exit***.

Um den Hostnamen mittels einer IP-Adresse des Hosts zu ermitteln, muss für jedes Netzwerk eine Reverse-Lookupzone erstellt werden. Im Prinzip funktioniert die Erstellung der Zone wie bei den anderen Zonentypen. Der einzige Unterschied befindet sich im Namen der Zone.

Ein Host mit der Adresse 195.241.26.67 wird in der Domäne in-addr.arpa als 67.26.241.195.in-addr.arpa dargestellt. Damit dieser Host von einem Client mit dieser IP-Adresse erkannt werden kann, muss dem DNS für 26.241.195.in-addr.arpa eine

Zone hinzugefügt werden. Alle PTR-Einträge für das Netzwerk 195.241.26.0 würden dieser Reverse-Lookupzone hinzugefügt werden.

4.6 Routing und RAS (Remote Access Service)

4.6.1 Allgemeines

Das Routing und der Remote Access Service werden in einem Netzwerk benötigt um Verbindungen zu anderen Netzwerken zu ermöglichen.

Unter Windows Server 2003 können Sie mit Routing und RAS folgende Aufgaben bewältigen:

- Verbinden von LAN-Segmenten (Subnetzen) in einem Netzwerk
- Verbinden von Intranets, die sich an verschiedenen Standorten befinden
- Bereitstellen des Zugriffs auf eigene Netzwerkressourcen für Remotecomputer

Damit all dies ermöglicht wird, benötigen Sie einen Router. Ein Router ist ein Gerät, das die Fähigkeit besitzt, Pakete zwischen Teilen eines Netzwerks weiterzuleiten. Sie ermöglichen darüber hinaus die Skalierung eines Netzwerks und eine Verwaltung der verwendeten Bandbreite.

Grundsätzlich gib es zwei verschiedene Typen von Routern:

Hardwarerouter

Ein dediziertes Gerät, auf dem eine spezielle Software ausgeführt wird, die ausschließlich dem Routing dient.

Softwarerouter

Ein Router, der sowohl Routing, als auch andere Aufgaben übernimmt. Im Falle von Windows Server 2003 Routing und RAS handelt es sich dabei um einen solchen Dienst.

Eine Routinglösung besteht immer aus drei verschiedenen Komponenten: einer Routingschnittstelle, einem Routingprotokoll und Routingtabellen.

4.6.2 Die Routingschnittstelle

Eine physikalische oder logische Schnittstelle, über welche die Pakete weitergeleitet werden. Windows Server 2003 unterscheidet hier zwischen zwei verschiedenen Typen:

LAN-Schnittstellen (Local Area Network, lokales Netzwerk):

Dieser Schnittstellentyp entspricht einer gewöhnlichen Netzwerkkarte. In der Regel bedarf es keines Authentifizierungsvorgangs, um diese Schnittstelle zu aktivieren.

Schnittstellen für „Wählen bei Bedarf“:

Dieser Typ ist eine Punkt-zu-Punkt-Verbindung, die nur nach einer Authentifizierung zu Stande kommt. Implementierung dieses Typs findet man vor allem bei der Verwendung von VPNs (Virtual Private Network, Virtuelle Private Netzwerke). Ein VPN ist die Erweiterung eines privaten Netzwerks über ein öffentliches Netzwerk.

4.6.3 Die Routingtabelle

Diese Tabelle besteht aus einer Reihe von Routen, die Informationen zu bestimmten Positionen der Netzwerkkennungen in einem Netzwerk enthalten. Mit Hilfe dieser Informationen kann die optimale Route in einem Netzwerk berechnet werden.

© 2005, Microsoft Österreich GmbH

Routingtabellen werden aber nicht nur in Routern angewendet, sondern auch ganz normale Hosts (Computer) besitzen Routingtabellen.

In einer Routingtabelle gibt es drei verschiedene Eintragstypen:

- **Netzwerkroute**
  Stellt einen Pfad zu einer bestimmten Netzwerkkennung dar
- **Hostroute**
  Dies ist ein Pfad zu einer Netzwerkadresse. Damit werden im Normalfall benutzerdefinierte Routen zu bestimmten Computern erstellt, um den Verkehr zu steuern und zu optimieren.
- **Standardroute**
  Falls keine Routen für ein bestimmtes Ziel gefunden werden, wird die Standardroute verwendet, um die Pakete weiterzuleiten. Dadurch wird die Konfiguration der einzelnen Hosts vereinfacht.

So zeigen Sie die Routinginformationen des lokalen Rechners an:

1. Klicken Sie auf START - AUSFÜHREN.
2. Geben Sie bei Öffnen den Befehl CMD ein und bestätigen Sie mit ENTER.
3. An der Eingabeaufforderung geben Sie den Befehl ROUTE PRINT ein und drücken ENTER.

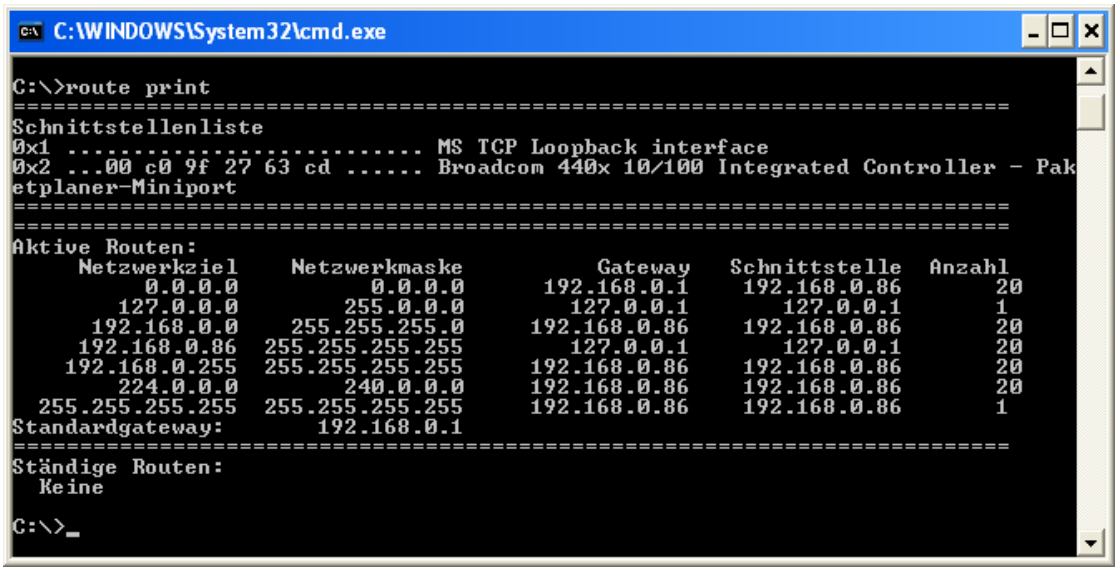


Abb. 45: Anzeige der Routinginformationen

Jeder Eintrag in der Routingtabelle besteht aus folgenden Informationsfeldern:

Feld	Bedeutung
Netzwerkziel	Gibt das Netzwerkziel der Route an. Dort kann eine IP-Netzwerkadresse (die Hostbits sind auf 0 gesetzt), eine IP-Adresse oder– im Fall der Standardroute – 0.0.0.0 stehen.
Netzwerkmaske	Gibt die Subnetzmaske an, die dem Netzwerkziel zugeordnet ist. Die Werte entsprechen entweder einer Subnetzmaske für eine IP-Netzwerkadresse, 255.255.255.255 für eine Hostroute bzw. 0.0.0.0 für die Standardroute.

Gateway	Gibt die Weiterleitungs-IP-Adresse bzw. IP-Adresse der nächsten Abschnitte bekannt, über die die definierten Adressen erreichbar sind.
Schnittstelle	Gibt die Nummer der Netzwerkschnittstelle für die angegebene Route an.
Metrik	Stellt ein ganzzahliges Kostenmaß für eine Route dar. Üblicherweise wird die Route mit der niedrigsten Anzahl verwendet.

© 2005, Microsoft Österreich GmbH

5 Lokale Benutzerverwaltung und in einer Domäne

Diese Kapitel erläutert die Implementierung und Konfiguration des Benutzermanagements unter Windows Server 2003 in einer Arbeitsgruppe und in einer Domäne.

5.1 Überblick – Definition für lokale Benutzerverwaltung

Der Zugriff auf Ressourcen und Informationen eines Netzwerks kann nicht jedem gestattet werden. Jeder Benutzer muss sich zu diesem Zweck identifizieren, d. h. sich mit seinem Benutzernamen und einem geheimen Kennwort anmelden.

Da Windows Server 2003 ein Mehrbenutzerbetriebssystem ist, bedarf es auch einer Möglichkeit, Benutzer und Gruppen anzulegen, um diesen dann Berechtigungen für den Zugriff auf Ressourcen einzuräumen.

Generell wird bei der Verwaltung der Benutzer zwischen Einzelplatzrechner und einer Arbeitsgruppe einerseits und einer Domäne andererseits unterschieden.

- Wenn Einzelplatzrechner und Computer sich in einer Arbeitsgruppe befinden, werden Benutzer immer lokal verwaltet.
- Nur bei Domänen kann ein Benutzer zentral im so genannten Active Directory angelegt werden und hat somit die Möglichkeit, sich an jedem Rechner in der Domäne anzumelden.

5.2 Die Benutzerverwaltung in einer Arbeitsgruppe

Bei der Benutzerverwaltung in einer Arbeitsgruppe werden die einzelnen Konten, Benutzer und Gruppenkonten auf der lokalen Workstation oder dem Server einer Arbeitsgruppe angelegt. In diesem Zusammenhang wird sehr häufig der Begriff **lokale Benutzerverwaltung** verwendet, da die Konten auf jedem einzelnen Arbeitsplatzrechner und Server erstellt werden müssen. Der Windows Server 2003 wird in diesem Fall nicht als Domänencontroller betrieben. Die lokale Benutzerverwaltung steht nur bei Member-Servern und bei Workstations zu Verfügung.

So öffnen Sie die lokale Benutzerverwaltung:

1. Klicken Sie auf START – PROGRAMME – VERWALTUNG – COMPUTERVERWALTUNG.
2. Wählen Sie im linken Teil der Konsole den Punkt LOKALE BENUTZER UND GRUPPEN, der sich im System befindet.
3. Sie können nun zwischen BENUTZER und GRUPPEN wählen.

© 2005, Microsoft Österreich GmbH

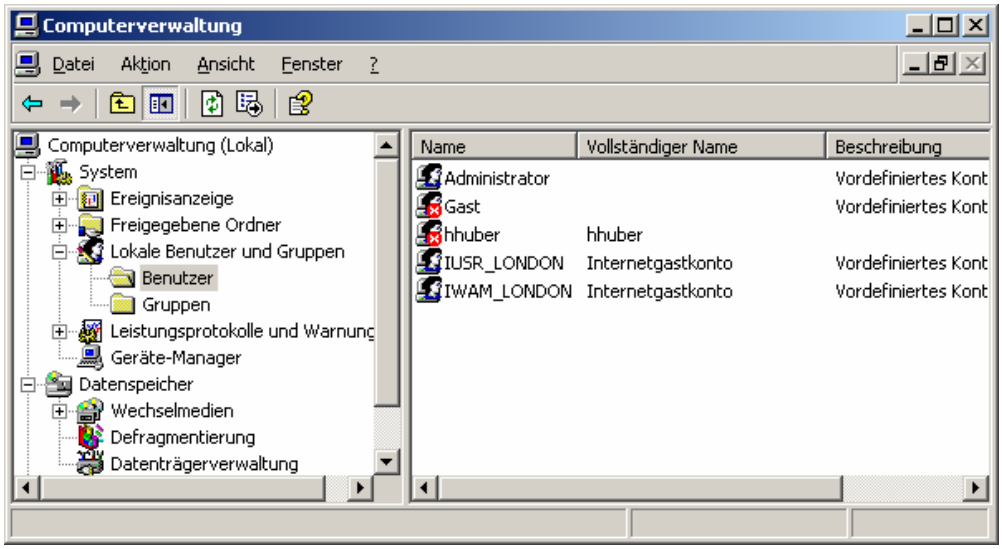


Abb. 46: MMC der lokalen Benutzerverwaltung

Die Vorgangsweise ist jedoch immer dieselbe:

Benutzer werden angelegt und anschließend einer oder mehreren Gruppen zugeordnet. Diesen Gruppen werden Berechtigungen erteilt. Ein Benutzer kann beliebig vielen Gruppen zugeordnet werden. Berechtigungen aus den diversen Gruppen addieren sich.

Standardmäßig sind drei Benutzerkonten angelegt.

- **Administrator**: Der Benutzer, der alle Rechte und Berechtigungen auf dem Server besitzt und dementsprechend sämtliche Konfigurationsaufgaben erledigen kann.
- **Gast**: Stellt ein vordefiniertes Konto dar, mit dem ein Gastzugriff auf den Computer oder die Domäne möglich ist. Die Berechtigungen für diesen Benutzer sind sehr eingeschränkt.
- **SUPPORT_xxxxxxxx**: Ein spezielles Konto, das der Hilfedienstgruppe zugeordnet ist, mit welchem primär Verbindungen mittels der Hilfe- und Supportdienste hergestellt werden. Diese sind auch für die Verwaltung dieses Kontos zuständig, d. h. dieses Konto wird automatisch angelegt, sobald eine Remoteunterstützungssitzung hergestellt wird.

Das Konto für den Gastzugriff und die Remoteunterstützung sind nach der Installation deaktiviert und können bei Bedarf aktiviert werden.

Wenn Sie das Administrator-Konto deaktivieren, können Sie sich nicht mehr am System anmelden. Sie müssen beim Starten des Computers die F8 Taste betätigen, damit Sie in den „Abgesicherten Modus“ wechseln. In diesem Modus können Sie sich als Administrator anmelden, selbst wenn das Konto deaktiviert ist.

Jedes Benutzerkonto wird einem Benutzer zugeordnet und kann diverse Informationen speichern.

5.2.1 Standardgruppen in Windows Server 2003

Unter Windows Server 2003 gibt es folgende Standardgruppen:

- **Administratoren**: Mitglieder dieser Gruppe haben vollen Zugriff auf den Server und können Benutzern Berechtigungen einräumen. Wird ein Server einer Domäne hinzugefügt, werden die Administratoren automatisch zu der Gruppe Domänen-Administratoren hinzugefügt.
- **Benutzer**: Jeder Benutzer, der in einer Domäne angelegt wird, wird dieser Gruppe standardmäßig zugeordnet. Mitglieder dürfen keine zufälligen oder beabsichtigten Änderungen am System vornehmen, sind aber in der Lage, Anwendungen zu starten, Drucker zu verwenden und den Computer zu sperren. Benutzer können jedoch keine Verzeichnisse freigeben oder lokale Drucker anlegen. Wird der Computer in einer Domäne verwendet, sind die zugeordneten Benutzer automatisch Mitglieder der Gruppen „Domänen-Benutzer" und „Authentifizierte Benutzer" sowie der Interaktiv-Gruppe.
- **Sicherungs-Operatoren**: Mitglieder dieser Gruppe können Daten sichern und wiederherstellen, unabhängig von den Berechtigungen, die für die jeweiligen Daten gelten. Sie können jedoch keine Sicherheitseinstellungen ändern.
- **DHCP-Administratoren**: Diese Gruppe wird eingerichtet, sobald ein DHCP-Server installiert wird. Mitglieder dieser Gruppe haben administrativen Zugriff auf den DHCP-Server, können jedoch keine anderen administrativen Aufgaben am Server erledigen.
- **DHCP-Benutzer**: Mitglieder dieser Gruppe haben Nur-Lesezugriff auf den DHCP-Dienst.
- **Gäste**: Für Mitglieder dieser Gruppe wird beim Einloggen ein temporäres Profil angelegt, das beim Abmelden wieder gelöscht wird. Das Gastkonto ist Mitglied dieser Gruppe.
- **Hilfedienstgruppe**: Mit Hilfe dieser Gruppe können Administratoren die Zugriffsrechte von Hilfestellungsanwendungen definieren. Dieser Gruppe sollten Sie jedoch keine Benutzer zuordnen.
- **Netzwerkkonfigurations-Operatoren**: Mitglieder dieser Gruppe dürfen die TCP/IP-Einstellungen ändern. Standardmäßig sind dieser Gruppe keine Mitglieder zugeordnet.
- **Systemmonitorbenutzer**: Mitglieder dieser Gruppe können den Leistungsmonitor lokal und auf Remoteclients verwenden, ohne dass sie Mitglied der Administratorengruppe sein müssen.
- **Leistungsprotokollbenutzer**: Diese Gruppe verfügt über Rechte, um die Protokollierung von Leistungsindikatoren auf diesem Computer zu planen.
- **Hauptbenutzer**: Mitglieder dieser Gruppe besitzen ähnliche Rechte wie Administratoren, mit ein paar Ausnahmen: Sie dürfen Benutzer und Gruppen anlegen, ändern und löschen (ebenso dürfen Sie weitere Hauptbenutzer anlegen), sie haben Zugriff auf Netzwerkfreigaben, dürfen jedoch keinen Besitz von Dateien übernehmen und können keine Dateien und Verzeichnisse sichern bzw. wiederherstellen; außerdem dürfen Mitglieder der Hauptbenutzergruppe keine Gerätetreiber laden und keine Sicherheits- und Überwachungsprotokolle einsehen.
- **Druck-Operatoren**: Diese können Drucker und Druckwarteschlangen in der Domäne managen.
- **Replikations-Operator**: Diese Gruppe unterstützt die Dateireplikation in Domänen. Fügen Sie dieser Gruppe keine Benutzer hinzu.
- **WINS-Benutzer**: Haben Nur-Lesezugriff auf den WINS (Windows Internet Name Service)-Server. Diese Gruppe ist verfügbar, sobald ein WINS-Server installiert ist. In einer reinen Windows Server 2003- und Windows XP Professional-Umgebung kann auf die Installation eines WINS-Servers verzichtet werden.

© 2005, Microsoft Österreich GmbH

5.2.2 Benutzer einer Arbeitsgruppe manuell anlegen

So legen Sie einen lokalen Benutzer an:

1. Klicken Sie auf START – VERWALTUNG – COMPUTERVERWALTUNG.
2. In der Konsolenstruktur klicken Sie auf LOKALE BENUTZER UND GRUPPEN.
3. Klicken Sie auf BENUTZER.
4. Im Menü AKTION klicken Sie auf NEUER BENUTZER...
5. Geben Sie die Daten ein und klicken Sie auf ERSTELLEN.
6. Klicken Sie auf SCHLIEßEN.

Um diese Schritte auszuführen, müssen Sie zumindest Mitglied einer der Gruppen „Administratoren" oder „Hauptbenutzer" sein oder die Rechte dafür erteilt bekommen haben.

Der **Benutzername** selbst kann bis zu **20 Zeichen lang**, muss jedoch eindeutig sein. Zeichen, die nicht verwendet werden dürfen, sind:

„ / \ [ ] : ; | , + * ? < >

Außerdem darf der Benutzername nicht nur aus Punkten und Leerzeichen bestehen.

Im Feld **Kennwort** und **Kennwort bestätigen** können Sie ein Passwort mit einer Länge von bis zu **127 Zeichen** eingeben.

In einem Netzwerk, in dem Clients verwendet werden, die Windows 95 oder Windows 98 benutzen, sollte das Kennwort nicht länger als 14 Zeichen sein, da die Benutzer sich sonst möglicherweise nicht anmelden können.

In der Detailansicht auf der rechten Seite der Konsole werden die Benutzer nun angezeigt. Sofern diese nicht mit einem roten Schild mit einem weißen X gekennzeichnet sind, können sich diese Benutzer nun am System anmelden. Das rote Schild bedeutet, dass das Konto deaktiviert ist. Sie müssen es zuerst aktivieren, damit sich die Benutzer anmelden können.

© 2005, Microsoft Österreich GmbH

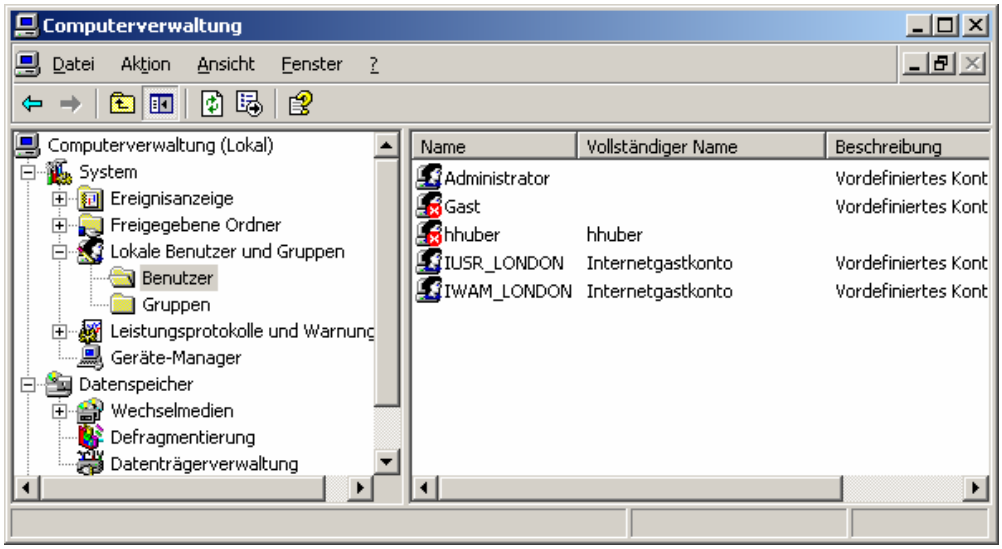


Abb. 47: Benutzerverwaltung - mit zwei deaktivierten Benutzerkonten

Mit einem Doppelklick auf den entsprechenden Benutzer können Sie die Eigenschaften über die einzelnen Register des angezeigten Dialogfensters bearbeiten.

Folgende Register stehen bei der lokalen Benutzerverwaltung zur Verfügung:

ALLGEMEIN	Hier können Sie den Namen und die Beschreibung für den Benutzer ändern. Weitere Optionen sind: ◆ Benutzer muss Kennwort bei der nächsten Anmeldung ändern ◆ Benutzer kann Kennwort nicht ändern ◆ Kennwort läuft nie ab ◆ Konto ist deaktiviert ◆ Konto ist gesperrt
MITGLIEDSCHAFT	Teilen Sie dem Benutzer eine oder mehrere Gruppen zu, indem Sie auf den Knopf HINZUFÜGEN drücken. Danach drücken Sie auf ERWEITERT und JETZT SUCHEN, wählen eine Gruppe von den Suchergebnissen aus und bestätigen mit OK.
PROFIL	Hier können Sie einen Profilpfad sowie ein Anmeldeskript angeben, das beim Anmelden ausgeführt wird. Für eine genauere Beschreibung sehen Sie sich den Punkt Benutzerprofile weiter unten an. Wollen Sie servergelagerte Profile verwenden, müssen Sie hier UNC-Pfade zu einer Netzwerkfreigabe angeben, auf die der Benutzer Schreibrechte besitzt.
UMGEBUNG	Hier können Sie die Startumgebung für die Terminaldienste konfigurieren.
SITZUNGEN	Stellt Konfigurationsmöglichkeiten der Zeitlimits für Terminaldienste zur Verfügung
REMOTESTEUERUNG	Auf diesem Reiter werden die Remotesteuerungseinstellungen für die Terminaldienste

	bearbeitet.
TERMINALDIENSTPROFILE	Für die Terminaldienste können Sie eigene Profile definieren.
EINWÄHLEN	Erteilt oder verweigert dem Benutzer Einwahlrechte auf dem Server.

Sobald ein Benutzer sich das erste Mal an einem System anmeldet, wird an dem lokalen Rechner, an dem sich der Benutzer befindet, ein Unterverzeichnis in „Dokumente und Einstellungen" für diesen User angelegt. In diesem Ordner – dem Profilordner des Benutzers – werden u. a. der Ordner „Eigenen Dateien" und die persönlichen Anwendungsdaten des Benutzers gespeichert.

Wird ein Benutzer gelöscht, bleiben die Dateien und Ordner des Benutzers im Verzeichnis „Dokumente und Einstellungen" erhalten.

Dies hat aber auch Nachteile: Meldet sich der Benutzer von einem anderen Computer am System an, so kann er nicht ohne weiteres auf seine persönlichen Daten zugreifen, da diese eben nicht auf dem aktuellen Rechner gespeichert sind.

Ein weiteres Problem stellt die Datensicherung dar: Soll eine zentrale Datensicherung implementiert werden, dann müssen die Daten auch zentral verfügbar gemacht werden. Einen Ausweg aus diesem Dilemma bieten uns „Benutzerprofile" an. Sehen Sie sich hierzu den Punkt Benutzerprofile – Kap.: 6.2.2 an.

5.2.3 Eine lokale Gruppe manuell anlegen

So legen Sie eine neue Gruppe an:

1. Klicken Sie auf START – VERWALTUNG – COMPUTERVERWALTUNG.
2. In der Konsolenstruktur klicken Sie auf LOKALE BENUTZER UND GRUPPEN.
3. Klicken Sie auf GRUPPEN.
4. Im Menü AKTION wählen Sie NEUE GRUPPE. . . .
5. Geben Sie den Namen der Gruppe im Feld Gruppenname ein.
6. Ergänzen Sie eventuelle Benutzernamen mittels HINZUFÜGEN.
7. Klicken Sie auf ERSTELLEN.
8. Klicken Sie auf SCHLIEßEN.

Bei der Namensgebung für Gruppen gelten die gleichen Regeln, wie für Benutzernamen. Über die Auswahl der Gruppeneigenschaften (Rechtsklick auf den Gruppennamen), können Sie nachträglich prüfen, welche Benutzer einer Gruppe zugeordnet sind.

© 2005, Microsoft Österreich GmbH

5.3 Benutzerverwaltung in einer Domäne

Mit der Einführung des **Active Directory** in Windows 2000 wurde ein neuer Verzeichnisdienst eingeführt, der bei Windows Server 2003 erweitert und in vielen Punkten wesentlich verbessert wurde. Das Active Directory ist somit das Zentrum für die Sicherheit und Delegierung von Verwaltungsberechtigungen einer Windows Server 2003-Domäne.

Im übertragenen Sinn ist ein Verzeichnisdienst mit einem Telefonbuch vergleichbar. Im Verzeichnisdienst von Windows Server 2003 – dem Active Directory – sind Benutzer, Gruppen und andere Ressourcen hinterlegt.

In modernen Netzwerken, in denen sich mehrere Server befinden, auf denen die Ressourcen verteilt sind, benötigen wir **Verzeichnisdienste**, um Benutzer und Ressourcen finden zu können. Mit der steigenden Zahl der Benutzer und Server eines Netzwerks – heute hat jeder Benutzer sein eigenes Benutzerkonto – sind derartige Verzeichnisdienste unerlässlich. Darin werden diverse Objekte wie Benutzer, Gruppen, Freigaben von Verzeichnissen usw. hinterlegt. Jedes dieser Objekte verfügt dabei wieder über diverse Attribute wie z. B. die E-Mail-Adresse eines Benutzers. Verzeichnisdienste werden damit zu einer zentralen Informationsstelle für die Benutzer des Netzwerks.

Begriffe im Active Directory

Im Active Directory werden unterschiedliche Begriffe verwendet, die kurz erläutert werden sollen.

Mögliche Objekte im Active Directory sind:

- Gesamtstruktur, Struktur
- Domäne
- Organisationseinheit
- Benutzer
- Gruppe
- Freigegebene Ordner
- Computer
- Drucker

In einer Schule können mehrere hundert oder auch tausend dieser Objekte auftreten. Um eine Übersicht über die große Zahl dieser Objekte zu erhalten, werden sie nach logischen und/oder physikalischen Gesichtspunkten gruppiert.

Die **Organisationseinheit** stellt die unterste Ebene für die Planung des Active Directory dar. Sofern Windows Server 2003 in der Betriebsart „**Windows Server 2003**" betrieben wird, kann eine Organisationseinheit selbst wieder eine oder mehrere Organisationseinheiten enthalten.

Jede Organisationseinheit dient letztlich der Aufnahme von Objekte wie z. B.: Benutzer, Gruppen oder Ressourcen sowie der Delegierung von Verwaltungsrechten oder der Hinterlegung von Gruppenrichtlinien.

© 2005, Microsoft Österreich GmbH

Eine zentrale Stelle im Active Directory nimmt die **Domäne** ein. Sie ist die **unterste Einheit für die zentrale Verwaltung** – also die Administration der Benutzer und Gruppen. Daneben ist eine Domäne die **natürliche Grenze für Sicherheitseinstellungen**. Berechtigungen können innerhalb einer Domäne vererbt werden, aber nicht über diese hinaus. Da das primäre Kommunikationsprotokoll von Windows Server 2003 TCP/IP ist, wird zur Identifizierung der Domänen der DNS-Name verwendet.

In diesem Skriptum wird allgemein der DNS-Name „MeineSchule.local" verwendet. Bei einer konkreten Installation sollten Sie den DNS-Namen Ihrer Schule z. B. hlw-bmdf.ac.at verwenden.

In jeder Domäne muss mindestens ein **Domänencontroller** und ein **Windows DNS-Server** für diese Domäne betrieben werden.

Aus Gründen der Ausfallsicherheit sollten in jeder Domäne jedoch mindestens zwei Domänencontroller betrieben werden. Die höhere Ausfallsicherheit für das Active Directory führt auch zu einer Lastverteilung bei der Anmeldung der Benutzer.

Bsp: An einer durchschnittlichen Schule mit 500 Benutzern soll ein Windows Server 2003-Netzwerk mit mehreren Servern installiert werden. Der DNS-Name der Schule lautet *MeineSchule.local*. Für diese Schule ist eine einzige Domäne vorgesehen. Visuell wird diese durch ein Dreieck dargestellt.

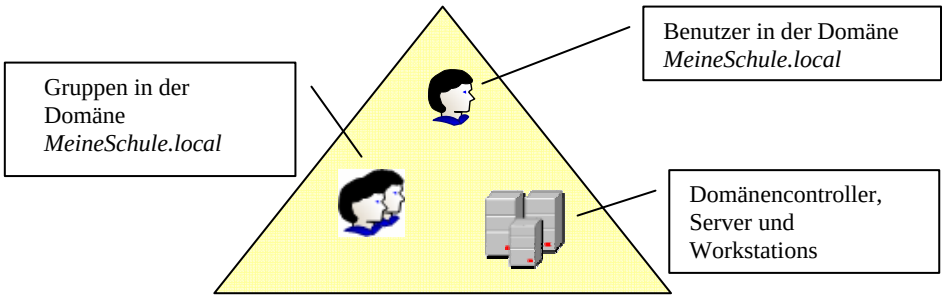


Abbildung 48: Domäne „MeineSchule.local" mit Benutzern, Gruppen und Servern

5.4 Planung des Active Directory

Bevor Benutzer, Gruppen oder Computerkonten im Active Directory erstellt werden, sollte das Active Directory bezüglich der Gliederung durch Organisationseinheiten geplant werden. Leider gibt es dafür kein Universalrezept, da jede Schule ihre Eigenheiten hat.

In den meisten Fällen wird man mit einer einzigen Domäne auskommen und kein Multidomänen-Modell verwenden.

Auf jeden Fall sollte man Benutzer, Gruppen und Computerkonten in getrennten Organisationseinheiten ablegen. Grundlage für die Organisation könnte das „Organigramm der Schule" durch Einteilung in Klassen etc. sein.

Ein möglicher Vorschlag für die Organisation der Benutzer und Gruppenkonten könnte so aussehen:

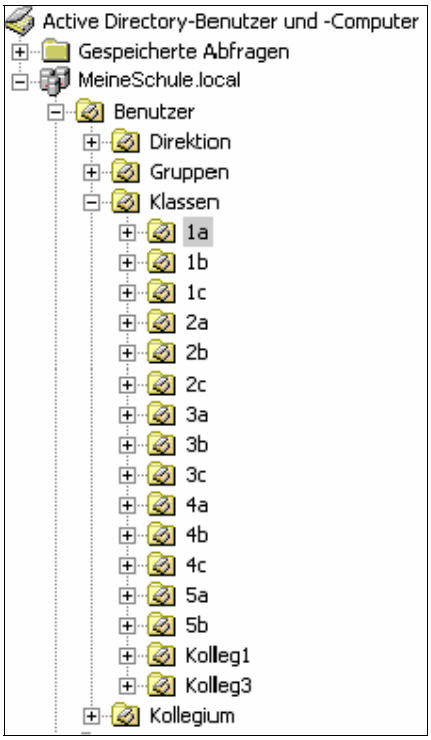


Abbildung 49: Ein Vorschlag für die Organisation der Benutzer (Fensterausschnitt)

Anmerkung: Mit Windows Server 2003 ist es möglich, Organisationseinheiten mittels Drag und Drop – also durch Ziehen mit der Maus – zu verschieben.

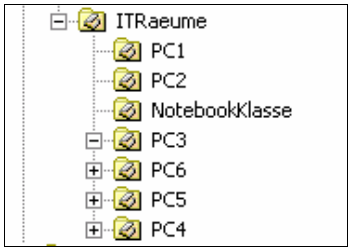


Abb. 50: Organisation der Computer einer Schule (Fensterausschnitt)

5.5 Anlegen eines Benutzers im Active Directory

Nachdem das Active Directory eine Struktur von Organisationseinheiten erhalten hat, müssen die Benutzer- und Gruppenkonten einer Domäne eingerichtet werden.

Dabei sind für jeden Benutzer

- ein Benutzername
- ein Kennwort
- ein persönlicher Ordner
- ein Ordner für sein Benutzerprofil
- eine E-Mail-Adresse
- etc.

anzulegen oder zu vergeben.

Das persönliche Verzeichnis wird sehr häufig auch Home- oder Basisverzeichnis des Benutzers genannt.

Bei mehreren hundert Benutzern kann diese Arbeit allerdings nicht mehr manuell bewältigt werden und es stellt sich die Frage, welche Programme diese Arbeit übernehmen.

Neben Scripting mit Windows Scripting Host liefert Microsoft mit Windows Server 2003 diverse neue Commandline-Tools wie z. B.: **dsadd.exe,** mit deren Hilfe Objekte im Active Directory angelegt, gelöscht oder abgefragt werden können.

Neben den bereits erwähnten Tools gibt es aber noch eine Vielzahl anderer Programme, wie z. B. **eUser**, **User Agent II** und andere, die kostenlos oder gegen Entgelt angeboten werden.

eUser wurde von Georg Steingruber erstellt. Dieses Programm können Schulen kostenlos über die Web-Site http://ms.asn-graz.ac.at beziehen.

User Agent II wurde von Peter Koen und Robert Beron neu entwickelt. Das Programm wird gegen eine Gebühr von 200 Euro exkl. USt. vertrieben. Nähere Informationen erhalten Sie über office@beron.at.

5.5.1 Manuelle Anlage eines Benutzerkontos im Active Directory

Im Gegensatz zur lokalen Benutzerverwaltung einer Arbeitsgruppe werden die Benutzer, Gruppen und Computer einer Domäne im Active Directory über eine eigene Managementkonsole verwaltet.

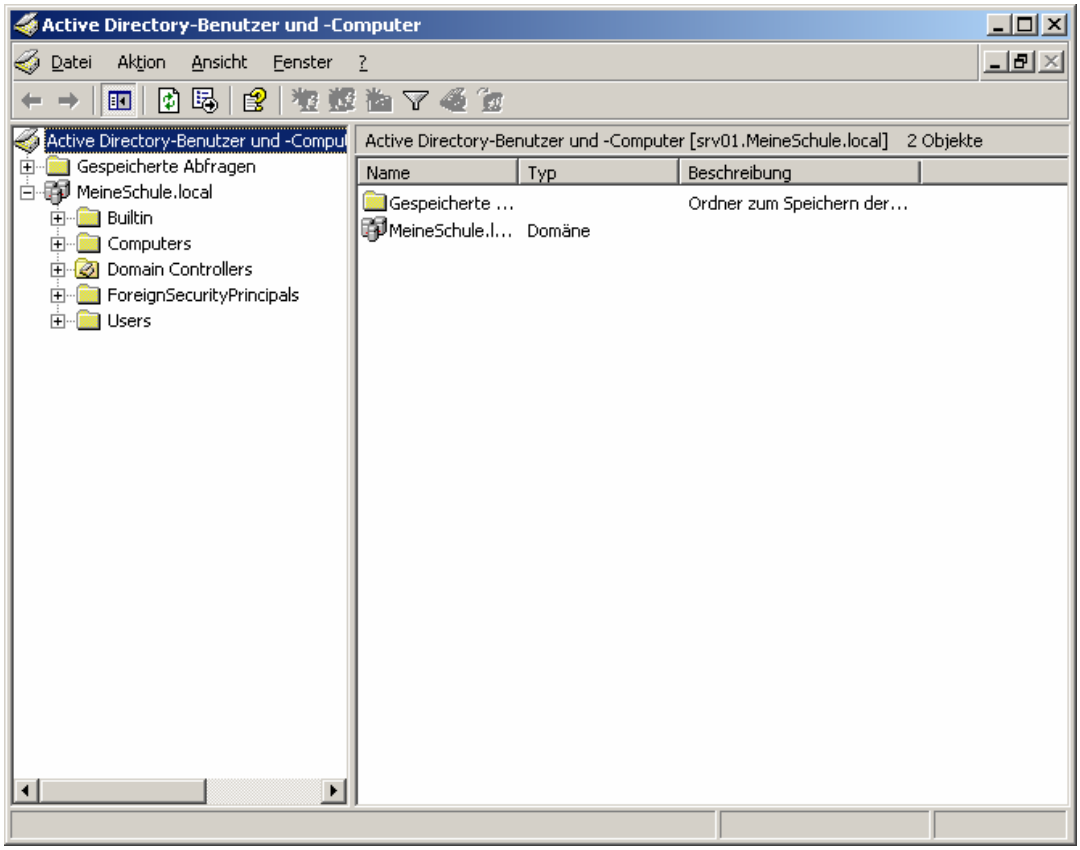


Abb. 51: MMC-Active-Directory- Benutzer und –Computer nach dem Einrichten der Domäne

Nachdem Sie Active Directory installiert haben, geschieht die Benutzer- und Gruppenverwaltung nur noch in der MMC, mit der Sie das Active Directory bearbeiten können. Der Knoten „Lokale Benutzer und Gruppen" in der MMC-Computerverwaltung wird deaktiviert.

Eine der Maximen in einem Netzwerk ist die Kontinuität. Benutzernamen, Gruppen und Namen von Ressourcen sollten immer nach einem bestimmten Schema aufgebaut werden. Bevor Sie sich an die manuelle Anlage der Benutzer und Gruppen in ihrem Active Directory machen, sollten Sie sich zuerst eine eindeutige Namenskonvention überlegen.

Wie soll das Benutzerkonto bei der Anmeldung heißen? Dafür gibt es unterschiedliche Möglichkeiten, die am Beispiel des Benutzers „John Doe" kurz erläutert werden sollen.

Soll der Benutzeranmeldename

- John.Doe
- Doe.John
- JDoe oder
- JohnD

lauten?

Weitere Fragen in diesem Zusammenhang sind:

- Sollen die Benutzernamen auf eine bestimmte Zahl von Zeichen beschränkt werden?
- Wie geht man mit Zeichen um, die nicht im „amerikanischen Zeichensatz" enthalten sind – z. B. Umlaute?

So legen Sie in Active Directory einer Domäne einen Benutzer an:

1. Klicken Sie auf START – ALLE PROGRAMM – VERWALTUNG.
2. Wählen Sie den Punkt ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
3. In der Managementkonsole wählen Sie in der Struktur Ihre Domäne aus.
   Darunter befindet sich ein Ordner namens USER, den Sie mit der linken Maustaste anklicken.
4. Wählen Sie aus dem Menü AKTION – NEU – BENUTZER.

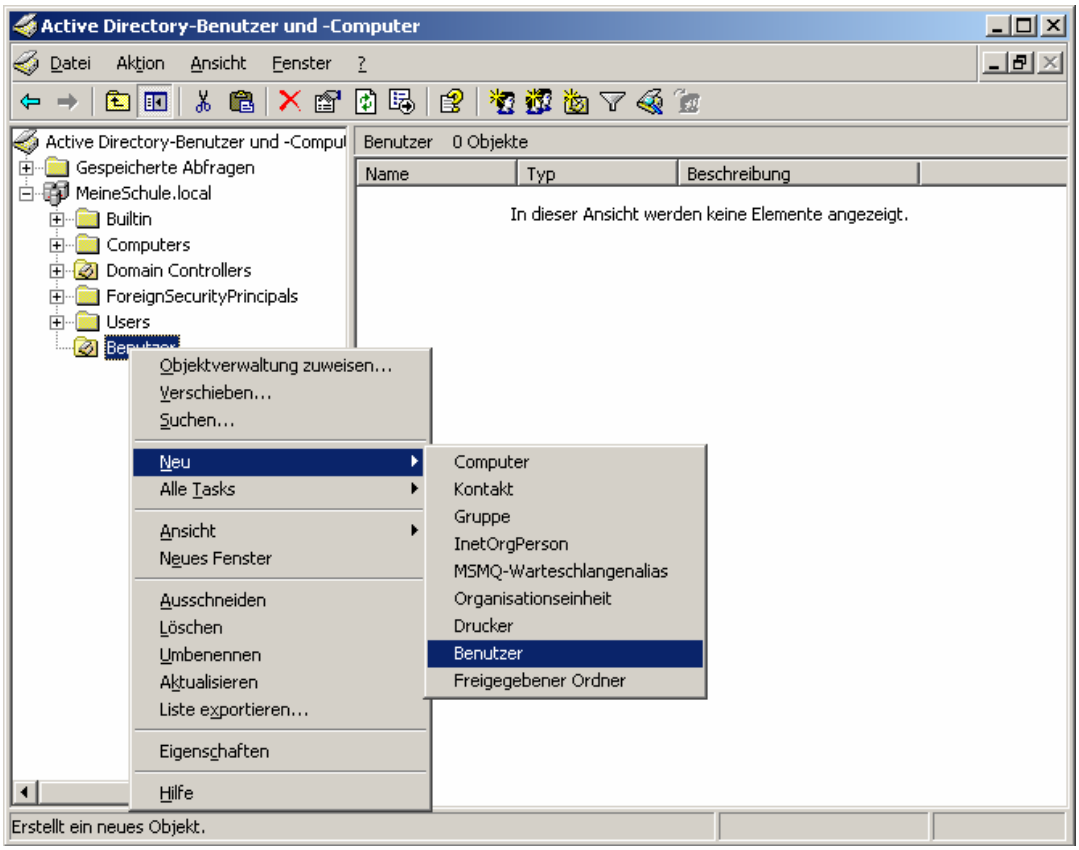


Abb. 52: MMC Active Directory-Benutzer und –Computer

5. Der Assistent zum Anlegen eines neuen Benutzer-Objekts wird angezeigt. Er unterscheidet sich geringfügig von der lokalen Benutzererstellung.

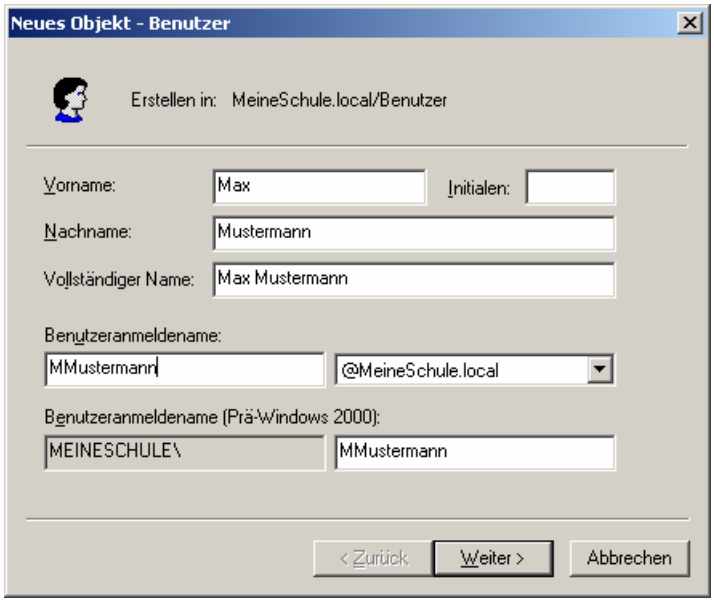


Abb. 53: Anlage eines Benutzerkontos

6. Auf der ersten Seite geben Sie die Anmeldedaten des Benutzers ein. Danach klicken Sie auf WEITER.
7. Geben Sie das Kennwort des Benutzers ein und wählen Sie aus den Kontooptionen die gewünschten Punkte.
8. Abschließend klicken Sie auf WEITER und FERTIGSTELLEN.

So bearbeiten Sie die Benutzereigenschaften:

1. Öffnen Sie über den Punkt VERWALTUNG die ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
2. Wählen Sie USERS unter der gewünschten Domäne.
3. In der Detailansicht auf der rechten Seite der Konsole werden die angelegten Benutzer und Gruppen aufgelistet.
4. Wählen Sie einen Benutzer und öffnen Sie das Eigenschaftsfenster mittels eines Doppelklicks auf diesen bzw. über das Menü AKTION – EIGENSCHAFTEN.

© 2005, Microsoft Österreich GmbH

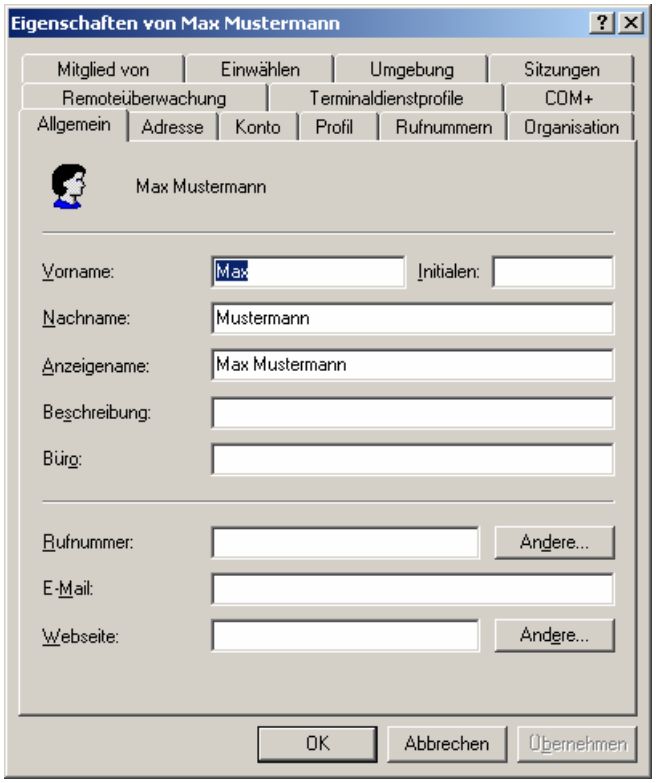


Abb. 54: Das Dialogfenster Benutzereigenschaften

Nachdem das Benutzerkonto angelegt ist, müssen weitere Informationen für dieses Konto angegeben werden. Zu den minimalen Einstellungen, die Sie unbedingt angeben müssen, gehören für jeden Benutzer:

- **Basisordner des Benutzers**: Dieser Ordner dient dem Benutzer für die Ablage seiner Dateien und ist somit ein persönlicher Ordner. Auf diesen Ordner sollte nur der Benutzer und der Administrator des Netzwerks zugreifen können. Dieser Ordner sollte unbedingt versteckt freigegeben werden.
- **Profil-Ordner**: Ordner, in dem das Profil des Anwenders gespeichert wird. In diesem Profil werden Daten oder Einstellungen wie z. B. Maus für Links- oder Rechtshänder, Hintergrund eines Desktops, Lesezeichen in Hilfedateien, Favoriten, der Ordner „Eigene Dateien" etc. hinterlegt.
- Als Pfad für diesen Ordner kann z. B. ein eigener Profil-Freigabe-Ordner – \\srv01\Profile\MMustermann.pds – angegeben werden. Alternativ kann der Ordner auch in den Basisordner des Benutzers gelegt werden.

Falls Sie zu dieser Variante tendieren, sollten Sie sich unbedingt eine Struktur überlegen, um Schüler- und Lehrerprofile unterscheiden zu können. Lehrerprofile könnten z. B. auf der Freigabe \\srv01\Lehrer abgelegt werden. Damit wird das Löschen von Schülerprofilen am Jahresende wesentlich erleichtert.

- **Anmeldeskript**: Mit einem Skript, einer Batch-Datei oder einem Programm, das bei der Anmeldung des Benutzers gestartet wird, wird die Arbeitsumgebung des Benutzers eingestellt.

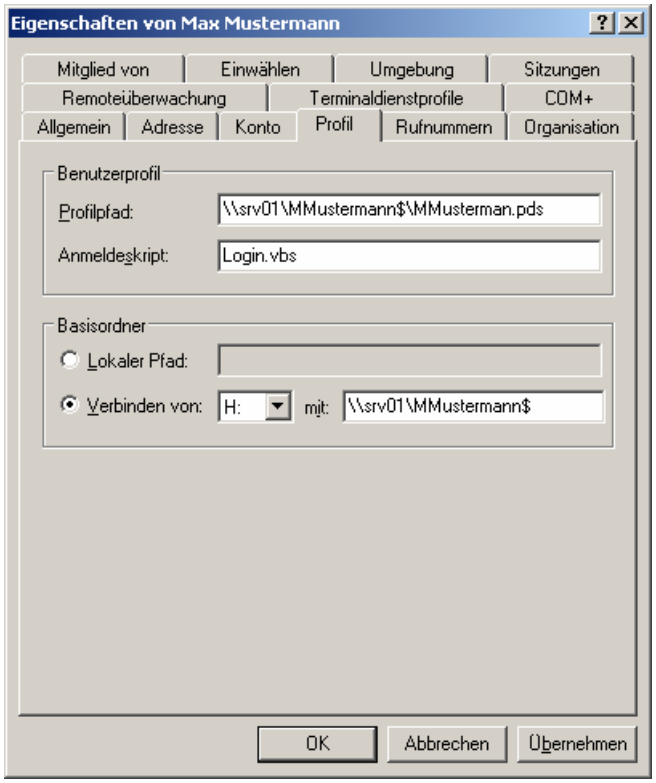


Abb. 55: Eigenschaften des Benutzers Max Mustermann

Aus der Vielzahl der Register lässt sich sofort erahnen, dass noch viele zusätzliche Einstellungen und Angaben pro Benutzer gemacht werden können. Allerdings haben Sie mit der Einstellung des Profilpfads und des Basisverzeichnisses die absolut notwendigen Arbeiten für die Anmeldung eines Benutzers abgeschlossen.

5.5.2 Benutzerprofile

Mit Hilfe von Benutzerprofilen werden die Desktopeinstellungen für die Arbeitsumgebung der einzelnen Benutzer erstellt und gepflegt. Für jeden Benutzer wird ein solches Profil angelegt, wenn er sich zum ersten Mal an einem Computer anmeldet.

Die Verwendung von Benutzerprofilen bietet durchaus Vorteile:

- Mehrere Benutzer können einen Computer verwenden. Wenn sich die Benutzer an ihren einzelnen Arbeitsstationen anmelden, werden die ursprünglich festgelegten Desktopeinstellungen wiederhergestellt.
- Anpassungen des Desktops haben keinerlei Auswirkung auf andere Benutzer.
- Benutzerprofile können auf dem Server gespeichert werden und sind so innerhalb des Netzwerks auf jedem Rechner verfügbar.

Unter Windows Server 2003 gibt es verschiedene Arten von Benutzerprofilen:

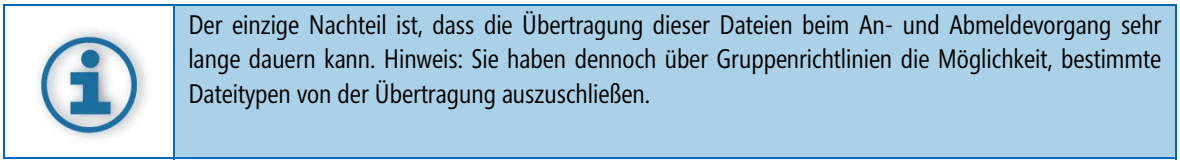
- **Lokale Benutzerprofile**: Diese werden lokal auf dem Datenträger erstellt und sind nur auf diesem verfügbar.
- **Servergespeicherte Benutzerprofile**: Werden von Administratoren erstellt und auf dem Server gespeichert. Bei jeder Anmeldung des Benutzers werden dessen Daten über das Netzwerk auf den Computer übertragen, an dem sich der Benutzer anmeldet. Bei der Abmeldung werden die möglicherweise aktualisierten Daten wieder zurückgespeichert.

© 2005, Microsoft Österreich GmbH

- **Temporäre Benutzerprofile**: Werden dann verwendet, wenn das eigene Benutzerprofil aus irgendwelchen Gründen nicht geöffnet werden kann. Änderungen, die an temporären Benutzerprofilen durchgeführt werden, können nicht gespeichert werden.
- **Verbindliche Profile**: Dies sind servergespeicherte Profile, die vom jeweiligen Benutzer nicht geändert werden können. Lediglich Administratoren können Änderungen an den Einstellungen vornehmen.

Vor allem in größeren Netzwerken und in Netzwerken, in denen die Benutzer häufig an verschiedenen Rechnern arbeiten, bieten servergespeicherte Benutzerprofile einige Vorteile:

- Die Administrierung kann zentral erfolgen.
- Rechner können problemlos getauscht werden, da die Benutzerdaten jedes Mal vom Server geladen werden.
- Datensicherungen können ebenfalls am Server durchgeführt werden.
- Den Benutzern steht bei jeder Anmeldung ihre gewohnte Arbeitsumgebung zur Verfügung.



Der einzige Nachteil ist, dass die Übertragung dieser Dateien beim An- und Abmeldevorgang sehr lange dauern kann. Hinweis: Sie haben dennoch über Gruppenrichtlinien die Möglichkeit, bestimmte Dateitypen von der Übertragung auszuschließen.

So erstellen Sie ein vorkonfiguriertes Benutzerprofil

1. Erstellen Sie ein neues Benutzerkonto, dessen Profil als Vorlage verwendet werden soll.
2. Melden Sie sich mit diesem neuen Benutzernamen an.
3. Passen Sie den Desktop an und installieren Sie Anwendungen, um das Profil dieses Benutzers zu konfigurieren.
4. Melden Sie sich ab, und melden Sie sich als Administrator an.
5. Klicken Sie auf START – SYSTEMSTEUERUNG – SYSTEM.
6. Öffnen Sie die Registerkarte ERWEITERT und klicken Sie bei BENUTZERPROFILE auf Einstellungen.
7. Wählen Sie bei AUF DIESEM COMPUTER GESPEICHERTE PROFILE den gerade erstellten Benutzer aus.
8. Klicken Sie auf KOPIEREN NACH.

   Falls Sie ein Standardprofil für die gesamte Domäne wünschen, geben Sie den Pfad zu NETLOGON\Default User auf dem Domänencontroller ein. Auf diese Weise wird das Standardbenutzerprofil für die Domäne erstellt.

   Wollen Sie lediglich für den lokalen Computer das Standardprofil ändern, kopieren Sie das Profil in das Verzeichnis *sytemroot*\Dokumente und Einstellungen\Default User.
9. Klicken Sie unter Benutzer auf ÄNDERN.
10. Geben Sie bei OBJEKTNAMEN „**Jeder**“ ein.

Kopieren und Löschen von Benutzerprofilen

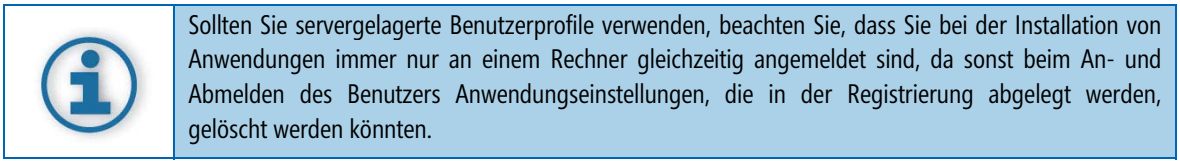
Das Kopieren und Löschen von Profilen geschieht jeweils in der Systemsteuerung unter SYSTEM auf dem Reiter ERWEITERT. Dort finden Sie in der Mitte den Punkt BENUTZERPROFILE. Klicken Sie danach auf EINSTELLUNGEN.

Beachten Sie jedoch, dass Sie kein Benutzerprofil kopieren oder löschen können, das zu dem aktuell angemeldeten Benutzer oder einem beliebigen Benutzer gehört, dessen Profil gerade in Verwendung ist.

© 2005, Microsoft Österreich GmbH

So erstellen Sie ein servergespeichertes Benutzerprofil für einen Benutzer

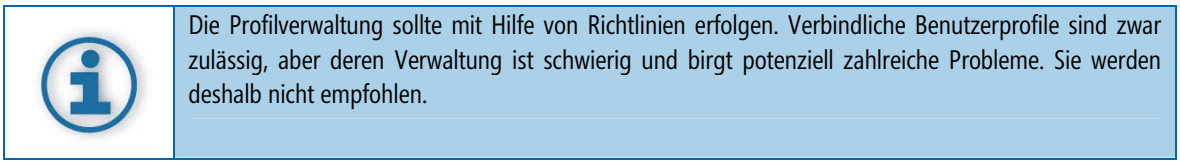
1. Starten Sie Active Directory-Benutzer und -Computer.
2. Klicken Sie im Kontextmenü des entsprechenden Benutzers auf EIGENSCHAFTEN.
3. Klicken Sie auf die Registerkarte PROFIL.
4. Geben Sie in Profilpfad die Pfadinformationen im Format \\Servername\Freigabename$\Benutzername ein.
5. Klicken Sie auf OK.



So erstellen Sie ein verbindliches Benutzerprofil

1. Starten Sie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
2. Klicken Sie im Kontextmenü des entsprechenden Benutzers auf EIGENSCHAFTEN.
3. Klicken Sie auf die Registerkarte PROFIL.
4. Geben Sie in Profilpfad die Pfadinformationen und am Ende die Dateinamenerweiterung ***.man*** ein (mandatory=verpflichtend).
5. Klicken Sie auf OK.

Alternativ dazu können Sie die auf dem Server gespeicherte Datei **Ntuser.dat** in **Ntuser.man** umbenennen. Durch diese Erweiterung wird das Profil schreibgeschützt.



Als Profilpfad sollte für jedes Benutzerkonto ein vollständiger Pfad angegeben werden, z. B. \\Server\Freigabename\Benutzername.

Erstellen Sie hierzu für *Freigabename* einen Profilordner, wenn dieser noch nicht vorhanden ist, und erteilen Sie für authentifizierte Benutzer die Freigabeberechtigung „Nur Lesen“. Der freigegebene Ordner muss vor der Verwendung erstellt werden.

5.6 Gruppenverwaltung im Active Directory

Jede Gruppe im Active Directory verfügt über einen Bereich, der bestimmt, in welchem Umfang die Gruppe verwendet werden kann. Dabei unterscheidet Windows Server 2003 zwischen drei verschiedenen Gruppenbereichen und zwei Gruppentypen.

5.6.1 Gruppenbereiche

Domänenlokale Gruppen

Die Mitglieder einer domänenlokalen Gruppe können für die direkte Zuweisung auf spezielle Ressourcen, die nicht direkt im Active Directory gespeichert werden (z. B. Dateiserverfreigaben und Druckerwarteschlangen), verwendet werden. Die Gruppen werden jedoch nur dazu benutzt, um Berechtigungen innerhalb einer Domäne zuzuweisen.

Achtung: Unterscheiden Sie bitte zwischen einer **lokalen Gruppe** einer Workstation oder eines Member-Servers und einer **domänen-lokalen Gruppe**. Eine domänen-lokale Gruppe kann auf einer Workstation oder einem Member-Server nicht für die Vergabe von Rechten verwendet werden, weil sie dort gar nicht verfügbar ist!

Folgende Mitglieder können einer lokalen Gruppe zugewiesen werden:

- Gruppen mit dem Bereich „Global"
- Gruppen mit dem Bereich „Universell"
- Konten
- Andere Gruppen mit dem Bereich „Lokal"
- Eine beliebige Kombination der eben genannten Objekte

Verwendungszweck: Domänen-lokale Gruppen werden für die Erteilung von Zugriffsberechtigungen auf Ressourcen – Ordner, Dateien, Drucker – verwendet.

Globale Gruppen

Die Mitglieder einer globalen Gruppe können ausschließlich Gruppen und Konten aus der Domäne sein, in der die Gruppe definiert wurde. Berechtigungen können jedoch in jeder Domäne der Gesamtstruktur zugewiesen werden.

Diese Art von Gruppen sollte zur Verwaltung von Verzeichnisobjekten verwendet werden, die eine häufige Wartung erfordern – speziell Computer- und Benutzerkonten. Die Gruppe ist zwar in ihrer Domäne und in allen vertrauenswürdigen Domänen sichtbar, Mitglieder dieser Gruppe können jedoch nur aus der eigenen Domäne stammen.

Die zugewiesenen Rechte und Berechtigungen der Gruppe sind zwar nur innerhalb einer Domäne gültig. Sie können diese Gruppe jedoch auf verschiedene Domänen verteilen und in universellen Gruppen (siehe nächster Punkt) zusammenfassen.

Verwendungszweck: Globale Gruppen werden für die Organisation von Benutzern verwendet. Sie werden nach unterschiedlichen Gesichtspunkten – Organigramm, Funktion eines Benutzers, etc. – gebildet.

Universelle Gruppen

Diese Gruppen sollten zur Vereinheitlichung von Gruppen verwendet werden, die sich über mehrere Domänen erstrecken. Dabei sollten auf den einzelnen Domänen die Konten in globalen Gruppen zusammengefasst werden. Die globalen

Gruppen können Sie nun in einer universellen Gruppe vereinheitlichen. Dies hat den Vorteil, dass sich Änderungen an den Mitgliedschaften in den globalen Gruppen nicht auf die universelle Gruppe auswirken.

Beachten Sie, dass Sie universelle Gruppen nur einsetzen sollten, wenn sie sich möglichst selten ändern, da diese Gruppen im globalen Katalog gespeichert sind. Dies bedeutet auch, dass Änderungen an dieser Gruppe in der gesamten Struktur repliziert werden. In einem einzigen LAN sollten dabei keine Leistungseinbußen auftreten, bei weiter verzweigten Standorten kann es jedoch zu erheblichen Leistungseinbußen kommen.

Die Gruppen selbst können in jeder Domäne verwendet werden.

Verwendungszweck: Universelle Gruppen werden ausschließlich im Mehrdomänenmodell verwendet. Sie dienen dem Export von Benutzerkonten in fremde Domänen.

5.6.2 Gruppentypen

Zusätzlich zu den Gruppenbereichen ermöglicht Windows Server 2003 auch eine Unterscheidung zwischen zwei verschiedenen Gruppentypen:

Sicherheitsgruppen

Diese Gruppen dienen der Steuerung des Zugriffs auf Ressourcen. Sie sollten nicht als E-Mail-Verteilerlisten verwendet werden.

Beim Anlegen einer neuen Gruppe wird standardmäßig der Gruppentyp Sicherheitsgruppe verwendet.

Verteilergruppen

Diese Gruppen dienen nur als E-Mail-Verteilerlisten oder einfache administrative Gruppierungen. Dieser Gruppentyp kann nicht für die Vergabe von Berechtigungen oder Rechten verwendet werden.

5.6.3 Änderung des Gruppenbereichs

Neu erstellte Gruppen werden standardmäßig als Sicherheitsgruppen mit dem Bereich „Global" angelegt. Dieser Gruppenbereich kann nachträglich, sofern die Domänenfunktionsebene Windows 2000 im einheitlichen Modus oder Windows Server 2003 ist, folgendermaßen geändert werden:

Globale Gruppen in Universelle Gruppen

Nur zulässig, wenn die Gruppe, die Sie ändern möchten, keiner anderen Gruppe mit dem Bereich „Global" angehört.

Lokale Gruppen zu Universellen Gruppen

Die Gruppe, die Sie ändern möchten, darf jedoch keine andere lokale Gruppe enthalten.

Universelle Gruppen zu Globalen Gruppen

Die Gruppe, die Sie ändern möchten, darf jedoch keine andere universelle Gruppe enthalten.

Universelle Gruppen zu Lokalen Gruppen

Keine Beschränkung

© 2005, Microsoft Österreich GmbH

Der Gruppenbereich einer Gruppe kann mittels Active Directory-Benutzer und Computer geändert werden. Klicken Sie hierfür im Kontextmenü der Gruppe auf Eigenschaften.

5.6.4 Planen einer Gruppenstrategie

Erstellen Sie eine lokale Domänengruppe für die gemeinsame Nutzung von Ressourcen. Ermitteln Sie freigegebene Ressourcen wie Drucker, Dateien und Ordner. Erstellen Sie eine lokale Domänengruppe für jede der Ressourcen, fügen Sie Benutzer hinzu, die Zugriff auf die Ressourcen benötigen.

Fügen Sie globale Gruppen hinzu, die Zugriff auf die Ressourcen lokaler Domänengruppen benötigen. Wenn Sie eine Ressource in einer Domäne für mehrere globale Gruppen freigeben möchten, fügen Sie diese globalen Gruppen zur lokalen Domänengruppe hinzu, die Zugriff auf die freigegebene Ressource gewährt.

Verwenden Sie universelle Gruppen, um Zugriff auf Ressourcen in mehreren Domänen zu gewähren. Wenn Benutzerkonten Zugriff auf Dateifreigaben benötigen, die sich nicht in der Domäne der Benutzerkonten befinden, erstellen Sie eine universelle Gruppe für diese Benutzer und gewähren Sie für die Dateifreigaben Zugriff auf die universelle Gruppe.

Verwenden Sie universelle Gruppen bei einer statischen Mitgliedschaft. Universelle Gruppen funktionieren am besten, wenn Sie Benutzer hinzufügen, die wahrscheinlich nur selten aus der universellen Gruppe entfernt werden. Active Directory repliziert alle Änderungen in der Mitgliedschaft einer universellen Gruppe, wodurch der Netzwerkdatenverkehr erhöht wird.

5.6.5 Verschachteln von Gruppen und Vergabe der Berechtigungen

Verwenden Sie Sicherheitsgruppen auf der Grundlage der **A-G-U-DL-P**-Strategie. Diese Strategie bietet die höchste Flexibilität, während sie gleichzeitig die Komplexität beim Zuweisen von Zugriffsberechtigungen zum Netzwerk reduziert. Implementieren Sie darüber hinaus ein rollenbasiertes Sicherheitsmodell für die Erteilung von Berechtigungen.

In der A-G-U-DL-P-Strategie gilt Folgendes:

- Benutzerkonten (A) werden globalen Gruppen (G) hinzugefügt.
- Globale Gruppen werden universellen Gruppen (U) hinzugefügt.
- Universelle Gruppen werden lokalen Domänengruppen (DL) hinzugefügt.
- Ressourcenberechtigungen (P) werden lokalen Domänengruppen zugewiesen.

In einem **Single-Domänen-Modell** werden universelle Gruppen ausgelassen, so dass die Strategie **A-G-DL-P** lautet**.**

5.6.6 Benennungskonvention von Gruppen

Definieren Sie eine Gruppenbenennungskonvention, die den Gruppentyp, den Standort und den Zweck der Gruppe kennzeichnet. Schließen Sie die folgenden Informationen in die Benennungskonvention ein.

Benennungskonvention	Beispiele
Gruppentyp	Dom ..... für eine globale Gruppe Uni ..... für eine universelle Gruppe kein Präfix ..... für eine domänenlokale Gruppe

5.6.7 Manuelles Anlegen einer globalen Gruppe

Um eine globale Gruppe anzulegen, gehen Sie folgendermaßen vor:

1. Starten Sie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
2. Wählen Sie die Organisationseinheit aus, in der Sie eine globale Gruppe anlegen möchten.
3. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit und wählen Sie den Kontextmenüpunkt Neu-Gruppe aus.
4. In dem sich öffnenden Fenster können Sie dann den Namen der globalen Gruppe eingeben. Beachten Sie, dass der Name der Gruppe über den Verzeichnisbaum – Active Directory – der Domäne eindeutig sein muss.

   Sie sollten eine globale Gruppe mit einem Präfix wie z. B. „Dom" oder „Domain" versehen, um sie leichter von den lokalen Gruppen unterscheiden zu können. Darüber hinaus haben Sie dann auch die Möglichkeit, eine gleich lautende domänenlokale Gruppe – ohne Präfix – zu erstellen.

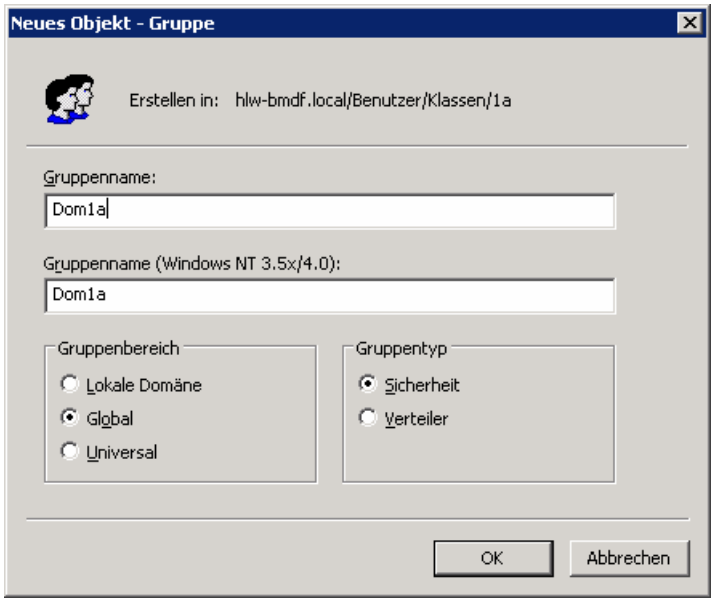


Abb. 56: Anlage einer globalen Gruppe

5. Vergessen Sie nicht, den Gültigkeitsbereich der Gruppe (Global) und den Gruppen-Typ (Sicherheit) zu kontrollieren.

Nach der Anlage der globalen Gruppe können Sie ihr Mitglieder zuweisen. Mitglieder der globalen Gruppe können Benutzer und/oder andere globale Gruppen der Domäne sein.

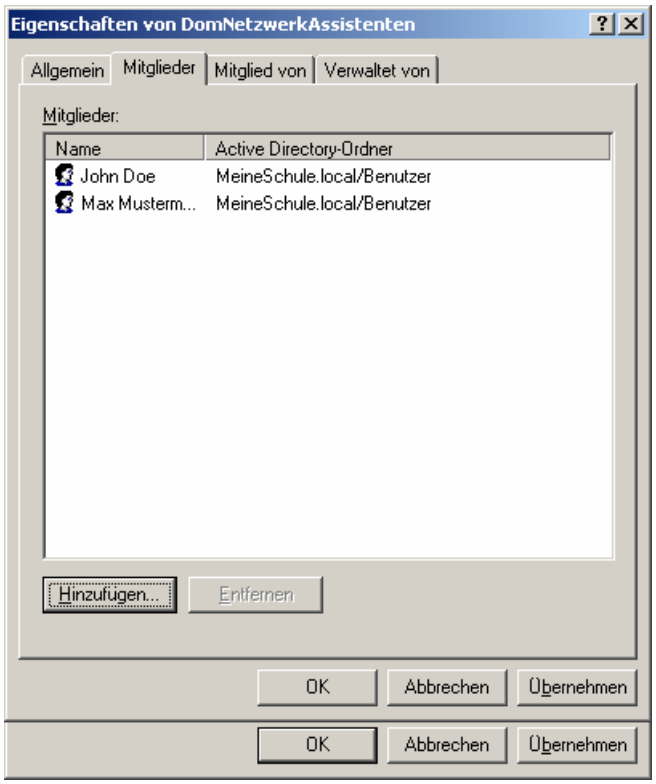


Abb. 57: Register Mitglieder der globalen Gruppe Dom1a

Endlich ist es auch möglich, Benutzer durch **Drag und Drop** Gruppen zuzuweisen. Um einer Gruppe mehrere Benutzer zuzuweisen, müssen Sie diese mittels Shift- oder Strg-Taste markieren. Anschließend positionieren Sie den Mauscursor auf dem Symbol eines der markierten Benutzer und ziehen diesen auf die Gruppe, in der dieser Benutzer Mitglied werden sollen.

© 2005, Microsoft Österreich GmbH

6 Sicherheitsrichtlinien

Dieses Kapitel beschäftigt sich mit Gruppenrichtlinien in einer Domäne.

6.1 Allgemeines

Um grundsätzliche Sicherheitseinstellungen am System vorzunehmen, stellt Windows Server 2003 so genannte Sicherheitsrichtlinien zur Verfügung.

Es gibt sie, je nach Art der Installation, in verschiedenen Varianten:

- Lokale Sicherheitsrichtlinie
- Sicherheitsrichtlinie für Domänen
- Sicherheitsrichtlinie für Domänencontroller

In diesen Sicherheitsrichtlinien können Sie allgemeine Einstellungen zur Benutzung des Servers und der Konten, der Systemdienste, der Ereignisprotokolle, des Dateisystems, der öffentlichen Schlüsseln u. v. a. bestimmen. Die Sicherheitsrichtlinien (Security Policies) sind ein mächtiges Instrument, um für Sicherheit im gesamten Netzwerk zu sorgen.

Editieren Sie jeweils die Sicherheitsrichtlinien für Ihre Serverfunktion. Wenn Sie einen Domänencontroller betreiben, wählen Sie die Sicherheitsrichtlinien für Domänencontroller usw.

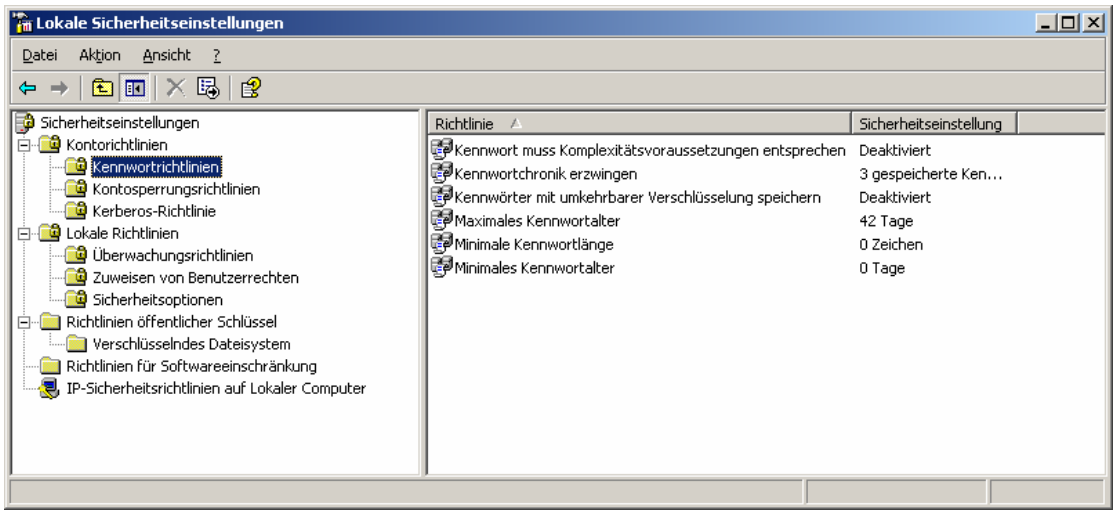


Abb. 58: Die lokalen Sicherheitsrichtlinien

6.1.1 Bearbeiten von Sicherheitsrichtlinien

So bearbeiten Sie die lokalen Sicherheitsrichtlinien:

1. Klicken Sie auf START – AUSFÜHREN.
2. Geben Sie den Befehl ***secpol.msc*** ENTER ein.

Die Managementkonsole zur Bearbeitung der lokalen Sicherheitsrichtlinien wird daraufhin geöffnet. Mit einem Doppelklick auf die jeweilige Richtlinie können Sie diese aktivieren oder deaktivieren.

Sicherheitsrichtlinien für Domänen und Domänencontroller können Sie über START – VERWALTUNG – SICHERHEITSRICHTLINIEN FÜR DOMÄNEN bzw. DOMÄNENCONTROLLER bearbeiten.

Sie können mit Hilfe der Sicherheitsrichtlinien zum Beispiel Kennwortrichtlinien definieren.

Dazu gehören unter anderem folgende Möglichkeiten:

Kennwort muss Komplexitäts-voraussetzungen entsprechen	Wenn Sie diese Richtlinie aktivieren, müssen die Kennwörter, die von den Benutzern gewählt werden, aus mindestens sechs Zeichen bestehen, die weder einen Teil noch den ganzen Benutzernamen enthalten dürfen. Zudem müssen Sie mindestens drei Zeichen aus den folgenden Kategorien enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen.
Kennwortchronik erzwingen	Hier können Sie verhindern, dass Benutzer ihre Kennwörter wiederholen.
Kennwörter mit umkehrbarer Verschlüsselung speichern	Diese Richtlinie ist bei der Verwendung von CHAP-Authentifizierung für Remotezugriffsdienste erforderlich.
Maximales Kennwortalter	Zwingen Sie die Benutzer, ihre Kennwörter in regelmäßigen Abständen zu ändern.
Minimale Kennwortlänge	Geben Sie hier Werte zwischen 1 und 14 ein.
Minimales Kennwortalter	Vor allem in Verbindung mit der Kennwortchronik empfehlenswert. Es verhindert, dass Benutzer ihre Kennwörter zu oft hintereinander ändern.

Neu in Windows Server 2003 sind die Sicherheitsrichtlinien in Verbindung mit drahtlosen Netzwerken, mit denen vor allem eine Verschlüsselung des Netzwerkverkehrs erzwungen werden kann. Sehen Sie sich hierzu den Zweig DRAHTLOSNETZWERKRICHTLINIEN (IEEE 802.11) an.

6.2 Gruppenrichtlinien

6.2.1 Allgemeines

Gruppenrichtlinien sind bereits unter Windows 2000 eingeführt worden und stellen ein leistungsfähiges Werkzeug zur Benutzer-, Computer-, Software- und Windows-Konfiguration dar. Außerdem können in den Gruppenrichtlinien bestimmte „Administrative Vorlagen“ (ADM-Dateien) verwendet werden, um Einstellungen am System vorzunehmen.

Einstellungen zur Software, bzw. zum Verhalten des Betriebssystems, werden im Allgemeinen in der Windows Registry abgelegt. Da diese aber relativ kompliziert aufgebaut ist und man sich in ihr mehr schlecht als recht zurechtfindet, wurde ein Editor geschaffen, in dem man die einzelnen Registrierungsschlüssel geordnet nach Kategorien wieder findet und bearbeiten kann.

Vor allem aber in größeren Netzwerken sind Gruppenrichtlinien von Vorteil, da der Verwaltungsaufwand minimiert wird. In Verbindung mit Active Directory können Gruppenrichtlinien einzelnen Benutzern, Computern und Gruppen zugewiesen

werden, die sich in einer Organisationseinheit befinden. Gruppenrichtlinien werden nach unten vererbt. Wurden mehrere Gruppenrichtlinien definiert, so werden diese in einer vorgegebenen Reihenfolge abgearbeitet.

6.2.2 Reihenfolge der Abarbeitung von Gruppenrichtlinien

1. Zuerst tritt die lokale Gruppenrichtlinie in Kraft.
2. Danach folgen die Gruppenrichtlinien für den Standort.
3. Hierauf folgen die Gruppenrichtlinien für die Domäne.
4. Als letztes werden die Gruppenrichtlinien für die Organisationseinheit angewendet.

Das heißt: Gruppenrichtlinien schreiben ihre Werte in die Registry. Später ausgeführte Gruppenrichtlinien überschreiben die vorher definierten Werte.

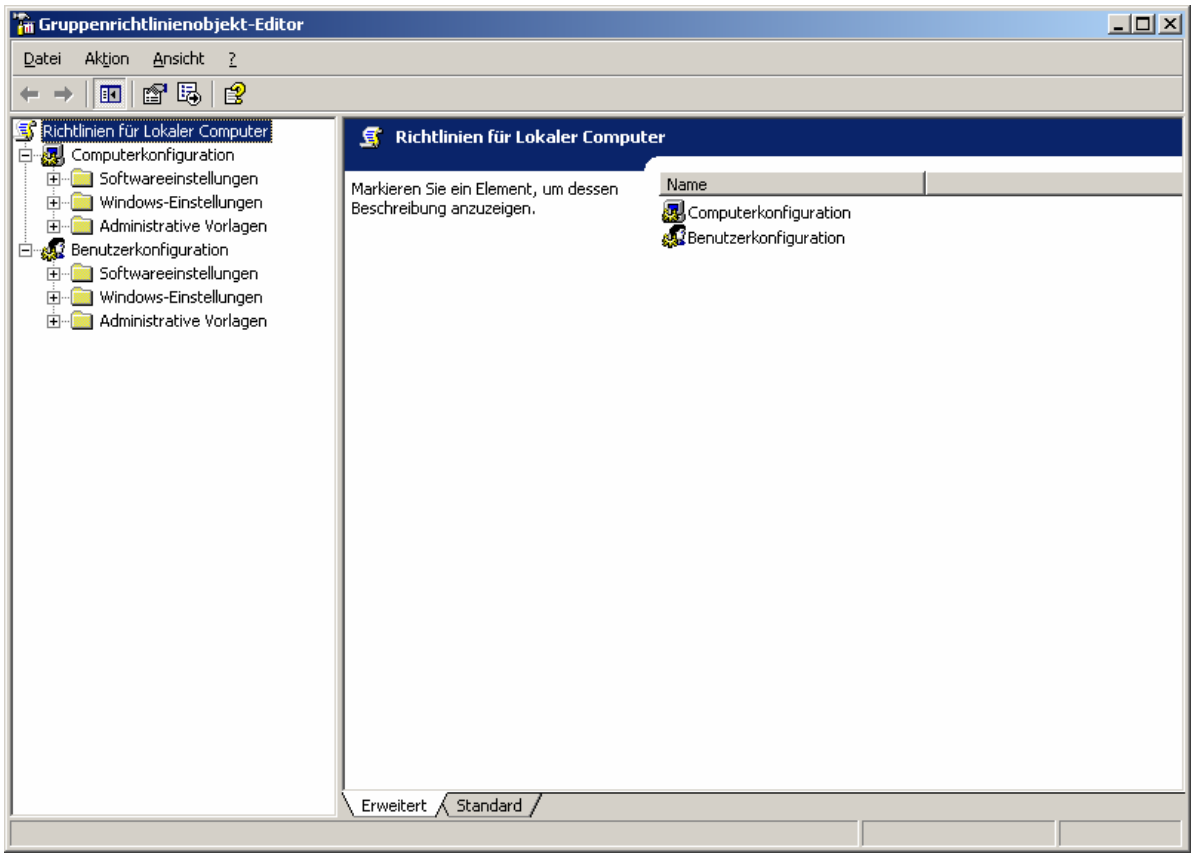


Abb. 59: Die Gruppenrichtlinien-Managementkonsole

6.2.3 Aufbau einer Gruppenrichtlinie

Bei den Gruppenrichtlinien wird prinzipiell zwischen Computer- und Benutzerkonfiguration unterschieden. Diese zwei Teilbereiche haben jedoch denselben Aufbau:

Softwareeinstellungen	Bei der lokalen Gruppenrichtlinie kommt dieser Richtliniensatz nicht zum Tragen, in einer Domäne jedoch kann hier Software definiert werden, die automatisch beim Systemstart, bzw. bei der ersten Anforderung des Benutzers installiert wird.
Windows-Einstellungen	Enthält Einstellungen zu Benutzern und Computern. Hier können Sie bei der Benutzerkonfiguration auch die Ordnerumleitung konfigurieren. (Sie müssen sich in einer Active-Directory-Domäne befinden).
Administrative Vorlagen	Dieser Ordner enthält bestimmte Vorlagendateien, die den Zugriff auf ausgewählte Registry-Schlüssel beinhalten. Sie finden diese Vorlagendateien in folgendem Verzeichnis: %Windir%\System32\GroupPolicy\Adm Solche Vorlagendateien können auch selbst erstellt werden, und im Internet finden Sie weitere Vorlagendateien, die die Konfigurationsmöglichkeiten erweitern.

Zu jeder Vorlagendatei finden Sie eine ausführliche Hilfedatei im Verzeichnis %Windir%\Help. So z. B.: Inetres.chm, System.chm, Conf.chm und Wmplayer.chm. Geben Sie hierzu einfach bei der Eingabeaufforderung %WINDIR%\HELP\<HILFEDATEI> ein.

Die lokalen Gruppenrichtlinien werden normalerweise auf Clientrechnern definiert, da diese Richtlinien nur gelten, wenn Benutzer sich direkt am Computer anmelden. Dies sollte aber bei den wenigsten Servern der Fall sein.

So bearbeiten Sie die lokalen Gruppenrichtlinien:

1. Klicken Sie auf START – AUSFÜHREN.
2. Geben Sie ***gpedit.msc*** ein und klicken Sie auf OK.
3. Sie können nun die lokale Gruppenrichtlinie bearbeiten.
4. Schließen Sie den Gruppenrichtlinienobjekt-Editor.

Nach der Bearbeitung der Gruppenrichtlinie sollte auch sichergestellt werden, dass sie angewendet wird.

Standardmäßig wird für Gruppenrichtlinien ein Aktualisierungsintervall definiert, so dass sie automatisch aktualisiert werden. Um die Aktualisierung erzwingen zu können, stellt Windows Server 2003 ein eigenes Befehlszeilenprogramm zur Verfügung.

So aktualisieren Sie eine Gruppenrichtlinie sofort:

1. Klicken Sie auf START - AUSFÜHREN.
2. Geben Sie den Befehl CMD ENTER ein.
3. Bei der Eingabeaufforderung geben Sie ***gpupdate*** ENTER ein.

Sobald mehrere Gruppenrichtlinien angewendet werden, kann es sehr schwierig sein, die geänderten Werte und Einstellungen wieder zu finden. Sie können sich mit der Managementkonsole ***rsop.msc*** den Richtlinienergebnissatz anzeigen lassen, der nur noch die tatsächlich geänderten Werte enthält.

So zeigen Sie den Richtlinienergebnissatz an:

1. Klicken Sie auf START - AUSFÜHREN.
2. Geben Sie ***rsop.msc*** ENTER ein.
3. Schließen Sie das Fenster.

Zur Analyse der verwendeten Richtlinien existiert ein weiteres Befehlszeilenwerkzeug: GPRESULT.

So verwenden Sie gpresult:

1. Starten Sie die Kommandozeilenkonsole über START – AUSFÜHREN – CMD ENTER
2. Geben Sie bei der Eingabeaufforderung den Befehl ***gpresult /v*** ENTER ein.
3. Sie können die Ergebnisse mit dem „>“ Zeichen bei der Befehlseingabe in eine Datei umleiten.

Angenehmer ist die Anzeige als HTML-Datei. Diese Ansicht des Gruppenrichtlinienergebnissatzes ist über das Hilfe- und Supportcenter erreichbar.

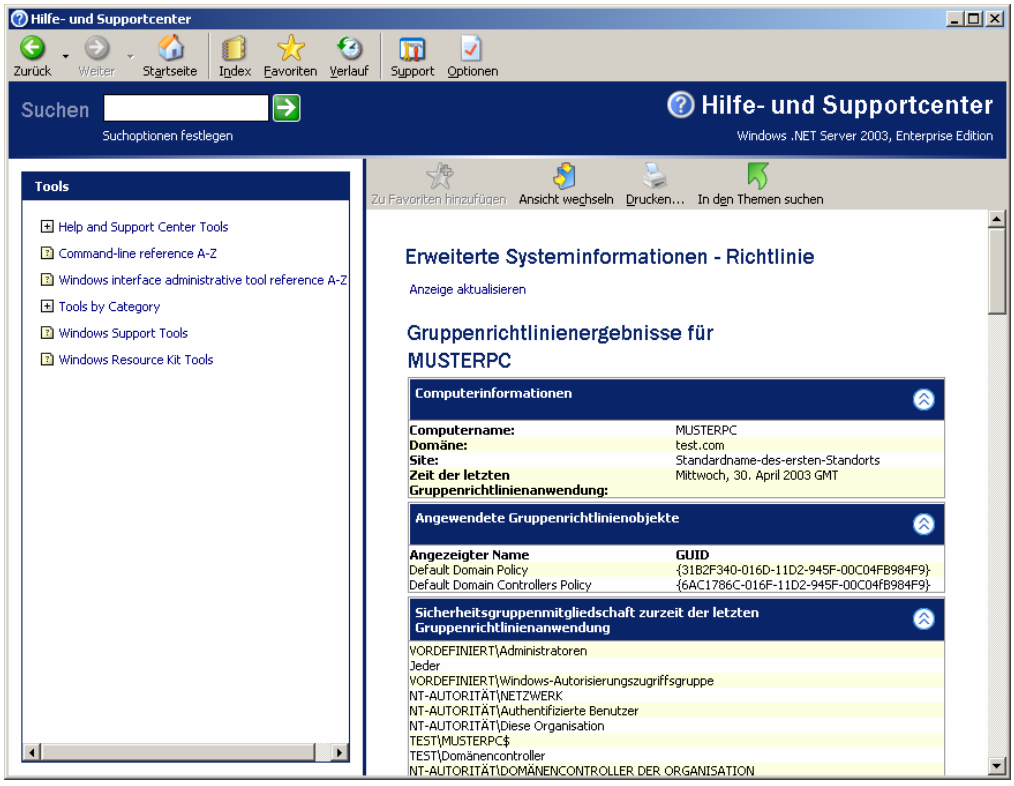


Abb. 60: Die angewendeten Gruppenrichtlinien im Hilfe- und Supportcenter

So zeigen Sie die HTML-Ansicht der Gruppenrichtlinienergebnisse an:

1. Klicken Sie auf START – HILFE UND SUPPORT.
2. In der Kategorie SUPPORTAUFGABEN wählen Sie beim Punkt TOOLS die SYSTEMINFORMATIONEN.
3. Klicken Sie auf ERWEITERTE SYSTEMINFORMATIONEN anzeigen.
4. Klicken Sie auf ANGEWENDETE GRUPPENRICHTLINIENEINSTELLUNGEN ANZEIGEN.

7 Zugriffsberechtigungen – Shares

Dieses Kapitel erläutert die Konfiguration von Zugriffsberechtigungen und Freigaben unter Windows Server 2003.

7.1 Überblick – Definition

Nach der Installation eines Servers oder Domänencontrollers kann kein Benutzer des Netzwerks auf Ressourcen der Server zugreifen, da nur Administratoren und Operatoren zur lokalen Anmeldung an einem Server berechtigt sind.

Damit Netzwerkbenutzer Ressourcen auf einem Server ablegen oder auf diese zugreifen können, muss der Administrator Ressourcen freigeben. Freigegebene Ordner und ihre Dateien und Unterordner sind durch Zugriffsberechtigungen geschützt.

Die **effektive Berechtigung** eines Benutzers auf einen Ordner setzt sich dabei aus zwei unterschiedlichen Berechtigungen zusammen:

- NTFS-Berechtigung einer Datei oder eines Ordners
- Freigaberecht der Ressource

7.2 NTFS-Berechtigungen

Bei der Installation des Betriebssystems muss das Dateisystem ausgewählt werden. Als Standard wird dabei das Windows Server 2003-eigene Dateisystem **NTFS** (New Technology File System) vorgeschlagen. Sie haben sich damit für ein stabiles, transaktionsorientiertes Dateisystem entschieden, das auch weitere Funktionen gewährleistet, wie z. B. Berechtigungen auf Dateien und Ordner oder die Möglichkeit, Zugriffe auf Daten zu überwachen.

Es stellt sich die Frage, warum Sie überhaupt Berechtigungen vergeben sollten? Berechtigungen dienen dem Schutz von Dateien, Ordnern oder Netzwerkressourcen. Mit ihnen erlaubt man Gruppen oder Benutzern, übers Netzwerk oder lokal auf Ressourcen zuzugreifen. So ist es z. B. möglich, einen bestimmten Benutzer zu berechtigen, eine bestimmte Datei lediglich zu lesen.

Berechtigungen werden im Dateisystem selbst gespeichert. Derartige Einträge nennt man ACE (**Access Control Entry**), die sich daraus ergebende Liste heißt ACL (**Access Control List**).

Bei der Erstellung eines Ordners oder einer Datei wird der Benutzer, der das Objekt anlegt, als **Besitzer des Objekts** eingetragen.

Der Besitz eines Objekts ist ein wichtiges Attribut, das ein Benutzer auf eine Ressource haben kann. Der Besitzer einer Ressource entscheidet nämlich, wer mit welcher Berechtigung auf sie zugreifen kann.

Aus einer Vielzahl von Einzelberechtigungen wurden **Standardberechtigungen** definiert, die der Administrator oder Besitzer eines Objekts vergeben kann.

- **Lesen**: Lesen einer Datei sowie Anzeige der Dateiattribute, der Berechtigungen und des Besitzers.
- **Schreiben**: Mit dieser Berechtigung kann die Datei überschrieben werden. Daneben werden auch Besitz und Berechtigungen angezeigt.
- **Lesen, Ausführen**: Diese Berechtigung ist notwendig, um Programme ausführen, also starten zu können.
- **Ändern**: Neben dem Lesen, Schreiben, Ausführen umfasst diese Berechtigung noch das Ändern und Löschen von Objekten wie z. B. einer Datei oder eines Ordners.

© 2005, Microsoft Österreich GmbH

- **Vollzugriff**: Diese Berechtigung ist die höchstmögliche, sie enthält alle anderen Berechtigungen und erlaubt die Übernahme des Besitzes an einem Objekt.

Ordner-Berechtigungen schließen, im Gegensatz zu Datei-Berechtigungen, die Option **Ordnerinhalte auflisten** ein. Durch diese Berechtigung werden die Dateien in einem Ordner und die Unterordner des Ordners aufgelistet.

Vergabe von Berechtigungen

Der Grund für diese Vorgangsweise ist, dass in einem Netzwerk mehr Benutzer als Gruppen angelegt sind. Gruppen werden meist nach **logischen, funktionellen, organisatorischen Gesichtspunkten** gebildet. Benutzer, die einer bestimmten Gruppe angehören, haben damit auch identische Zugriffsberechtigungen.

Wenn Sie die Berechtigungen einsehen oder ändern möchten, müssen Sie das gewünschte Objekt im Dateisystem auswählen und durch einen Rechtsklick das Kontextmenü aufrufen. In dem sich öffnenden Menü wählen Sie die Funktion **EIGENSCHAFTEN** aus.

In dem sich öffnenden Fenster wechseln Sie in das Register SICHERHEIT, in dem Sie die Berechtigungen des Objekts einsehen bzw. ändern können.

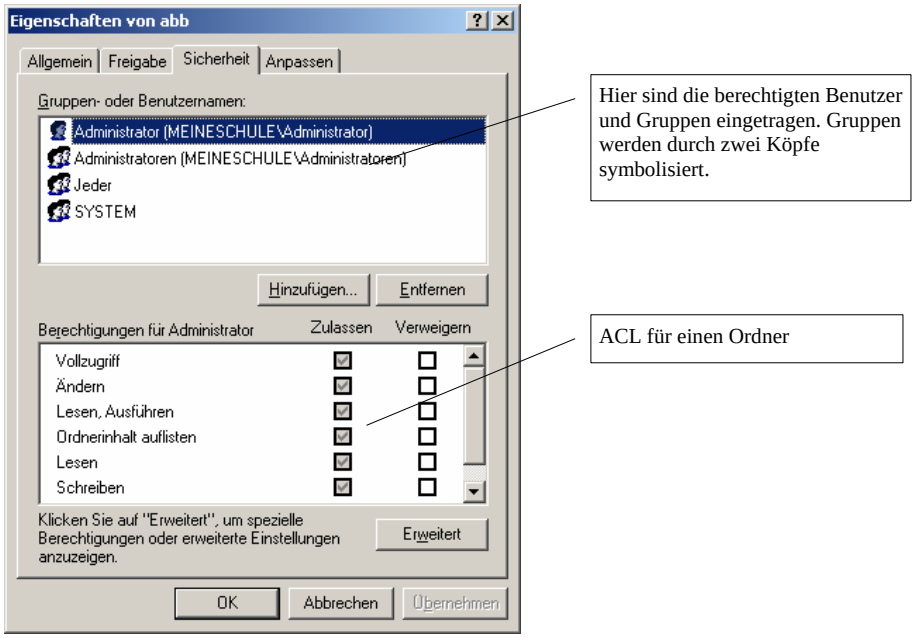


Abb. 61: Anzeige der Sicherheitseinstellungen eines Ordners

Windows Server 2003 arbeitet mit vererbbaren Berechtigungen, d. h. ein Objekt erbt die Berechtigungen des darüber liegenden Ordners. Ein neu erstellter Ordner erbt die Berechtigungen des übergeordneten Ordners.

Ob eine Berechtigung vererbt wurde oder nicht, können Sie leicht an den abgehakten Kontrollboxen ersehen. Vererbte Berechtigungen werden auf einer Workstation angehakt und deaktiviert angezeigt. An einem Windows Server 2003 werden sie angehakt und grau unterlegt dargestellt. In beiden Fällen können Sie die Berechtigungen nicht unmittelbar ändern.

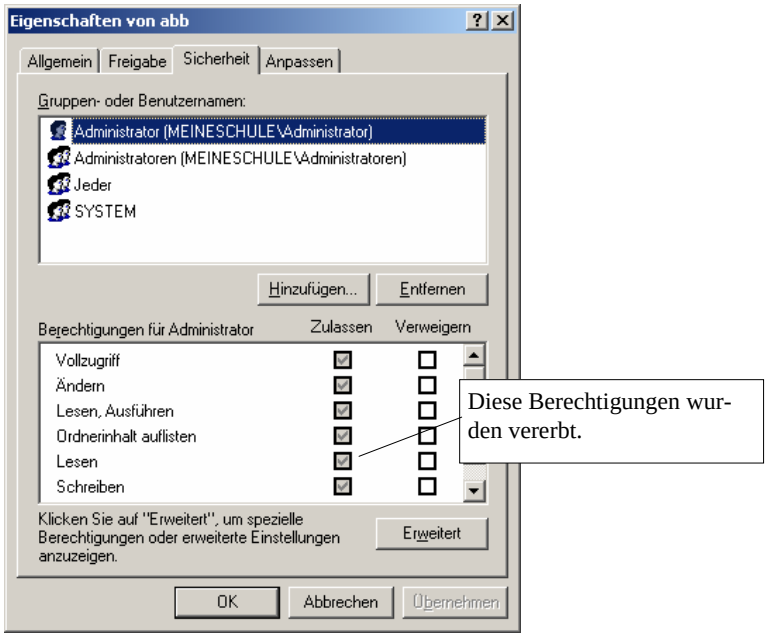


Abb. 62: Eigenschaften eines Ordners

Um die Berechtigung der Gruppe „Benutzer“ zu ändern, muss zuerst die Vererbung ausgeschaltet werden. Mit einem Klick auf die Schaltfläche ERWEITERT gelangen Sie in die erweiterten Sicherheitseinstellungen des Ordners. Im unteren Abschnitt des Fensters muss die Kontrollbox BERECHTIGUNGEN ÜBERGEORDNETER OBJEKTE, SOFERN VERERBBAR, ÜBER ALLE UNTERGEORDNETEN OBJEKTE VERBREITEN. DIESE OBJEKTE INKLUSIVE DEN HIER DEFINIERTEN EINTRÄGE MIT EINBEZIEHEN leer sein. (siehe Abb. 63).

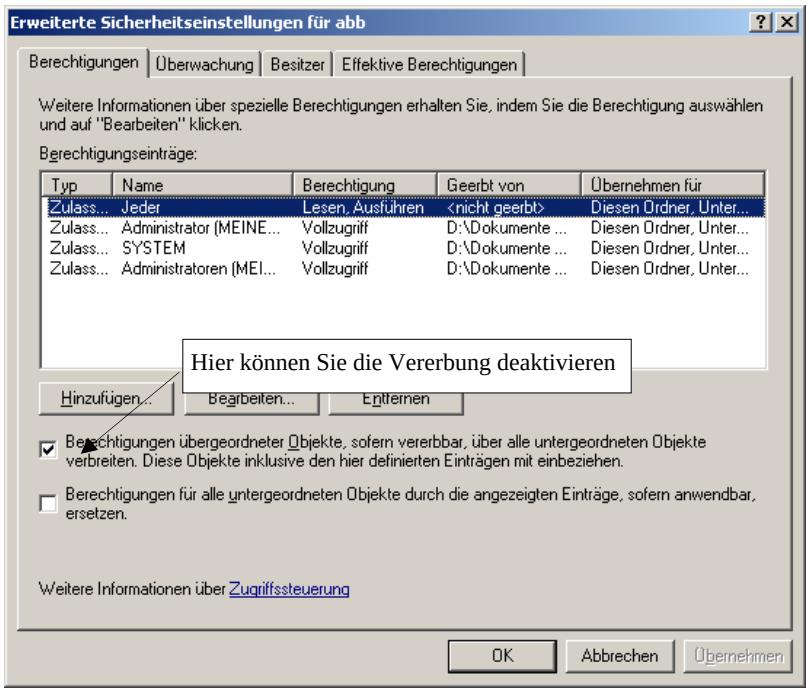


Abb. 63: Erweiterte Sicherheitseinstellungen eines Ordners

Nach dem Klick auf die Kontrollbox erhalten Sie eine Warnmeldung des Betriebssystems, dass von nun an keine Vererbung mehr stattfindet. Je nachdem, ob Sie die vererbten Rechte übernehmen oder alle Sicherheitseinstellungen für diesen Ordner löschen möchten, müssen Sie entweder die Schaltfläche KOPIEREN oder ENTFERNEN anklicken.

Welche Berechtigungen im Einzelnen durch das Setzen der Kontrollbox einer Standardberechtigung wirklich vergeben werden, können Sie im oberen Teil des Fensters ersehen. Wenn Sie einen detaillierten Überblick wünschen, müssen Sie lediglich den Benutzer oder die Gruppe anklicken und anschließend die Schaltfläche BEARBEITEN ... wählen.

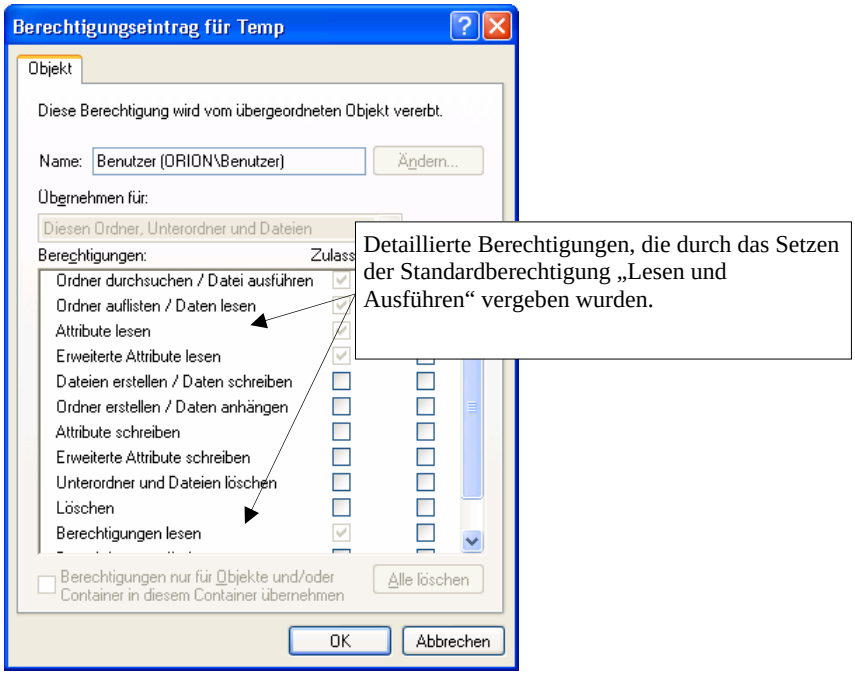


Abb. 64: Berechtigungseintrag für eine bestimmte Gruppe (Screenshot einer Workstation)

Die effektive Berechtigung eines Benutzers setzt sich aus den einzelnen Berechtigungen zusammen, die er durch die Mitgliedschaft in unterschiedlichen Gruppen erhalten hat. Alle Berechtigungen addieren sich, wobei das Verweigern der Berechtigung eine höhere Priorität hat als das Zulassen!

Unter Windows Server 2003 haben Sie endlich die Möglichkeit, die effektiven Berechtigungen eines Benutzers oder einer Gruppe sofort zu ermitteln.

Im Register EFFEKTIVE BERECHTIGUNGEN des Fensters „Erweiterte Sicherheitseinstellungen für ...“ können Sie sofort die effektiven Berechtigungen ermitteln. Nachdem Sie auf das Register geklickt haben, müssen Sie über die Schaltfläche AUSWÄHLEN... den Benutzer oder die Gruppe eingeben, für die Sie die effektiven Berechtigungen ermitteln möchten.

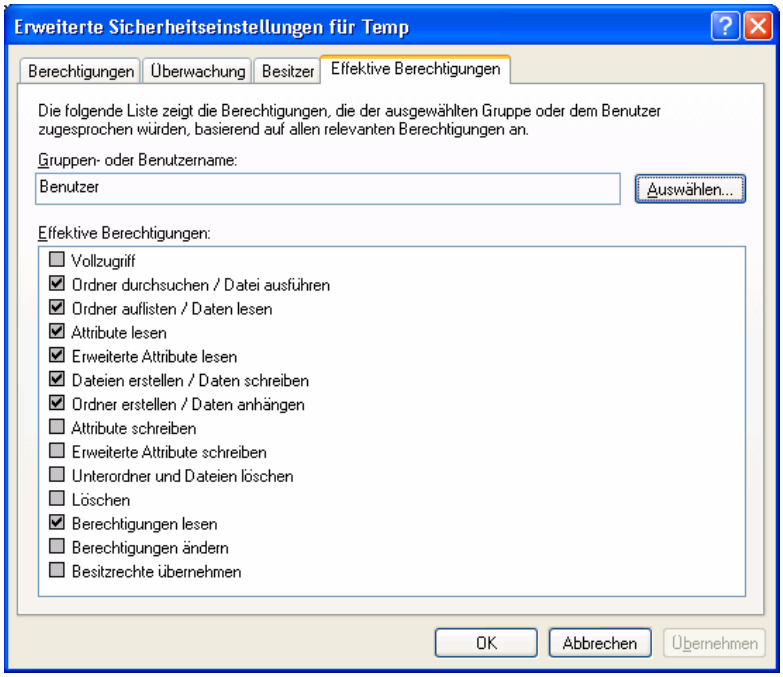


Abb. 65: Effektive Berechtigungen der Gruppe „Benutzer" für einen bestimmten Ordner

Üblicherweise haben Dateien durch Vererbung die Berechtigung des übergeordneten Ordners. Dies kann allerdings auch geändert werden. Die Zugriffsberechtigung auf eine Datei kann ausgedehnt oder auch eingeschränkt werden!

7.3 Freigabe einer Ressource - Berechtigungen

Wie bereits eingangs erwähnt müssen Ressourcen durch den Administrator freigegeben werden, damit Benutzer auf sie zugreifen können.

Standardmäßig sind für Administratoren für jedes Laufwerk administrative Freigaben definiert, die jeweils die Bezeichnung des Datenträgers gefolgt von einem Dollarzeichen ($) tragen. So ist Datenträger C: über die administrative Freigabe C$ erreichbar.

Versteckte Freigaben

Freigabenamen, die mit $ enden, werden den Benutzern im Windows Explorer nicht angezeigt, eine Verbindung kann aber trotzdem hergestellt werden.

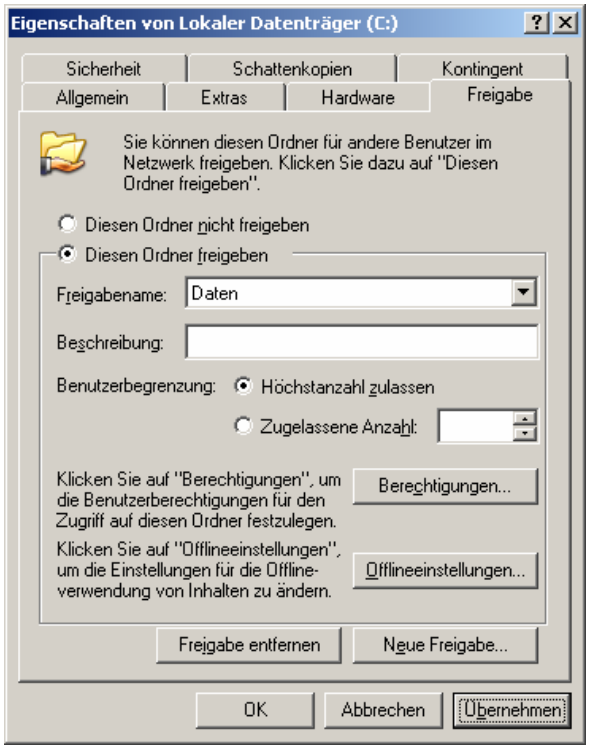


Abb. 66: Freigabe von Ordnern

Bei der Freigabe eines Ordners können folgende Berechtigungen erteilt werden:

- **Lesen**: Diese Berechtigung ist die Standardberechtigung in der Gruppe „Jeder". Sie ermöglicht es Benutzern, sich Datei- und Unterordnernamen und Daten in Dateien anzusehen und Programme auszuführen.
- **Ändern**: Das Ändern ist in keiner Gruppe eine Standardberechtigung. Es gelten sowohl die Berechtigungen von Lesen und zusätzlich das Hinzufügen von Dateien und Unterordnern, das Ändern der Dateiinhalte und das Löschen von Ordnern und Dateien.
- **Vollzugriff**: Dies ist die lokale Standardberechtigung der Gruppe „Administratoren". Sie ermöglicht neben allen Berechtigungen zum Lesen und Ändern auch die Möglichkeit zum Ändern der NTFS-Berechtigungen.

In der Produktfamilie Windows Server 2003 erhält die Gruppe **Jeder** in einer neuen freigegebenen Ressource automatisch die Berechtigung **Lesen** (die Berechtigung mit der stärksten Einschränkung).

Bei den vorherigen Versionen des Windows Server war das Standard-Freigaberecht mit **Jeder/Vollzugriff** definiert.

Die Änderung ist eine Folge der Microsoft-Initiative „Trustworthy Computing" und soll den Zugriff auf Ressourcen sicherer machen.

In der Praxis ist diese Vorgehensweise jedoch nicht praktikabel, Sie sollten gleich beim Erstellen der Freigabe die Gruppe „Jeder" aus der Freigabeberechtigung durch Authenticated Users ersetzen. Wenn Sie der Gruppe zusätzlich das Freigaberecht Vollzugriff einräumen, können Sie, so wie früher, die effektive Berechtigung durch die NTFS-Datei- und Ordnerberechtigungen vergeben.

© 2005, Microsoft Österreich GmbH

Beachten Sie bitte, dass es einen wesentlichen Unterschied darstellt, ob eine Gruppe in der Liste der Freigabeberechtigungen eingetragen ist oder nicht.

Hat ein Benutzer oder eine Gruppe keine Freigaberechte auf einem Ordner, so kann er sich nicht einmal mit dieser Ressource verbinden.

7.3.1 Manuelle Freigabe eines Ordners

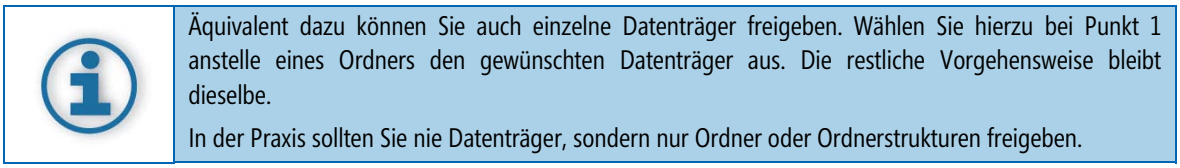
So geben Sie einen Ordner frei:

1. Wählen Sie im Windows Explorer einen Ordner aus.
2. Aus dem Kontextmenü des Elements wählen Sie FREIGABE UND SICHERHEIT.
3. Aktivieren Sie den Reiter FREIGABE.
4. Klicken Sie auf NEUE FREIGABE.
5. Geben Sie den Freigabenamen und eine Beschreibung an.
6. Mit dem Befehl BERECHTIGUNGEN... können Sie die Zugriffsberechtigungen für die Freigabe definieren.

   Standardmäßig erhält die Gruppe „Jeder" bei einer neuen Freigabe eine Nur-Lese-Berechtigung.
7. Klicken Sie auf OK.
8. Klicken Sie auf ÜBERNEHMEN, wenn Sie weitere Freigaben definieren möchten, ansonsten auf OK, um das Freigabefenster zu schließen.

Nachdem Sie den Ordner freigegeben haben, können sich die Netzwerkbenutzer mit Berechtigung zu dieser Freigabe verbinden.

Im Windows Explorer sind die Freigaben mit einer Hand unter dem Symbol der entsprechenden Ressource gekennzeichnet.



Äquivalent dazu können Sie auch einzelne Datenträger freigeben. Wählen Sie hierzu bei Punkt 1 anstelle eines Ordners den gewünschten Datenträger aus. Die restliche Vorgehensweise bleibt dieselbe.

In der Praxis sollten Sie nie Datenträger, sondern nur Ordner oder Ordnerstrukturen freigeben.

7.3.2 Entfernen einer Freigabe

Mit dem Entfernen einer Freigabe können Sie die Zugriffsberechtigung auf einen Ordner wieder aufheben.

So entfernen Sie eine Freigabe:

1. Wählen Sie im Windows Explorer eine Freigabe.
2. Öffnen Sie aus dem Kontextmenü den Befehl FREIGABE UND SICHERHEIT.
3. Aus dem Reiter FREIGABE wählen Sie in der Auswahlliste den entsprechenden FREIGABENAMEN.
4. Klicken Sie auf FREIGABE ENTFERNEN.

Die Berechtigungen, die Sie für Freigaben setzen können, beschränken sich auf Vollzugriff, Änderungen und Lesezugriff. Zusätzlich haben Sie aber die Möglichkeit, die Zugriffsbeschränkungen im Dateisystem über die Eigenschaften zu bearbeiten.

© 2005, Microsoft Österreich GmbH

Wenn Sie selbst eine Verbindung zu einer Freigabe herstellen möchten, können Sie dies über das Kontextmenü der Netzwerkumgebung erreichen.

So stellen Sie eine Verbindung zu einem Netzlaufwerk her:

1. Klicken Sie auf START.
2. Zeigen Sie auf ARBEITSPLATZ und drücken Sie die rechte Maustaste.
3. Klicken Sie auf NETZLAUFWERK VERBINDEN. . . .

Das Dialogfenster Netzlaufwerk verbinden wird angezeigt.

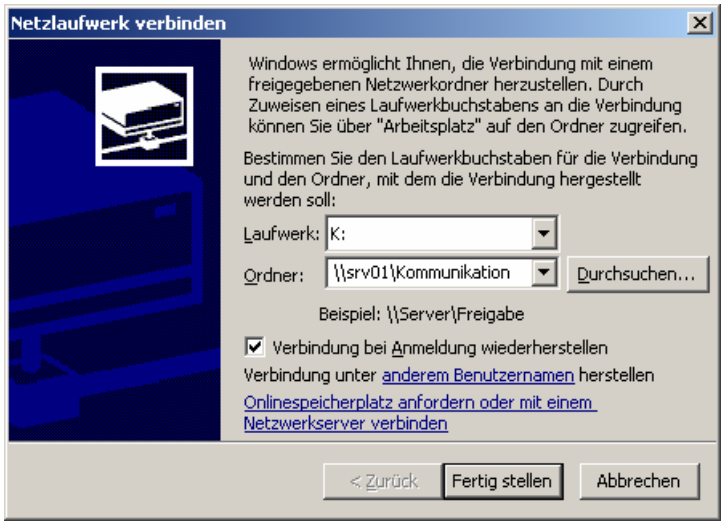


Abb. 67: Dialogfenster "Netzlaufwerk verbinden"

4. Wählen Sie einen Laufwerksbuchstaben und geben Sie den Freigabenamen im Feld „Ordner" an. Sie können auch nach einer Freigabe suchen, indem Sie DURCHSUCHEN. . . anklicken.

   Die Angabe des Ordners muss in UNC-Notation geschehen, z. B:
   \\<servername\<freigabename>
5. Wenn Sie die Verbindung unter einem anderen Benutzernamen herstellen wollen, klicken Sie auf den Link ANDERER BENUTZERNAMEN.
6. Klicken Sie auf FERTIGSTELLEN.

Die Anzahl und Namen der freigegebenen Ordner sowie Informationen über deren Benutzung können Sie über die Computerverwaltung herausfinden.

So betrachten Sie die freigegebenen Ordner und Dateien:

1. Klicken Sie auf START – VERWALTUNG – COMPUTERVERWALTUNG.
2. Wählen Sie den Ordner FREIGEGEBENE ORDNER unter dem Zweig System.

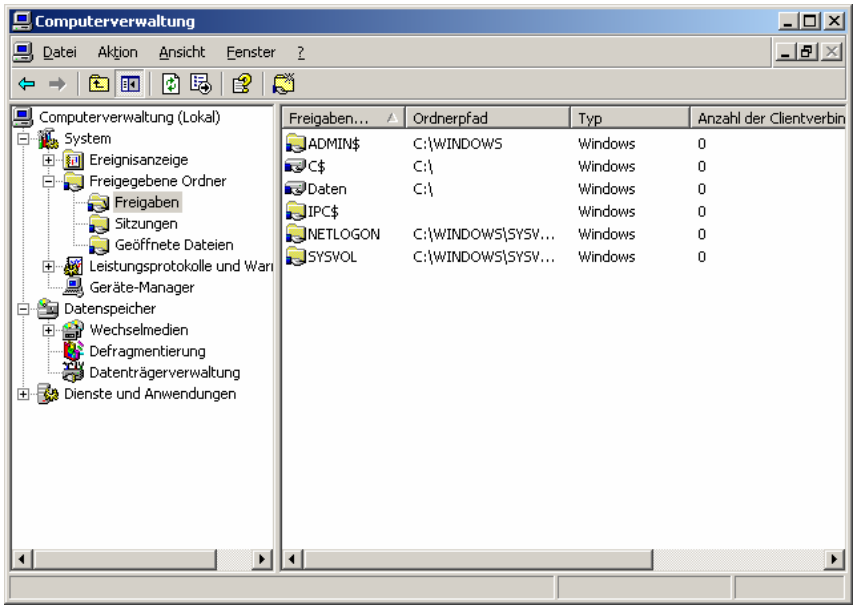


Abb. 68: Freigegebene Ordner anzeigen

3. Sie können die entsprechenden Freigaben, Sitzungen und die Namen der geöffneten Dateien betrachten, sofern gewünscht die Freigaben aufheben und Verbindungen trennen. Dies geschieht jeweils durch Markieren einer Freigabe und der Verwendung des Menüpunktes AKTION.
4. Schließen Sie die Computerverwaltung.

Die Computerverwaltung können Sie auch über das Kontextmenü des ARBEITSPLATZ - Symbols erreichen. Wählen Sie dort den Menüeintrag VERWALTEN.

Im Active Directory müssen freigegebene Ordner im Verzeichnis veröffentlich werden. Dies geschieht über die „Active Directory-Benutzer und -Computer"-Managementkonsole.

7.3.3 Freigaben im Active Directory

So veröffentlichen Sie eine Freigabe im Active Directory:

1. Öffnen Sie die ACTIVE DIRECTORY-BENUTZER UND –COMPUTER-Konsole über START – VERWALTUNG.
2. Markieren Sie Ihre Domäne und klicken Sie im Menü AKTION auf den Eintrag NEU.
3. Klicken Sie auf FREIGEGEBENER ORDNER.

4. Sie werden zur Eingabe des Namens und des Netzwerkpfads aufgefordert. Geben Sie einen entsprechenden Freigabenamen ein und klicken Sie abschließend auf OK.

7.3.4 Spezielle Freigaben

Unter Windows Server 2003 werden je nach Konfiguration des Computers einige weitere spezielle freigegebene Ressourcen zu Verwaltungszwecken angelegt. Es wird empfohlen, diese nicht zu löschen oder zu ändern. Die nachfolgenden freigegebenen Ressourcen werden zwar im Windows Explorer unter dem Arbeitsplatz nicht angezeigt, können jedoch mit Hilfe des Dienstprogramms „Freigegebene Ordner" angezeigt werden:

Laufwerksbuchstabe$
Dieser stellt die administrative Freigabe dar, mit der Administratoren eine Verbindung zum Stammverzeichnis eines Laufwerks herstellen können.

ADMIN$
Dient zur Remoteverwaltung eines Rechners. Der Pfad bezieht sich immer auf das Systemstammverzeichnis (z. B. C:\Windows)

IPC$
Diese Ressource dient zum Freigeben der Named Pipes, sie für die Kommunikation zwischen Programmen erforderlich sind. Des Weiteren wird IPC$ während der Remoteverwaltung zum Anzeigen der auf dem Rechner freigegebenen Ressourcen verwendet. Diese Freigabe kann nicht gelöscht werden.

NETLOGON
Diese Freigabe ist auf Domänencontrollern erforderlich.

PRINT$
Wird bei der Remoteverwaltung von Druckern verwendet.

FAX$
Wird von Faxclients zum Senden von Faxen verwendet. Dient hauptsächlich als Zwischenspeicher und zur Ablage von Deckblättern.

Wenn Sie die Berechtigungen für die oben genannten, speziell freigegebenen Ressourcen geändert haben, können die Standardeinstellungen möglicherweise wieder hergestellt werden, wenn Sie den Serverdienst beenden und neu starten.

8 Einrichten von Clients

Dieses Kapitel erläutert Möglichkeiten für eine automatisierte Einrichtung und Verwaltung von Clients innerhalb eines Netzwerks mit Windows Server 2003.

8.1 Überblick – Definition

Das Aufsetzen einer großen Zahl von Clientrechnern ist manuell nicht zu bewältigen, die manuelle Installation wäre viel zu zeitaufwendig. Für derartige „Deployment Szenarien" sollten andere Hilfsmittel genutzt werden.

Außerdem ist zu berücksichtigen, dass es im Schulbetrieb möglich sein muss, einen Clientrechner oder einen ganzen EDV-Saal jederzeit und ohne viel Aufwand wieder aufzusetzen. Mit vorausschauenden Überlegungen und wenigen Vorarbeiten spart der Administrator später viel kostbare Arbeitszeit.

Für das Einrichten von Clients stehen dem Administrator im Wesentlichen vier Möglichkeiten zur Verfügung:

- Manuelle Installation mit einer CD
- Unattended (unbeaufsichtigtes) Setup über das Netzwerk mit Hilfe von vordefinierten Antwortdateien
- Klonen von Clientrechnern mit Hilfe von Software eines Drittanbieter (z. B. Ghost) unter Verwendung von Sysprep.exe
- Aufsetzen von Clientrechnern mittels Remote Installation Services (RIS)

Alle diese Installationsmethoden haben Vor- und Nachteile:

Methode	Vorteil	Nachteil
Manuelle Installation	Einfache Durchführung ohne Vorbereitung.	Die Installation muss auf jedem Computer mit einer CD lokal erfolgen.
Unattended Setup	Die Installation ist von jedem Computer aus möglich, der Netzwerkzugriff hat. Unterschiedliche Hardware kann eingesetzt werden.	Üblicherweise wird diese Installation über das Netzwerk durchgeführt (sie wäre aber auch mit CD und einer Antwortdatei auf Diskette möglich). Dazu müssen auf dem Server alle Installationsdateien (CD) abgelegt sein. Die Installation kann relativ lange dauern (normale Installationsdauer). Sofern auch Anwendungen installiert werden sollen, benötigen auch diese die Möglichkeit eines unattended Setup.
Klonen	Effizienteste und schnellste Möglichkeit, einen Client aufzusetzen.	Auf dem Server wird Speicherplatz für das Image benötigt. Klon-Software eines Drittanbieters ist notwendig.

RIS	Kann von einem Server aus zentral bereitgestellt werden.	Eine spezielle Hardware (Netzwerkkarte) ist erforderlich. Außerdem ist Speicherplatz auf dem Server erforderlich, eine umfangreiche Vorbereitung notwendig.

In dieser Anleitung wird dabei in erster Linie auf die dritte Möglichkeit (Klonen eines Clientrechners) eingegangen, da diese Methode für den Schulbetrieb am effizientesten ist. Nähere Informationen zu RIS sind im Anhang C beschrieben.

8.2 Klonen eines Clientrechners

8.2.1 Voraussetzungen

Ab Windows 2000 wurde in dieser Betriebssystemgeneration ein voll funktionsfähiges Plug-and-play-System integriert. Es bewirkt, dass das Klonen von Clientrechnern keine absolut identische Hardware mehr benötigt. Einzig die folgenden Komponenten des Master- und Zielcomputers müssen identisch sein:

- HAL (Hardware Abstraction Layer)
- ACPI-Unterstützung (Advanced Configuration and Power Interface)
- Treiber für Massenspeichergeräte

Sollten Computer vorhanden sein, bei denen diese Komponenten sich unterscheiden, müssen mehrere Abbilder (Images) bereitgestellt werden.

Um einen Clientrechner mit dieser Methode installieren zu können, ist ein funktionsfähiges Image erforderlich. Wie Sie dieses Image korrekt erstellen, wird im Folgenden beschrieben.

Zusätzlich ist ein Klon-Programm von einem Drittanbieter erforderlich, da weder das Serverbetriebssystem noch das Clientbetriebssystem von Windows eines enthalten. Zu den bekanntesten Klon-Programmen auf dem Markt zählen:

- Symantec Ghost (http://www.symantec.com/ghost)
- PowerQuest DriveImage (http://www.powerquest.com/driveimage/)

8.2.2 Installation des Clientrechners

Um ein voll funktionsfähiges Image eines Rechners erzeugen zu können, ist es sinnvoll, den Mastercomputer mit allen erforderlichen Anwendungsprogrammen neu zu installieren. Die anschließende Konfiguration des Computers wird von einem administrativen Account (nicht vom Administrator selbst!) vorgenommen, der sowohl das Betriebssystem als auch die installierten Anwendungen korrekt an die Umgebung anpasst und konfiguriert (auch den Internet Explorer!).

Die Anwendungsprogramme sollte der Administrator nicht selbst konfigurieren, sondern diese Arbeit einem administrativen Account überlassen.

Da alle Einstellungen im Profil dieses Benutzers abgespeichert werden, ist es notwendig, dass diese auch den späteren Benutzern zur Verfügung gestellt werden. Ansonsten kann es vorkommen, dass Anwendungsprogramme ständig eine Nachinstallation von Dateien anfordern, weil die entsprechenden Registry-Keys bei diesem Benutzer fehlen, obwohl bereits

alles korrekt installiert ist. Sobald also der Mastercomputer den Wünschen entspricht, ist das Profil dieses administrativen Accounts in den Bereich „Default User" unter „Dokumente und Einstellungen" zu kopieren. Damit wird erreicht, dass ein neu angemeldeter Benutzer diese Einstellungen als Vorlage in sein eigenes Profil kopiert bekommt.

8.2.3 Vorbereiten des Clientrechners für die Duplizierung

Da beim ersten Start des geklonten Zielcomputers das Administratorkennwort neu gesetzt wird, muss es beim Mastercomputer gelöscht werden. Außerdem muss der Mastercomputer vor dem Klonen aus der Domäne herausgenommen werden.

Der Computer muss vor der Erstellung des Images unbedingt aus der Domäne entfernt werden!

Alle Dateien, die für den regulären Betrieb des Computers nicht notwendig sind, sollten entfernt werden. Darunter fallen z. B. alle temporären Dateien sowie Einträge in der Ereignisanzeige (Überwachungs-, System- und Ereignisprotokoll).

Danach befinden sich immer noch eindeutige Informationen (z. B. die SIDs) auf diesem Computer.

Diese Informationen werden vom Programm **SYSPREP.EXE** automatisch vom Mastercomputer entfernt. Das Programm SYSPREP.EXE befindet sich in der Datei **DEPLOY.CAB** auf der Windows Server 2003 CD im Verzeichnis **\SUPPORT\TOOLS**. Dieses Programm muss am Laufwerk C: im Verzeichnis SYSPREP abgelegt werden. Für die korrekte Funktionsweise ist außerdem die Datei **SETUPCL.EXE** im gleichen Verzeichnis erforderlich.

Beim ersten Start des Zielcomputers fehlen nun einige Informationen, die Sysprep entfernt hat. Dies bedeutet, dass ein Mini-Installations-Assistent aufgerufen wird und die erforderlichen Informationen einholt. Diese Informationen können allerdings auch in eine Antwortdatei mit dem Namen **SYSPREP.INF** geschrieben werden. Bei der Erstellung der Datei ist der Setup-Manager (SETUPMGR.EXE) behilflich. Dieses Programm befindet sich ebenfalls in der Datei DEPLOY.CAB auf der Server-CD.

Um beim ersten Start des Zielcomputers nicht die Fragen des Setup-Assistenten beantworten zu müssen, ist es sinnvoll, eine vorgefertigte Antwortdatei (SYSPREP.INF) zu erstellen.

Nähere Informationen finden Sie in der Schritt-für-Schritt-Anleitung im Kapitel 9.3

Nachdem SYSPREP.EXE ausgeführt wurde, fährt das System automatisch herunter. Mit Hilfe einer Klon-Software kann nun ein Image des Computers erzeugt und am Server abgelegt werden.

8.2.4 Zielrechner klonen

Der Zielrechner ist mit einer Startdiskette zu starten, die automatisch die Netzwerkverbindung zum Server herstellt. Wenn nun das Klon-Programm gestartet wird, kann das Image auf den Zielcomputer übertragen werden.

8.2.5 Erster Start des geklonten Zielrechners

Es wird ein Mini-Setup-Assistent gestartet, der die fehlenden Informationen (z. B. Beitritt zur Domäne, Administratorkennwort) einholt. Damit der Administrator diese Informationen nicht bei jedem Zielcomputer von Hand eingeben muss, ist es sinnvoll, die Antworten vorher in einer Antwortdatei (SYSPREP.INF) abzulegen.

Der Setup-Assistent sucht dabei entweder im Laufwerk A: oder im Verzeichnis C:\SYSPREP nach dieser Datei. Wenn sie gefunden wird, werden sämtliche Antworten daraus entnommen, und die Installation, die nur wenige Minuten dauert, wird automatisch absolviert.

8.3 Schritt-für-Schritt-Anleitung

8.3.1 Einleitung

Da das Klonen nicht den Server, sondern das Clientbetriebssystem Windows XP betrifft, wurde auf eine entsprechende Übung, die das gesamte Szenario nachstellt, verzichtet. Aus diesem Grund ist hier die genaue Schritt-für-Schritt-Anleitung zum Klonen des Clientbetriebssystems Windows XP beschrieben.

8.3.2 Desktop- und Dateieinstellungen

Folgende Schritte müssen Sie unternehmen: Melden Sie sich als Administrator an, klicken Sie mit der rechten Maustaste irgendwo auf den Desktop, rufen Sie im Kontextmenü den Punkt EIGENSCHAFTEN auf und wechseln Sie auf die Registerkarte DESKTOP.

Klicken Sie im unteren Teil auf den Button DESKTOP ANPASSEN und nehmen Sie die in der Abbildung gezeigten Einstellungen vor. Dadurch werden die Standard-Desktopelemente eingeblendet und der Desktopbereinigungs-Assistent wird ausgeschaltet.

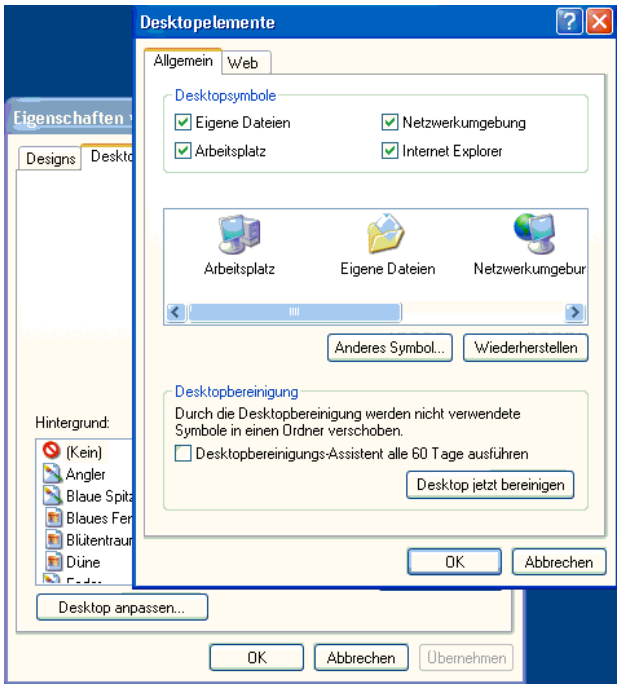


Abb. 69: Desktopelemente einstellen

Rufen Sie den Windows-Explorer auf, klicken Sie den Menüpunkt EXTRAS – ORDNEROPTIONEN an und wechseln Sie auf die Registerseite ANSICHT.

Nun müssen Sie folgende erweiterte Einstellungen deaktivieren (die Häkchen entfernen):

- Automatisch nach Netzwerkordnern und Druckern suchen
- Einfache Dateifreigabe verwenden (empfohlen)
- Erweiterungen bei bekannten Dateitypen ausblenden
- Geschützte Systemdateien ausblenden (empfohlen) – Das Warnfenster mit „Ja" bestätigen

Wählen Sie dann im Bereich VERSTECKTE DATEIEN UND ORDNER die Option ALLE DATEIEN UND ORDNER ANZEIGEN.

Klicken Sie daraufhin den Button FÜR ALLE ÜBERNEHMEN, damit diese Einstellungen für die gesamte Festplatte gültig sind.

8.3.3 Benutzeranmeldung einstellen

Aus Sicherheitsgründen sollte die Benutzeranmeldung so umgestellt werden, dass die klassische Anmeldung verwendet wird. Dazu ist in der Systemsteuerung das Programm BENUTZERKONTEN aufzurufen.

Durch einen Klick auf den Punkt ART DER BENUTZERANMELDUNG ÄNDERN erscheint das nachfolgende Fenster. Hier ist der Punkt WILLKOMMENSSEITE VERWENDEN zu deaktivieren und anschließend mit OPTIONEN ÜBERNEHMEN diese Einstellung zu bestätigen.

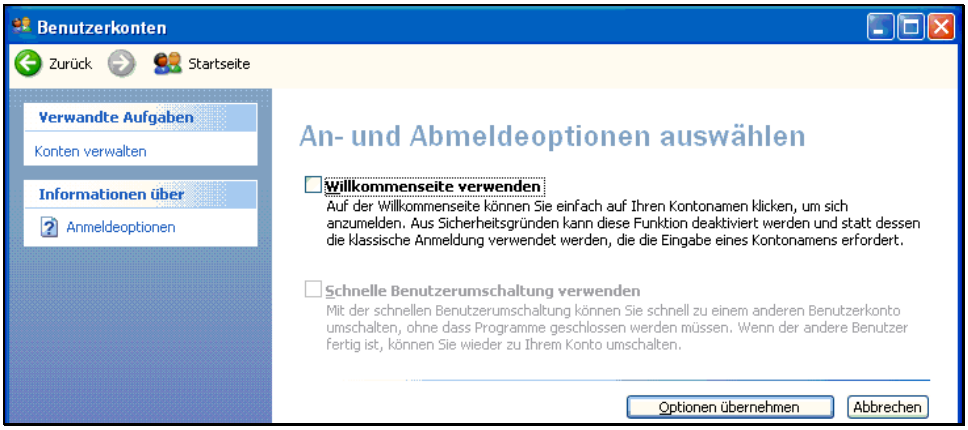


Abb. 70: Willkommenseite verwende

8.3.4 Anlegen eines zweiten administrativen Accounts

Melden Sie sich als Administrator an, klicken Sie mit der rechten Maustaste auf den ARBEITSPLATZ und rufen Sie im Kontextmenü den Punkt VERWALTEN auf.

Abb. 71: Aufruf der Computerverwaltung

Im Fenster COMPUTERVERWALTUNG öffnen Sie nun den Bereich LOKALE BENUTZER UND GRUPPEN und nach einem rechten Mausklick auf den Punkt BENUTZER den Menüpunkt NEUER BENUTZER. Geben Sie im erscheinenden Fenster den neuen Benutzernamen (z. B. Admin) ein.

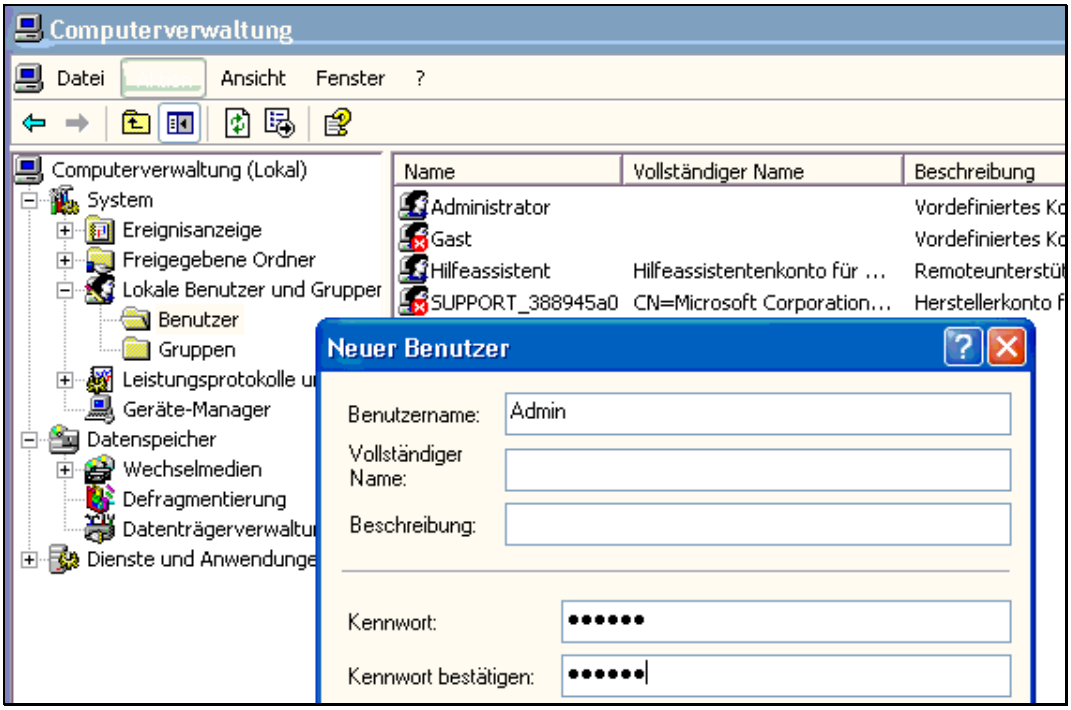


Abb. 72: Einen neuen administrativen Account anlegen

Wechseln Sie zum Menüpunkt GRUPPEN, und wählen Sie nach einem rechten Mausklick auf die Gruppe ADMINISTRATOREN den Menüpunkt MITGLIEDER HINZUFÜGEN.

Im Fenster EIGENSCHAFTEN VON ADMINISTRATOREN klicken Sie nun auf den Button HINZUFÜGEN. Im erscheinenden Fenster BENUTZER WÄHLEN geben Sie den vorhin erstellten Benutzernamen ein und bestätigen mit OK.

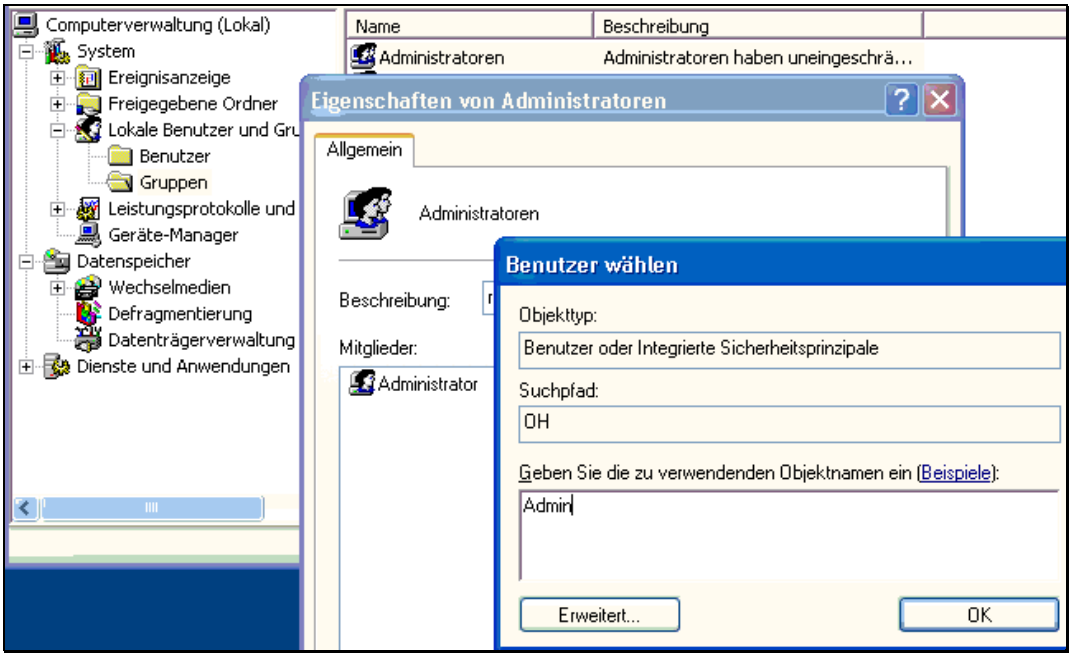


Abb. 73: Benutzer auswählen

Schließen Sie das Fenster EIGENSCHAFTEN VON ADMINISTRATOREN mit OK und auch das Fenster COMPUTERVERWALTUNG.

8.3.5 Lokales Administratorkennwort löschen

Dazu müssen Sie das Fenster WINDOWS-SICHERHEIT mit der Tastenkombination „Strg-Alt-Entf" öffnen und KENNWORT ÄNDERN auswählen.

Nun geben Sie das alte Kennwort des Administrators ein und lassen die beiden Felder für das neue Kennwort und die Kennwortbestätigung frei. Daraufhin das Fenster mit OK schließen.

8.3.6 Standardeinstellungen und Software am Referenzcomputer installieren

Melden Sie sich als Administrator ab und mit dem neu erstellten Account (z. B. Admin) an und installieren Sie die gesamte Software. Zusätzlich müssen mit diesem Account alle Einstellungen vorgenommen werden, die für die späteren Benutzer zur Verfügung stehen sollen (z. B. Desktop- und Dateieinstellungen – siehe Punkt 1.).

Weiters ist es sinnvoll, alle installierten Programme einmal zu starten und sämtliche Einstellungen („Extras – Optionen" sowie Symbolleisten) zu treffen.

8.3.7 Benutzerprofil für den Default User zur Verfügung stellen

Sie müssen sich als Administrator anmelden, mit der rechten Maustaste auf ARBEITSPLATZ klicken und EIGENSCHAFTEN auswählen, im erscheinenden Fenster SYSTEMEIGENSCHAFTEN auf die Registerkarte ERWEITERT wechseln und im Bereich BENUTZERPROFILE den Button EINSTELLUNGEN anklicken.

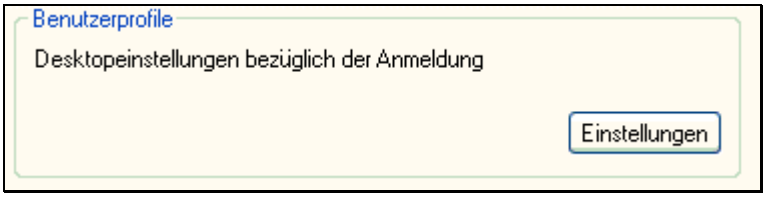


Abb. 74: Einstellungen der Benutzerprofile

Nun müssen Sie

im Fenster BENUTZERPROFILE das vorhin erstellte Benutzerprofil auswählen und auf den Button KOPIEREN NACH klicken,

im Feld PROFIL KOPIEREN NACH den Pfad des Default Users (C:\Dokumente und Einstellungen\Default User) auswählen und

im Bereich BENUTZER auf den Button ÄNDERN klicken und „Jeder" eingeben. Danach schließen Sie das Fenster mit OK. (Dadurch werden allen Benutzern die entsprechenden Benutzerrechte für dieses Profil in der Registry zugewiesen.)

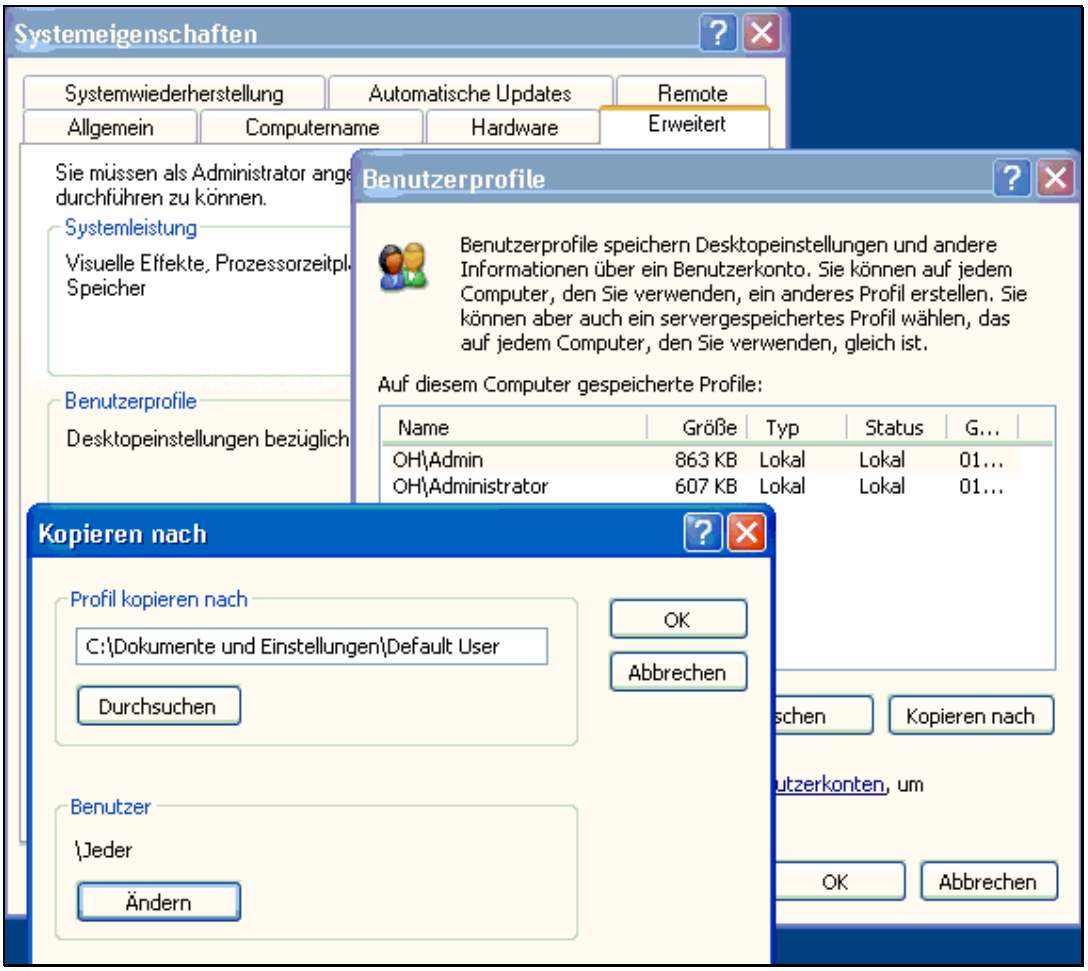


Abb. 75: Profil kopieren

Nach dem Klick auf OK erscheint ein Fenster zum Bestätigen des Kopierens. Dieser Vorgang muss mit JA bestätigt werden:

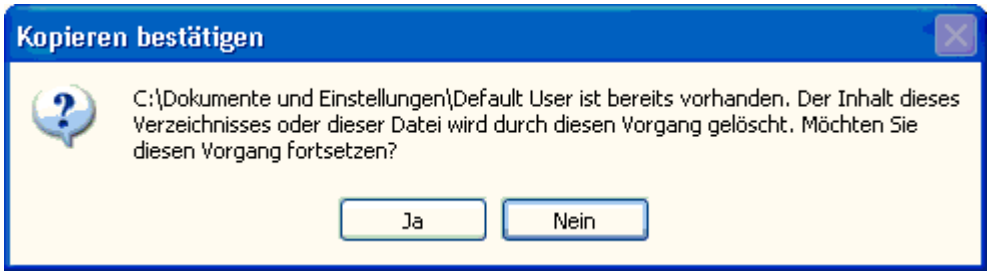


Abb. 76: Bestätigung mit Ja

Daraufhin können sämtliche Fenster mit OK geschlossen werden.

8.3.8 Setzen der lokalen Sicherheitsrichtlinie, so dass Kennwörter nicht ablaufen

Folgendes müssen Sie tun:

Die Systemsteuerung starten und im linken oberen Bereich auf ZUR KLASSISCHEN ANSICHT WECHSELN klicken. Daraufhin den Punkt VERWALTUNG aufrufen und anschließend das Programm LOKALE SICHERHEITSRICHTLINIE starten.

Anschließend öffnen Sie die Kontorichtlinien und wählen die KENNWORTRICHTLINIEN aus. Im rechten Fensterteil den Eintrag MAXIMALES KENNWORTALTER auswählen und mit einem Doppelklick öffnen.

Im Eingabefeld den Wert „0" (Null) eintragen und das Fenster mit OK schließen.

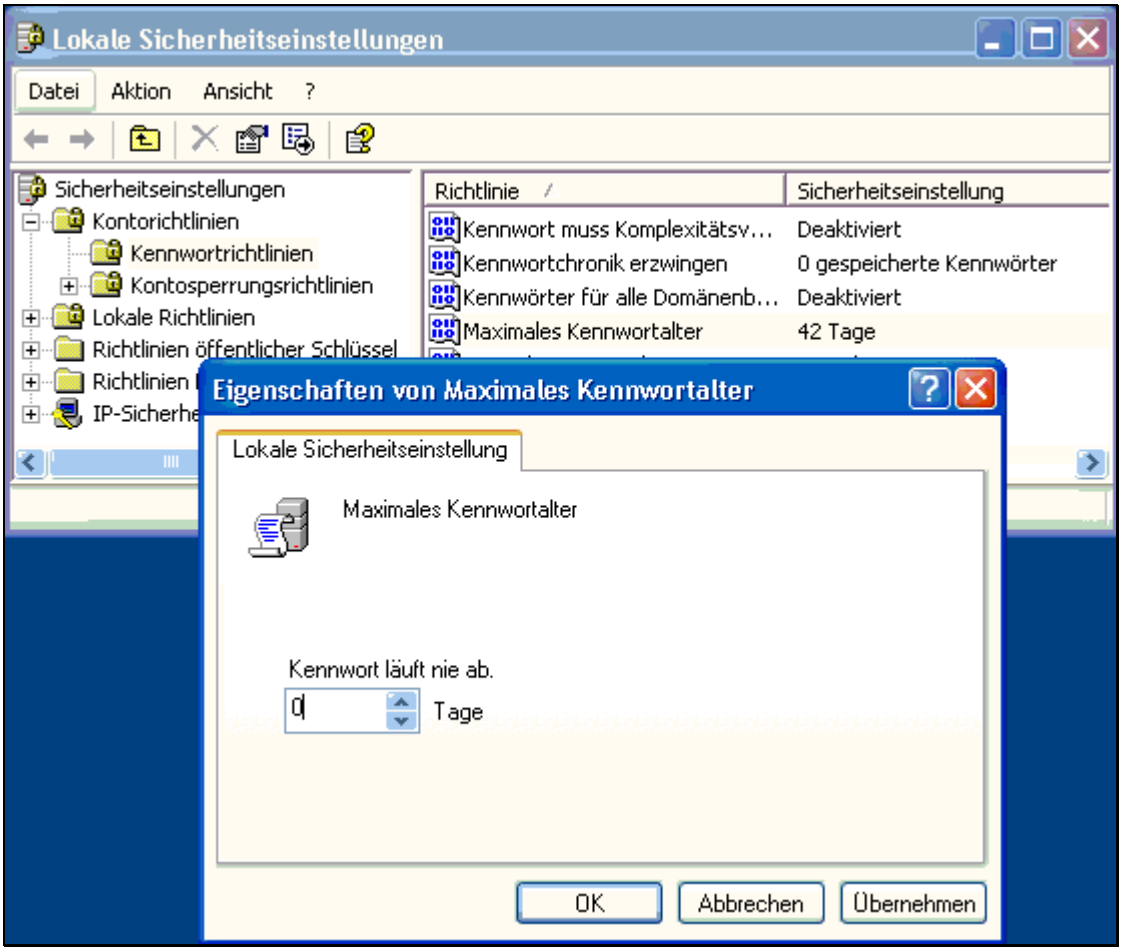


Abb. 77: Setzen des Kennwortalter

Die Fenster LOKALE SICHERHEITSEINSTELLUNGEN und VERWALTUNG schließen.

8.3.9 Erstellen der Datei „Syspref.inf“

Folgendes müssen Sie tun:

Auf der Systempartition (meist Laufwerk C:) einen Ordner mit dem Namen „SYSPREP“ erstellen. Die Datei „DEPLOY.CAB“ auf der CD im Verzeichnis „\SUPPORT\TOOLS“ auswählen und alle Dateien in den vorhin erstellten Ordner „C:\SYSPREP“ kopieren. Anschließend müssen Sie das Programm „SETUPMGR.EXE“ aus diesem Ordner starten.

Nach dem ersten Willkommensbildschirm wählen Sie den Punkt NEUE ANTWORTDATEI ERSTELLEN aus und im nächsten Fenster den Punkt SYSTEMVORBEREITUNGSINSTALLATION.

Im Fenster PLATTFORM wählen Sie die Option WINDOWS XP PROFESSIONAL und anschließend den Punkt JA, VOLLAUTOMATISIERTE INSTALLATION auswählen, um die EULA anzunehmen.

Auf den folgenden Seiten werden die Einstellungen der Workstations vordefiniert:

Software anpassen:	Name der Schule eintragen
Anzeigeeinstellungen:	Farben, Auflösung und Frequenz der Clientcomputer einstellen
Zeitzone:	„(GMT+01:00) Amsterdam, Berlin, Bern, ...“

Product Key angeben:	Eingabe des 25-stelligen Keys
Computername:	Die Option COMPUTERNAMEN AUTOMATISCH GENERIEREN auswählen
Administratorkennwort:	Das künftige lokale Administratorkennwort eingeben und UNBEDINGT das Kontrollkästchen ADMINISTRATORKENNWORT IN DER ANTWORTDATEI VERSCHLÜSSELN auswählen!
Netzwerkkomponenten:	STANDARDEINSTELLUNGEN auswählen
Arbeitsgruppe oder Domäne:	WINDOWS-SERVERDOMÄNE auswählen und Name der Domäne angeben; EIN COMPUTERKONTO IN DER DOMÄNE ERSTELLEN anhaken und einen zuvor angelegten Domänen-Benutzernamen (z. B. „install") sowie das Kennwort angeben
Telefonie:	DIESE EINSTELLUNGEN NICHT FESTLEGEN
Regionale Einstellungen:	Die Option REGIONALE EINSTELLUNGEN IN DER ANTWORTDATEI FESTLEGEN auswählen und DEUTSCH (ÖSTERREICH) als Standardwert auswählen
Sprachen:	keine zusätzlichen Sprachen auswählen
Drucker installieren:	Im Feld NETZWERKDRUCKERNAME den UNC-Namen des/der freigegeben Drucker/s (z.B. \\SRV01\hplaser4) eingeben und HINZUFÜGEN
Einmaliges Ausführen:	keine Befehle eingeben
Zusätzliche Befehle:	keine Befehle eingeben
Zu duplizierende OEM-Zeichenfolge:	nichts eingeben

Den „Windows-Installations-Manager" mit einem Klick auf den Button FERTIGSTELLEN abschließen. Im darauf folgenden Fenster den Speicherort der Datei „SYSPREP.INF" bestimmen (C:\SYSPREP) und den Installations-Manager beenden.

Die fertige „SYSPREP.INF" könnte folgendes Aussehen haben:

```
;SetupMgrTag
[Unattended]
    OemSkipEula=Yes

[GuiUnattended]

AdminPassword=d6ca9f0e2b64356fd9db6a0d2bf62d9176740f7d49c921f9930fc989c68
    EncryptedAdminPassword=Yes
    OEMSkipRegional=1
    TimeZone=110
    OemSkipWelcome=1

[UserData]
    ProductID=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
    FullName="Max Mustermann"
    OrgName="meineschule"
    ComputerName=*

[Display]
    BitsPerPel=24
    Xresolution=1024
```

© 2005, Microsoft Österreich GmbH

```
    YResolution=768
    Vrefresh=75
[RegionalSettings]
    LanguageGroup=1
    Language=00000c07
[SetupMgr]
    DistFolder=C:\sysprep\i386
    DistShare=whistlerdist
[GuiRunOnce]
    Command0="rundll32 printui.dll,PrintUIEntry /in /n \\srv01\hplaser4"
[Identification]
    JoinDomain=meineschule
    DomainAdmin=install
    DomainAdminPassword=kennwort
[Networking]
    InstallDefaultComponents=Yes
```

8.3.10 Den Computer automatisch einer OU zuweisen

Wenn in der fertigen „SYSPREP.INF“ per Hand noch folgende Zeile im Bereich [Identification] eingetragen wird, ist es sogar möglich, dass die Workstation automatisch einer OU zugewiesen wird:

```
[Identification]
    MachineObjectOU="OU=EDV2,OU=Stock1,OU=Raeume,DC=meineschule,DC=local"
```

8.3.11 Vorbereiten des Computers für das Klonen

Starten Sie die Datei „SYSPREP.EXE“ aus dem Ordner „C:\SYSPREP“ und bestätigen Sie das erste Fenster mit OK. Klicken Sie im nächsten Fenster das Kontrollkästchen MINISETUP, wählen Sie im Feld HERUNTERFAHREN die Option SHUTDOWN und klicken Sie anschließend auf den Button ERNEUT VERSIEGELN.

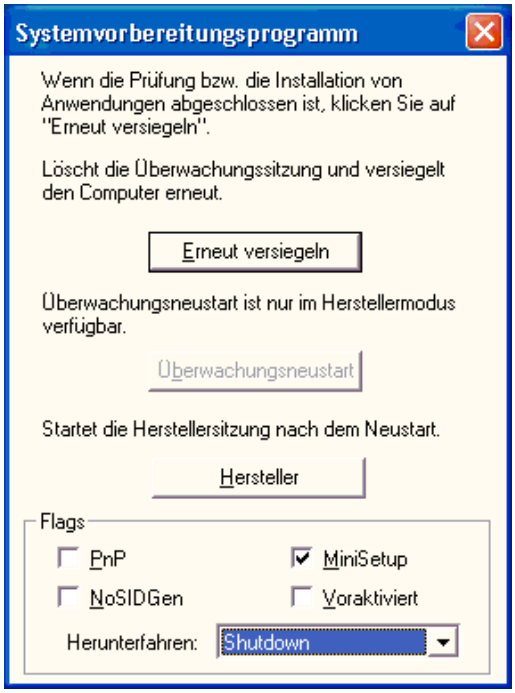


Abb. 78: Systemvorbereitungsprogramm

Wenn Sie die Sicherheitsabfrage im nächsten Fenster mit OK bestätigen, fährt der Computer automatisch herunter.

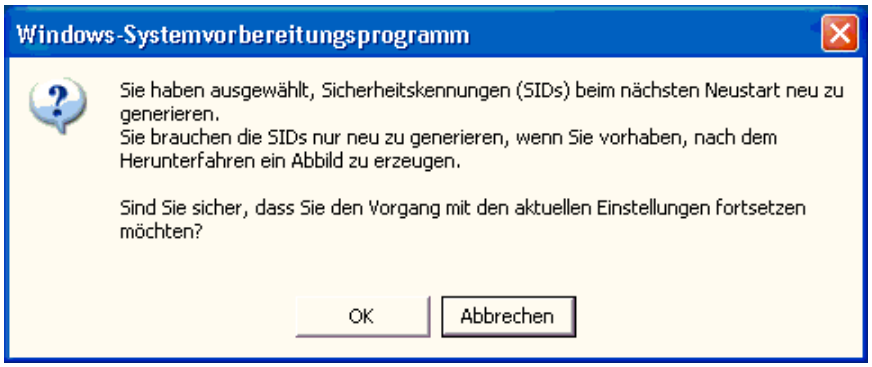


Abb. 79: Abfrage mit OK bestätigen

8.3.12 Klonen mit Ghost oder DriveImage

Der Computer darf nun auf keinen Fall wieder normal gestartet werden. Stattdessen wird nun mit einer Netzwerkstartdiskette eine Verbindung auf DOS-Ebene zu einem Freigabeverzeichnis auf dem Server hergestellt.

Ein Image einer solchen Netzwerkstartdiskette kann unter http://ms.asn-graz.ac.at heruntergeladen werden.

Nachdem die Verbindung zum Server hergestellt ist, kann mit einem beliebigen Klon-Programm (z. B. Ghost oder DriveImage) die Festplatte geklont werden.

Diese Imagedatei wird anschließend mit dem gleichen Klon-Programm auf beliebig viele Zielsysteme kopiert. Sobald diese Computer das erste Mal gestartet werden, startet ein kleines Installationsprogramm, um die Maschine korrekt zu konfigurieren. Sämtliche Antworten für dieses Installationsprogramm werden dabei aus der Datei „SYSPREP.INF" geladen.

© 2005, Microsoft Österreich GmbH

8.4 Automatisches Zuweisen von Druckern via Active Directory

8.4.1 Allgemeines

Das automatische Zuweisen von Druckern an verschiedene Clients ist relativ einfach. Es gibt verschiedene Möglichkeiten.

Sehr einfach gestaltet sich diese Aufgabe in einem Netzwerk, in dem Active Directory installiert ist. Dabei binden Sie die Zuweisung der einzelnen Drucker an die verschiedenen Clients mittels eines Skripts ein (nähere Erläuterung in Kapitel 8), welches beim Starten der Clientrechner ausgeführt wird.

So weisen Sie Clientrechnern einen Drucker automatisch per Script zu:

1. Wählen Sie START, VERWALTUNG, ACTIVE DIRECTORY, BENUTZER UND COMPUTER aus
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Domänennamen und wählen Sie EIGENSCHAFTEN.

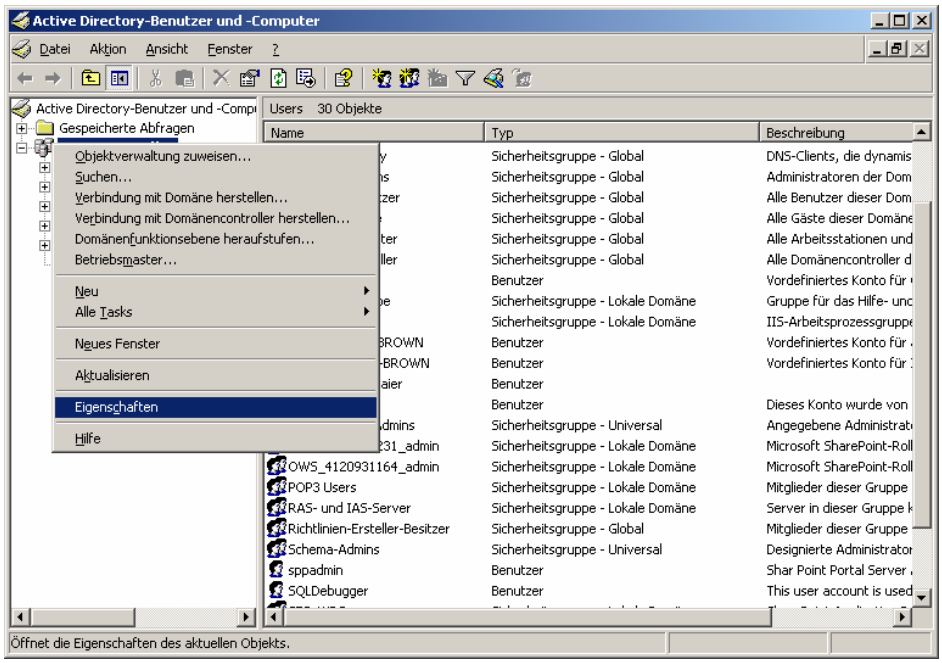


Abb. 80: Active Directory Verwaltung – Ansicht Eigenschaften der Domäne

3. Wählen Sie die Registerkarte GRUPPENRICHTLINIE.
4. Wählen Sie die DEFAULT DOMAIN POLICY aus und klicken Sie auf BEARBEITEN.

   Es öffnet sich der **Gruppenrichtlinienobjekt – Editor**.
5. Erweitern Sie den Zweig BENUTZERKONFIGURATION und wählen Sie den Punkt SKRIPTS (ANMELDEN/ABMELDEN).

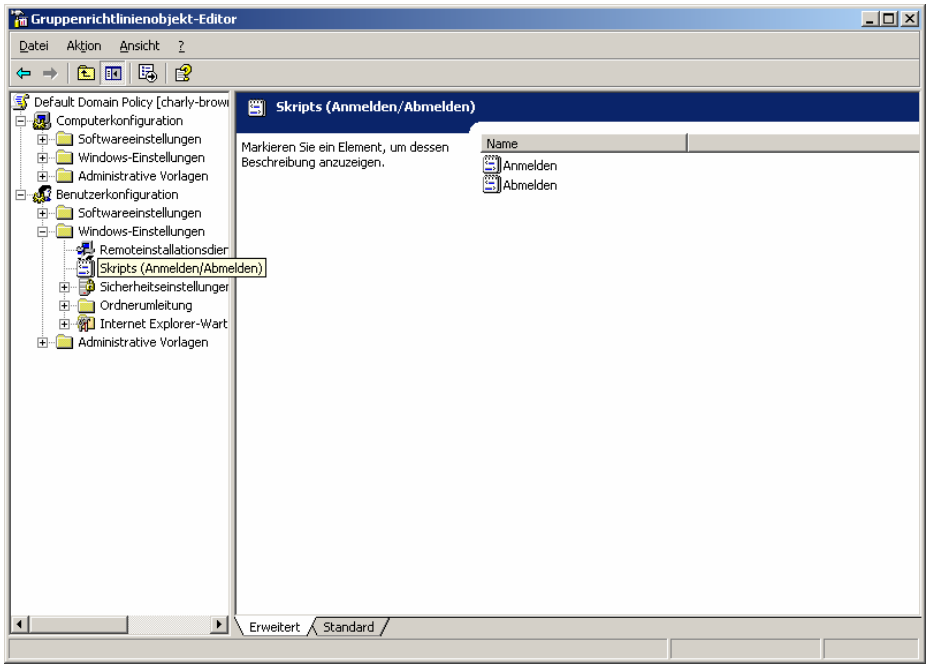


Abb. 81: Gruppenrichtlinienobjekt-Editor – Ansicht Skripts

6. Öffnen Sie das Script ANMELDEN mit einem Doppelklick.
7. Klicken Sie auf HINZUFÜGEN.
8. Klicken Sie auf DURCHSUCHEN, und wählen Sie im sich öffnenden Dialog die entsprechende Skriptdatei aus. Klicken Sie auf ÖFFNEN.

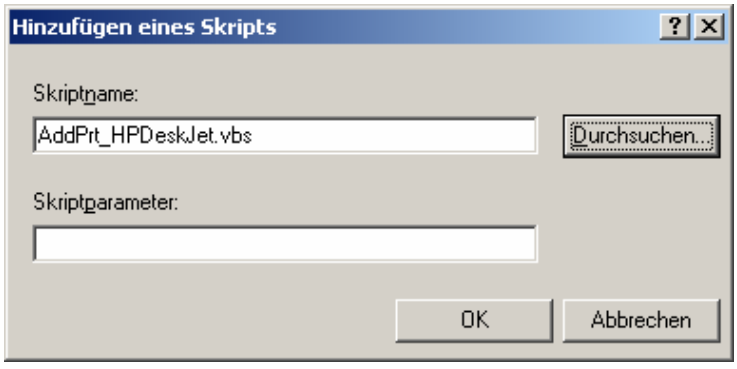


Abb. 82: Hinzufügen eines Skripts

9. Geben Sie eventuell benötigte Parameter ein, und klicken Sie auf OK.
10. Testen Sie die Einstellungen des Skripts, indem Sie den Clientrechner neu starten und überprüfen, ob der Drucker ausgewählt und der Client mit diesem korrekt verbunden wurde.

    Die automatische Einbindung eines Druckers ist hiermit abgeschlossen.

9 Drucken – Druckserver

Diese Kapitel behandelt die Druckserverfunktionalität von Windows Server 2003. Sie werden Drucker und Druckaufträge sowohl lokal als auch im Netzwerk verwalten können.

9.1 Überblick - Definition

Die Serverfunktion „Druckserver" ermöglicht Ihnen das Verwalten und Zuteilen von gemeinsamen Druckern.

Diese Serverrolle ist in der Web Edition der Windows Server 2003-Familie NICHT enthalten.

Dieses Kapitel erläutert, wie Sie einen Server als Druckserver einrichten. Nach der erfolgreichen Installation und Konfiguration des Servers erfahren Sie, wie Sie zusätzliche Einstellungen vornehmen und weitere Features nutzen können.

9.2 Allgemeine Begriffsdefinition

Nachfolgend finden Sie die wichtigsten Begriffe im Bezug auf die Serverrolle „Druckserver" sowie deren Bedeutung und Definition. Eine genauere Definition einzelner Begriffe finden Sie weiter unten in diesem Kapitel.

Druckgerät

Darunter ist das physische Endgerät zu verstehen, das die endgültige Ausgabe der Daten auf Papier oder einem anderen Medium vornimmt.

(Logischer) Drucker

Unter einem Drucker ist eine logische Darstellung eines physikalischen Druckgeräts zu verstehen. Es können mehrere Darstellungen, also Drucker, für ein Druckgerät angelegt werden. So ist es zum Beispiel möglich, verschiedenen Benutzergruppen verschiedene Prioritäten zuzuweisen.

Nähere Informationen zum Verwalten der Prioritäten finden Sie weiter unten im Kapitel.

Anschluss/Port

Unter Anschluss versteht man die Verbindung zwischen dem Computer oder Druckserver und dem Druckgerät. Dies kann etwa der LPT Port sein, wenn das Druckgerät lokal angeschlossen ist, oder aber auch eine Adresse im Netzwerk, wenn das Druckgerät über eine Netzwerkschnittstelle verfügt. Die Installation unterscheidet sich je nach gewähltem Anschluss.

Ein Druckgerät ist somit mittels des Anschlusses an einen (logischen) Drucker gebunden.

Druckserver

Ein Druckserver ist ein Computer, der für die Verwaltung der Drucker in einem Netzwerk verwendet wird. Die Rolle des Druckservers kann grundsätzlich jeder Computer im Netzwerk übernehmen. Es bietet sich jedoch an, als Druckserver einen Computer zu verwenden, auf dem Windows Server 2003 betrieben wird..

Nähere Informationen dazu erhalten Sie im Laufe des weiteren Kapitels.

© 2005, Microsoft Österreich GmbH

Druckauftrag

Den Quellcode, der sowohl die zu druckenden Daten als auch die Druckbefehle enthält, bezeichnet man als Druckauftrag. Druckaufträge werden nach Datentypen unterschieden. Die Einteilung richtet sich nach den gegebenenfalls erforderlichen Änderungen, die die Druckwarteschlange an dem Auftrag vornehmen muss, um ein korrektes Druckergebnis zu erzielen.

Druckwarteschlange

Die Software, die ein an den Drucker gesendetes Dokument entgegennimmt und auf einem Datenträger oder im Arbeitsspeicher ablegt, bis der Drucker zum Ausführen des Auftrags bereit ist.

Druckertreiber

Ein Programm, das es anderen Programmen ermöglichen soll, mit einem bestimmten Drucker zu arbeiten, ohne dabei die Besonderheiten der Druckerhardware und der internen Druckersprache kennen zu müssen. Durch die Verwendung von Druckertreibern, welche die druckerspezifischen Feinheiten handhaben, können Programme mit einer Vielzahl unterschiedlicher Drucker problemlos kommunizieren.

Druckerpool

Ein Druckerpool ist ein logischer Drucker, der durch mehrere Anschlüsse des Druckerservers mit mehreren Druckern verbunden ist. Er repräsentiert sozusagen eine zentrale Anlaufstelle für Druckaufträge, die, ohne ein genaueres Wissen des Benutzers über die tatsächlich angeschlossenen Drucker, an Druckgeräte weitergeleitet und von diesen verarbeitet wird.

Nähere Informationen dazu erhalten Sie weiter unten in diesem Kapitel.

© 2005, Microsoft Österreich GmbH

9.3 Druckvorgang allgemein

Im Folgenden finden Sie eine Übersicht über die Vorgänge, die ablaufen, wenn ein Dokument von einem Client unter Windows XP an einen Drucker gesendet wird. Der Drucker ist an einen Computer angeschlossen, auf dem ein Betriebssystem der Windows Server 2003-Produktfamilie ausgeführt wird. (Einige Prozesse weichen von den folgenden Angaben ab, wenn Druckclients verwendet werden, auf denen ein Betriebssystem ausgeführt wird, das nicht auf Windows basiert.)

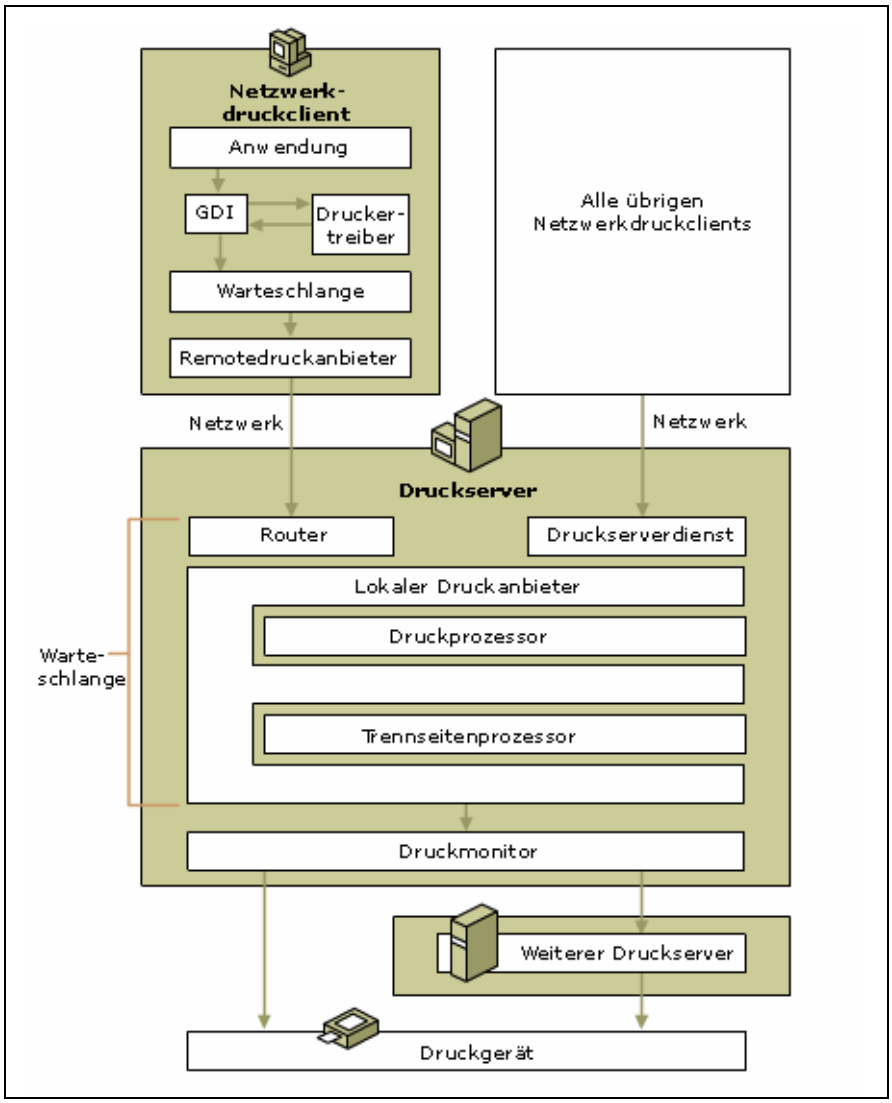


Abb. 83: Druckvorgang allgemein aus Windows Server 2003 Hilfe und Support

Ein Benutzer an einem Clientcomputer unter Windows XP möchte ein Dokument drucken.

- Wenn das Dokument aus einer Windows-Anwendung heraus gesendet wird, ruft die Anwendung die GDI (Graphics Device Interface) auf, die wiederum den Druckertreiber für den Zieldrucker aufruft. Mithilfe der von der Anwendung stammenden Dokumentinformationen tauschen die GDI und der Treiber Daten aus, um den Druckauftrag in die Sprache des Druckers zu übertragen. Anschließend wird der Druckauftrag an die clientseitigen Druckerspooler

übergeben. Wenn der Client ein anderes Betriebssystem als Windows oder eine nicht unter Windows ausgeführte Anwendung verwendet, wird diese Aufgabe in ähnlicher Form von einer anderen Komponente übernommen, die in diesem Fall die GDI ersetzt.

- Der Clientcomputer sendet den Druckauftrag an den Druckserver. Bei Clients unter Windows XP, Windows 2000 oder Windows NT 4.0 führt der clientseitige Spooler einen RPC (Remote Procedure Call, Remoteprozeduraufruf) an die Serverseite des Spoolers aus. Dieser fragt mithilfe des Routers den Remotedruckanbieter auf der Clientseite ab. Der Remotedruckanbieter leitet einen weiteren RPC an den Serverspooler ein, und dieser nimmt den Druckauftrag über das Netzwerk entgegen.
- Druckaufträge von Clients unter Windows XP, Windows 2000 oder Windows NT 4.0 weisen auf dem Druckserver den Datentyp EMF (erweiterte Metadatei) auf. Viele andere Anwendungen verwenden den Datentyp RAW (druckbereit).
- Der Router des Servers übergibt den Druckauftrag an den lokalen Druckanbieter auf dem Server (Komponente des Spoolers), der den Druckauftrag spoolt, d. h., auf den Datenträger schreibt.
- Der lokale Druckanbieter fragt den Druckprozessor ab. Der Druckprozessor erkennt den Datentyp des Auftrags und nimmt den Druckauftrag entgegen. Der Druckauftrag wird dann vom Druckprozessor seinem Datentyp entsprechend konvertiert.
- Wenn der Zieldrucker auf dem Clientcomputer definiert ist, entscheidet der Druckserver-Dienst, ob der Spooler des Servers den Druckauftrag ändern oder ihm einen anderen Datentyp zuweisen soll. Der Druckauftrag wird daraufhin an den lokalen Druckanbieter übergeben und von diesem auf den Datenträger geschrieben.
- Die Kontrolle über den Druckauftrag wird an den Trennseitenprozessor übergeben, der vor dem Auftrag ggf. eine Trennseite einfügt.
- Der Auftrag wird zurück an die Druckmonitore gespoolt. Bei bidirektionalen Druckern wird die beidseitige Kommunikation zwischen dem Sender und dem Drucker von einem Sprachmonitor verwaltet. Dieser übergibt den Druckauftrag dann an einen Anschlussmonitor. Wenn es sich nicht um einen bidirektionalen Drucker handelt, wird der Druckauftrag direkt an den Anschlussmonitor übergeben und von ihm anschließend an den Zieldrucker (oder einen anderen Netzwerkdruckserver) gesendet.
- Der Drucker empfängt den Druckauftrag, konvertiert jede Seite in das Bitmapformat und führt den Druckauftrag aus.

9.4 Vorüberlegungen

Wenn Sie die Serverrolle „Druckserver" installieren möchten, müssen Sie einige Punkte beachten:

- Nach einer Neuinstallation von Windows Server 2003 ist Ihr System bereits richtig und vollständig konfiguriert für die Installation der Serverrolle **Druckserver**. Wenn Sie dagegen ein Upgrade von einer früheren Betriebsystemversion auf Windows Server 2003 vorgenommen haben, sind weitere Punkte zu beachten. Diesbezüglich beachten Sie bitte die Hinweise im Hilfe & Support-Center!
- Falls Sie den Zugriff auf die Drucker auf bestimmte Gruppen oder Benutzer einschränken möchten, müssen Sie die freigegebenen Drucker im Active Directory veröffentlichen. Dadurch können Benutzer leichter nach verfügbaren Druckern suchen und sich zu diesen verbinden. Der Server muss einer Domäne angehören, wenn Sie diese Optionen nutzen wollen, andernfalls steht Ihnen diese Option nicht zur Verfügung.
- Als Dateisystem für die verwendeten Partitionen sollten Sie NTFS wählen, da andere Dateisysteme, wie etwa FAT oder FAT32, keine Sicherheitsfunktionen, Komprimierungsfunktionen, keine individuellen Berechtigungen und auch keine Verschlüsselung auf Dateiebene bieten, womit auch Druckerjobs nicht verschlüsselt werden können.

Des Weiteren sollten Sie die folgenden Anforderungen klären und eventuelle Vorarbeiten leisten, bevor Sie die Serverfunktion installieren.

© 2005, Microsoft Österreich GmbH

- Es ist von entscheidender Wichtigkeit, dass Sie wissen, von welchen Betriebssystemen die Druckaufträge gesendet werden. Je nachdem welches System die verschiedenen Benutzer ausführen, kann es notwendig sein, verschiedene Vorkehrungen zu treffen.
- Sie sollten stets dafür sorgen, dass Sie die aktuellen Druckertreiber nutzen, da veraltete Druckertreiber den Ablauf beeinträchtigen können. Nähere Informationen erhalten Sie von Ihrem Hardware-Hersteller oder im Hilfe & Support-Center.
- Ebenfalls sehr wichtig ist, wie der oder die Drucker an den Druckserver angeschlossen sind. Sie sollten eine Testseite am Drucker ausgeben lassen, um die aktuellen Einstellungen auf einen Blick einsehen zu können. Es sind jeweils andere Daten und Vorgehensweisen notwenig, wenn ein Drucker direkt am Druckerserver mittels eines Parallelports angeschlossen ist oder aber einen eigenen Netzwerkanschluss besitzt.
- Jeder Drucker sollte einen Namen, eine Bezeichnung und einen Freigabenamen erhalten, um ihn im Netzwerk leichter identifizieren zu können.

9.5 Lokaler vs. Netzwerkdrucker

Beim Drucken unterscheiden wir zwischen lokalen und Netzwerkdruckern. Der Unterschied liegt vor allem darin, dass die Druckverarbeitung beim lokalen Drucker direkt geschieht, während ein Druckjob beim Netzwerkdrucker an den Druckserver (=als lokaler Drucker am Server installierter und freigegebener Drucker) weitergeleitet wird. Wenn Sie einen lokalen Drucker auf einer Workstation/einem Server installieren, steht er jedem Benutzer zur Verfügung, der sich auf dieser Workstation/diesem Server anmeldet. Installieren Sie einen Netzwerkdrucker, so werden lediglich Sie selbst diesen Drucker unter „Systemsteuerung – Drucker" wieder finden. Jeder andere Benutzer muss diesen Drucker für sich selbst neu einrichten.

Ein Drucker, der über eine eigene Netzwerkkarte verfügt bzw. über Zusatzgeräte via TCP/IP erreichbar ist, wird als lokaler Drucker bezeichnet, da die Druckverarbeitung lokal am Server erfolgen wird und der fertige Druckerdatenstrom an die TCP/IP-Adresse des Druckers gesendet wird.

Um Benutzern im Netzwerk einen am Server lokal installierten Drucker zur Verfügung zu stellen, muss der Drucker am Server freigegeben werden. Auf den Workstations kann dann dieser freigegebene Drucker als Netzwerkdrucker eingerichtet werden. Da Netzwerkdrucker nur dem aktuell angemeldeten Benutzer zur Verfügung stehen, muss über ein Loginscript der Netzwerkdrucker bei jeder Anmeldung eines Benutzers zugewiesen werden (siehe Skript weiter unten in diesem Kapitel).

9.5.1 Installation mittels Serververwaltung

So installieren Sie die Serverfunktion „Druckserver" mittels der Serververwaltung:

1. Öffnen Sie die SERVERVERWALTUNG.
2. Wählen Sie die Funktion HINZUFÜGEN/ENTFERNEN.
3. Klicken Sie auf WEITER.
4. Wählen Sie die Serverfunktion DRUCKSERVER.
5. Wählen Sie, ob die Drucker, die Sie installieren möchten, nur Windows 2000- und Windows XP-Clients sind oder aber auch andere Betriebssysteme als Clients in Frage kommen. Je nach Ihrer Auswahl verläuft das Setup anders.
   - Wenn Sie die Option NUR WINDOWS 2000- UND WINDOWS XP-CLIENTS gewählt haben, wird im nächsten Schritt der DRUCKERINSTALLATIONS-ASSISTENT aufgerufen und neue Drucker werden hinzugefügt.
   - Wenn Sie die Option ALLE ARTEN VON WINDOWS-CLIENTS gewählt haben, wird im nächsten Schritt der DRUCKERINSTALLATIONS-ASSISTENT aufgerufen, neue Drucker werden hinzugefügt. Anschließend wird der ASSISTENT FÜR DIE DRUCKERTREIBERINSTALLATION ausgeführt.

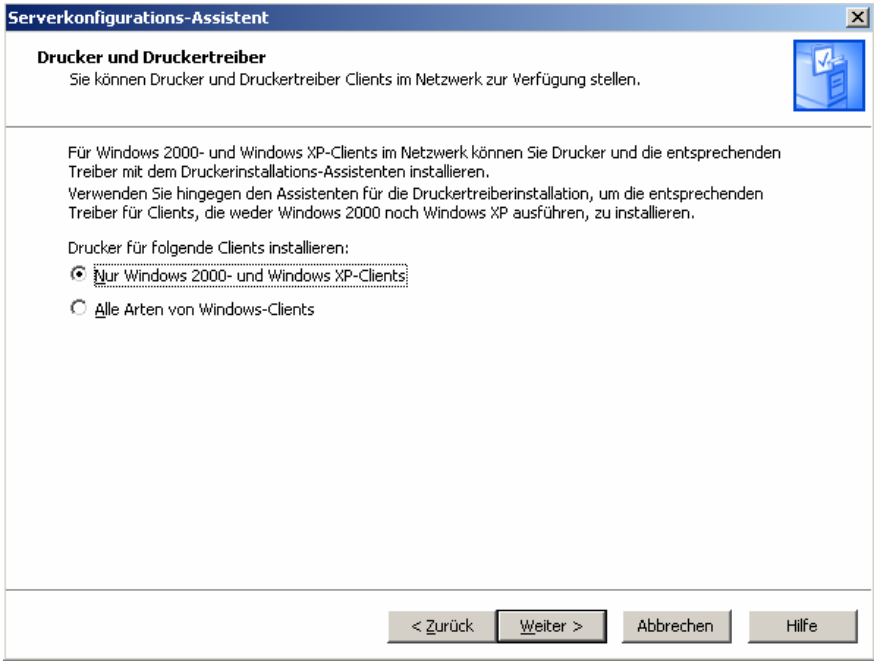


Abb. 84: Drucker- und Druckertreiber-Einrichtung

6. Wählen Sie eine Option und klicken Sie auf WEITER.
7. Bestätigen Sie Ihre Auswahl mit einem Klick auf WEITER.
8. Es startet der DRUCKERINSTALLATIONS-ASSISTENT.
9. Klicken Sie auf WEITER.

Der besseren Übersicht wegen teilt sich hier die Anleitung: Direkt im Anschluss finden Sie die Anleitung für die Installation eines lokalen Druckers, danach für einen Netzwerkdrucker.

Wählen Sie die Option LOKALER DRUCKER, DER AN DEN COMPUTER ANGESCHLOSSEN IST, wenn einer der folgenden Punkte zutrifft:

- Der Drucker ist direkt mit dem Druckserver verbunden.
- Der Drucker verfügt über einen eigenen Netzwerkanschluss.

Wählen Sie die Option NETZWERKDRUCKER ODER DRUCKER, DER AN EINEN ANDEREN COMPUTER ANGESCHLOSSEN IST, wenn der folgende Punkt zutrifft:

- Dieser Druckserver soll Druckaufträge an einen weiteren Druckserver weiterleiten.

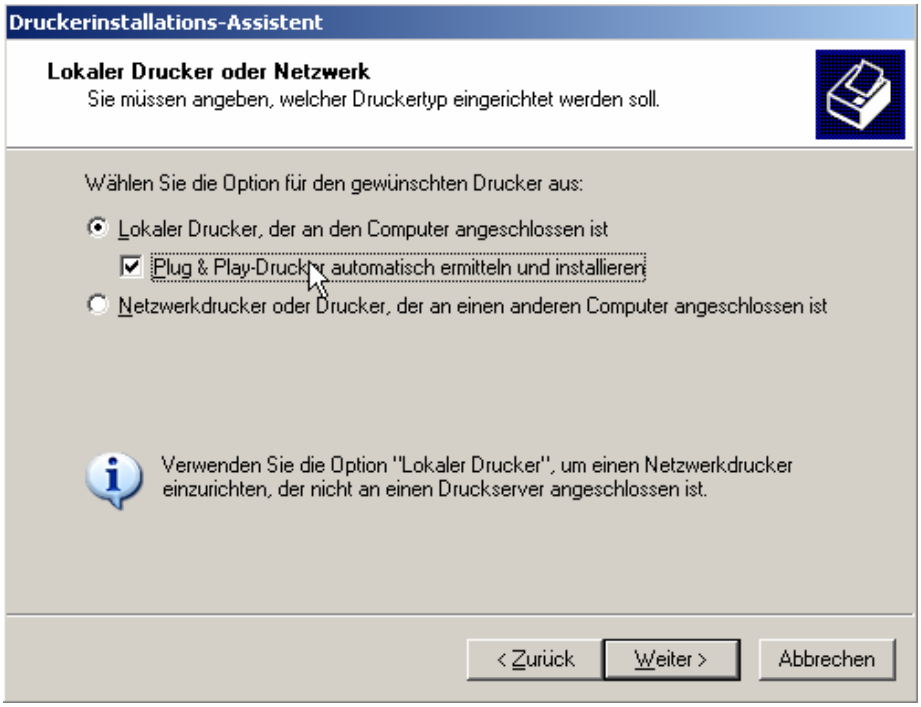


Abb. 85: Auswahl lokaler Drucker oder Netzwerk

Auf Clientrechnern werden normalerweise Drucker mit der Option NETZWERKDRUCKER ODER DRUCKER, DER AN EINEN ANDEREN DRUCKER ANGESCHLOSSEN IST installiert. Da es hier jedoch um die Installation eines Druckers geht, der von einem Druckserver Druckaufträge erhalten soll, sollten Sie die erste Variante wählen.

9.5.2 Installation eines Netzwerksdruckers via Assistent

So installieren Sie einen Netzwerkdrucker mittels des Druckerinstallations-Assistenten:

1. Wählen Sie die Option LOKALER DRUCKER, DER AN DEN COMPUTER ANGESCHLOSSEN IST und deaktivieren Sie die Option PLUG & PLAY-DRUCKER AUTOMATISCH ERMITTELN UND INSTALLIEREN.
2. Klicken Sie auf WEITER.
3. Wählen Sie die Option EINEN NEUEN ANSCHLUSS ERSTELLEN.
4. Wählen Sie STANDARD TCP/IP PORT aus der Liste aus.

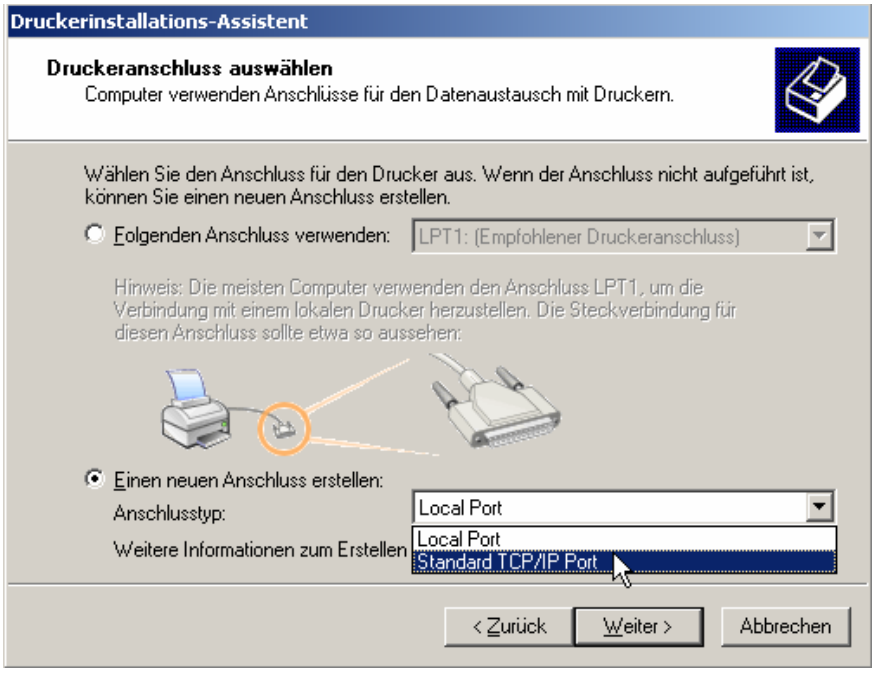


Abb. 86: Neuen Druckeranschluss erstellen

5. Es öffnet sich der ASSISTENT ZUM HINZUFÜGEN EINES STANDARD-TCP/IP-DRUCKERPORTS.
6. Klicken Sie auf WEITER.
7. Geben Sie die IP-ADRESSE oder den DRUCKERNAMEN des Netzwerkdruckers sowie den PORT an.

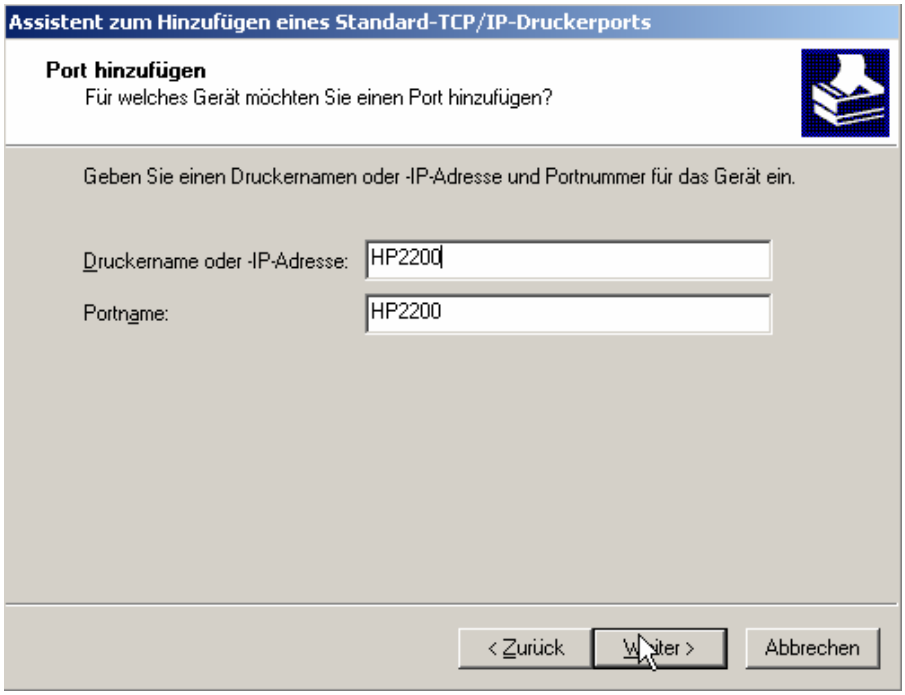


Abb. 87: Druckerport angeben

Diese Daten erhalten Sie, wenn Sie direkt, lokal am Netzwerkdrucker eine Testseite ausgeben lassen. Die meisten Drucker drucken daraufhin eine Seite mit Konfigurationsdaten aus! Sehen Sie eventuell in der Bedienungsanleitung des Druckers nach, wie Sie eine Testseite direkt am Gerät ausgeben!

8. Wenn der Drucker gefunden wurde, erscheint die Zusammenfassung. Andernfalls müssen Sie zurück gehen und es erneut versuchen.
9. Beenden Sie den ASSISTENT ZUM HINZUFÜGEN EINES STANDARD-TCP/IP-DRUCKERPORTS mit einem Klick auf FERTIG STELLEN

   Nun erscheint wieder der Bildschirm des Druckerinstallations-Assistenten
10. Wählen Sie den entsprechenden Druckerhersteller und Druckertypen oder klicken Sie auf Datenträger und geben den Ort zum Druckertreiber ein. Klicken Sie auf WEITER.

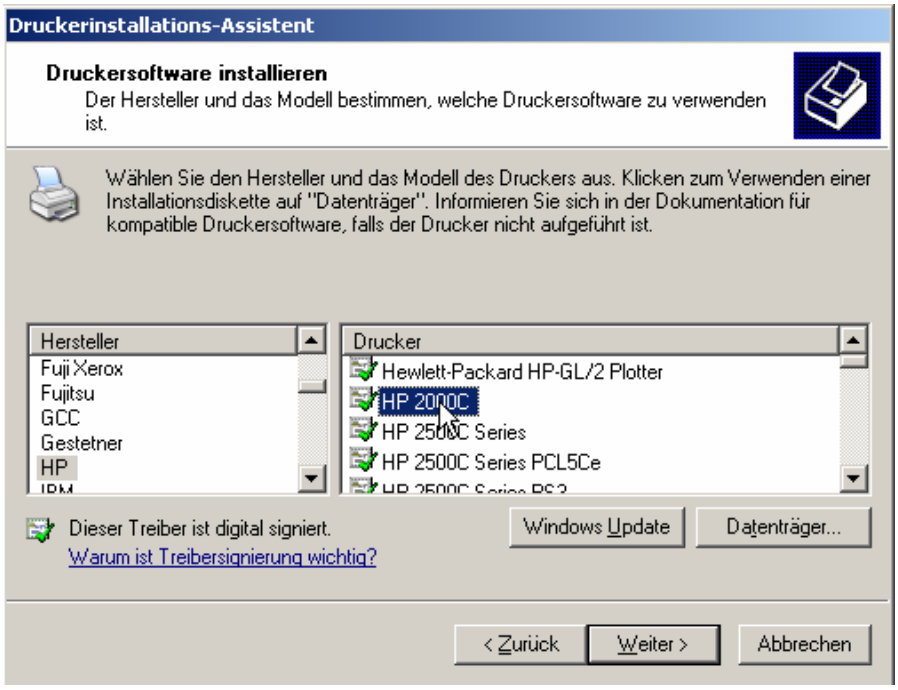


Abb. 88: Druckertreiber auswählen

11. Vergeben Sie einen Druckernamen und legen Sie fest, ob der Drucker als Standarddrucker verwendet werden soll und klicken Sie auf WEITER.
12. Geben Sie an, ob Sie den Drucker freigeben möchten, vergeben Sie dann einen entsprechenden Freigabenamen und klicken Sie auf WEITER.

Sie müssen mindestens einen Drucker freigeben, damit die Serverrolle „Druckserver“ richtig arbeitet. Andernfalls wird die Installation der Serverrolle abgebrochen!

© 2005, Microsoft Österreich GmbH

13. Geben Sie eine Standortbezeichnung und eventuell einen Kommentar an und klicken Sie auf WEITER.
14. Wählen Sie, ob Sie die Testseite drucken möchten und klicken Sie auf WEITER.
15. Wählen Sie, ob Sie einen weiteren Drucker installieren möchten und klicken Sie auf FERTIG STELLEN.

Wenn Sie zu Beginn die Option ALLE ARTEN VON WINDOWS-CLIENTS ausgewählt haben, startet nun der ASSISTENT FÜR DIE DRUCKERTREIBERINSTALLATION. Folgen Sie den Anweisungen und führen Sie den Assistent komplett aus.

Der ASSISTENT FÜR DIE DRUCKERTREIBERINSTALLATION erkennt nicht automatisch den Hersteller des Druckers. Stattdessen markiert er nur den ersten Eintrag aus der Herstellerliste. Wählen Sie den richtigen Treiber aus.

Die Auswahl eines falschen Treibers kann zu Problemen während des Betriebs des Druckservers führen!

Holen Sie sich gegebenenfalls einen neuen Treiber von der Webseite des Herstellers!

Nach der erfolgreichen Installation des Druckertreibers wird der Assistent für die Druckertreiberinstallation beendet.

Nachdem der Druckerinstallations-Assistent beendet ist, ist die Serverrolle „Druckserver" fertig konfiguriert und einsatzbereit. Sie können nun weitere Einstellungen für die Serverrolle „Druckserver" vornehmen.

9.5.3 Installation eines lokalen Druckers via Assistent

So installieren Sie einen lokalen Drucker mittels des Druckerinstallations-Assistenten:

1. Wählen Sie, ob der Drucker automatisch erkannt werden soll oder ob Sie den Drucker manuell angeben möchten.
2. Klicken Sie auf WEITER.

Wenn Sie einen lokal angeschlossenen Drucker installieren wollen, wählen Sie hier „Plug & Play Drucker automatisch ermitteln und installieren"!

Sie sollten diese Option NICHT wählen, wenn es sich um einen älteren Drucker handelt oder dieser Drucker keine Plug & Play-Unterstützung bietet.

3. Wählen Sie den richtigen Anschluss aus, meistens LPT1.

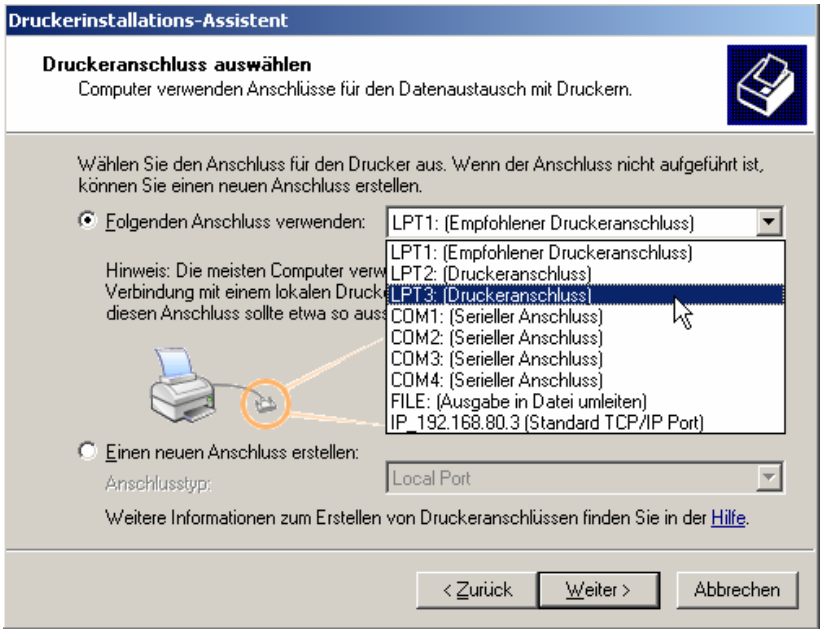


Abb. 89: Druckeranschluss auswählen

4. Klicken Sie auf WEITER.
5. Wählen Sie einen Druckertreiber aus der Liste oder klicken Sie auf die Schaltfläche DATENTRÄGER, um einen eigenen Treiber anzugeben. Folgen Sie den Anweisungen des Assistenten.

Eine einfache und schnelle Lösung bietet Ihnen das Windows Update, sofern Sie über einen Internetanschluss verfügen. Wählen Sie dazu die Schaltfläche und folgen Sie den Anweisungen des Assistenten. Der entsprechende Treiber wird aus dem Internet herunter geladen und installiert!

6. Klicken Sie auf WEITER.
7. Geben Sie einen Druckernamen an und klicken Sie auf WEITER.

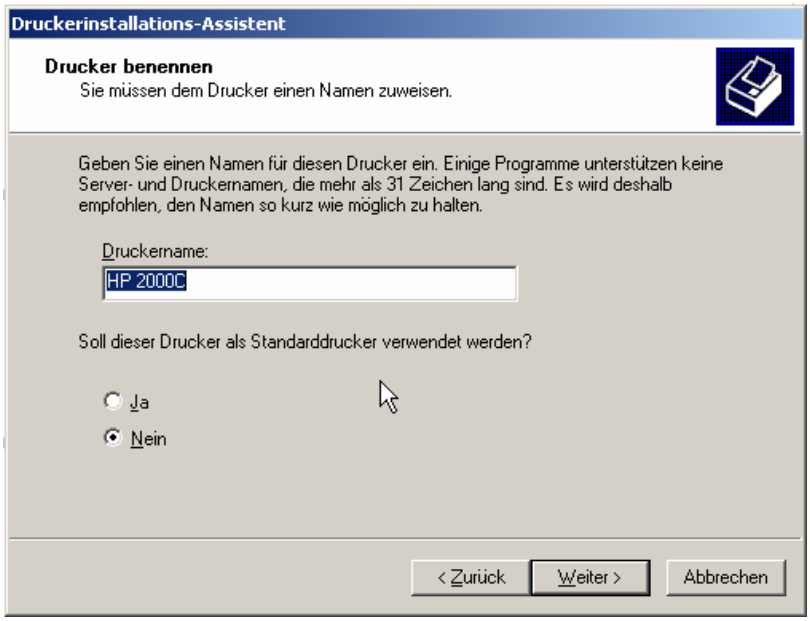


Abb. 90: Drucker benennen

8. Geben Sie an, ob der Drucker als Standarddrucker auf dem Server installiert werden soll, und klicken Sie auf WEITER.
9. Wenn Sie den Drucker freigeben möchten, wählen Sie die entsprechende Option, vergeben einen Namen und klicken auf WEITER.

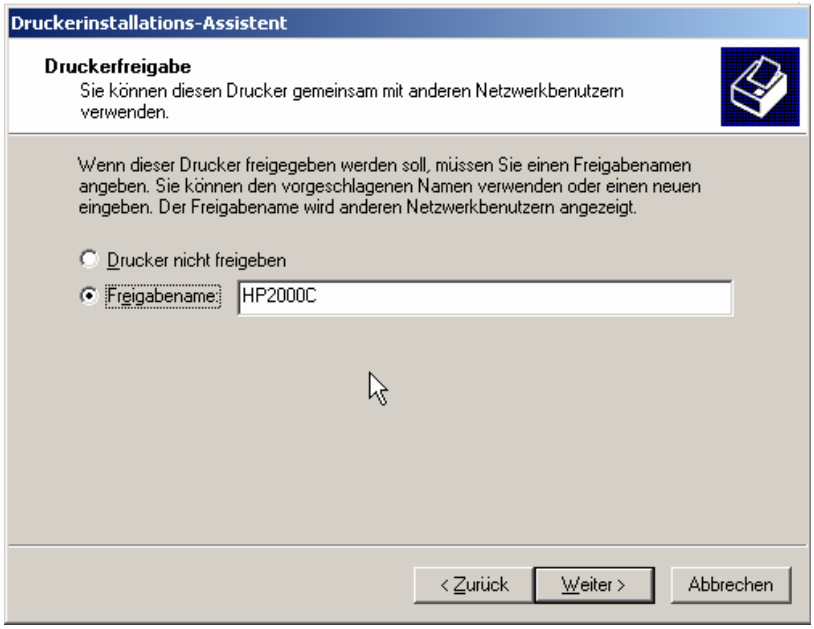


Abb. 91: Drucker freigeben

Sie müssen mindestens einen Drucker freigeben, damit die Serverrolle „Druckserver" richtig arbeitet. Andernfalls wird die Installation der Serverrolle abgebrochen!

10. Vergeben Sie eine Standortbezeichnung und einen Kommentar, und klicken Sie auf WEITER.

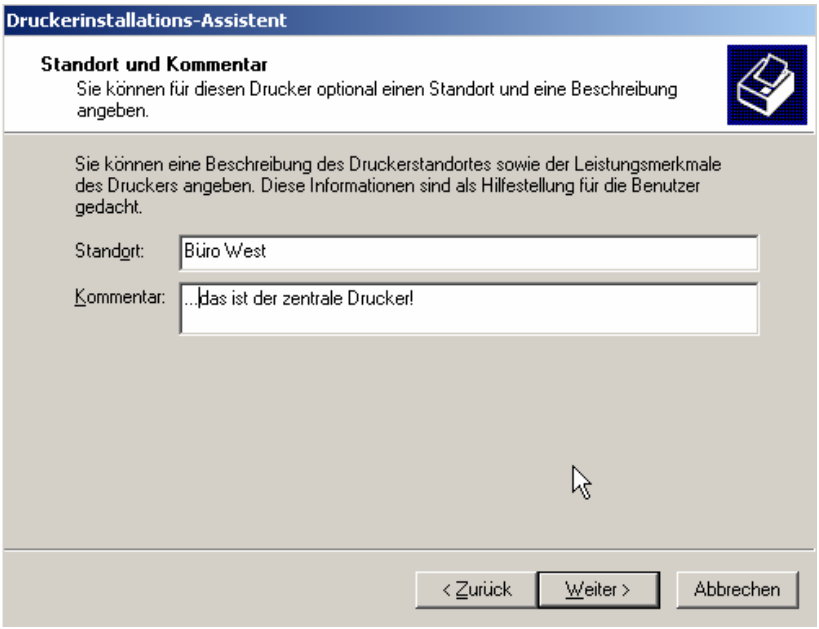


Abb. 92: Standort und Kommentar angeben

11. Wählen Sie, ob Sie eine Testseite drucken möchten, und klicken Sie auf WEITER.
12. Wählen Sie, ob Sie einen weiteren Drucker installieren möchten, und klicken Sie auf FERTIG STELLEN.

Die Installation eines lokalen Druckers und dessen Freigabe im Netzwerk ist hiermit abgeschlossen.

9.5.4 Druckerinstallation via Start Script in Active Directory

In einem Netzwerk mit installiertem Active Directory können Sie verschiedene Verwaltungsaufgaben, die regelmäßig beim Starten und Beenden von Clientrechnern ausgeführt werden sollen, in ein Script schreiben, das automatisch ausgeführt wird.

Dazu benötigen Sie ein Script, das je nach dem anzumeldenden Client einen entsprechenden Drucker auswählt und die Verbindung mit diesem herstellt.

Nachfolgendes Script ist ein Beispiel dafür, wie Sie einem Client via Windows Scripting Host (WSH) beim Starten einen freigegebenen Drucker zuweisen.

```
'---------------------------------------------------------
'Ausblenden eventueller Fehlermeldungen
'---------------------------------------------------------
on error resume next
```

```
'-------------------------------------------------------------
'Instanzieren des Windows Scripting Hosts
'-------------------------------------------------------------
Set Network = CreateObject("Wscript.Network")

'-------------------------------------------------------------
'Löschen eventuell bestehender Printerconnections
'-------------------------------------------------------------
For i = 0 To network.EnumPrinterConnections.Count - 1
    On Error Resume Next
    network.RemovePrinterConnection
network.EnumPrinterConnections.Item(i)
Next
'-------------------------------------------------------------
'Auslesen der ersten 4 Buchstaben des Computernamens
'-------------------------------------------------------------
sPCName = UCase(Left(network.ComputerName, 4))
'-------------------------------------------------------------
'Zuweisen der jeweiligen Drucker sowie des Defaultdruckers
'-------------------------------------------------------------
Select Case sPCName
Case "PC01"
    PrinterShare = "\\ITMain\Raum1Color"
    network.AddWindowsPrinterConnection PrinterShare
    PrinterShare = "\\ITMain\Raum_1_Laser"
    network.AddWindowsPrinterConnection PrinterShare
    network.SetDefaultPrinter PrinterShare
Case "PC02"
    PrinterShare = "\\ITMain\Raum1Color"
    network.AddWindowsPrinterConnection PrinterShare
    PrinterShare = "\\ITMain\Raum_2"
    network.AddWindowsPrinterConnection PrinterShare
    network.SetDefaultPrinter PrinterShare
Case "PC03"
    PrinterShare = "\\ITMain\Raum1Color"
    network.AddWindowsPrinterConnection PrinterShare
    PrinterShare = "\\ITMain\Raum_3"
```

© 2005, Microsoft Österreich GmbH

```
    network.AddWindowsPrinterConnection PrinterShare
    network.SetDefaultPrinter PrinterShare
End Select
```

Das angegebene Script ist lediglich ein Beispiel und nur für die Verwendung mit Windows 2000-Clients gedacht, in der hier vorliegenden Form jedoch nicht für den produktiven Einsatz geeignet!

Nähere Informationen zu Scripting im Allgemeinen und dem hier angeführten Startskript im Besonderen finden im Hilfe & Support-Center.

9.6 Drucker im Active Directory veröffentlichen

9.6.1 Allgemeines

Das Veröffentlichen eines Druckers im Active Directory hat zur Folge, dass Benutzer diesen Drucker suchen und sich mit ihm verbinden können.

Folgende Punkte sind zu beachten:

- Nur ein Drucker, der für die gemeinsame Nutzung freigegeben ist, kann veröffentlicht werden. Wenn Sie die Freigabe zurückziehen, wird die Veröffentlichung des Druckers automatisch aufgehoben.
- Wenn Sie den Druckerinstallations-Assistenten benutzen, um einen Drucker hinzuzufügen, und den Drucker dann freigeben, wird dieser automatisch in einem vorhandenen Active Directory veröffentlicht.

Vorraussetzung dafür ist jedoch, dass Sie innerhalb der GRUPPENRICHTLINIEN die Option NEUE DRUCKER AUTOMATISCH IM ACTIVE DIRECTORY VERÖFFENTLICHEN und die Option VERÖFFENTLICHEN VON DRUCKERN ZULASSEN aktiviert haben, was standardmäßig der Fall ist!

- Drucker werden vollautomatisch freigegeben, wenn Sie den **Druckerinstallations-Assistent** von einem Computer ausführen, auf dem Windows Server 2003 ausgeführt wird. Wenn Sie den **Druckerinstallations-Assistent** von einem Computer ausführen, auf dem Windows XP läuft, werden Drucker NICHT automatisch freigegeben.
- Sie müssen zum Verwalten eines Druckers berechtigt sein, um einen Drucker freigeben und veröffentlichen zu können.

9.6.2 Veröffentlichen des Druckers

So veröffentlichen Sie einen Drucker im Active Directory unter Windows Server 2003:

1. Öffnen Sie die Ansicht DRUCKER UND FAXGERÄTE.
2. Klicken sie mit der rechten Maustaste auf den Drucker, der veröffentlicht werden soll und wählen Sie den Punkt FREIGABE...
3. Auf dem Register FREIGABE markieren Sie die Option DRUCKER FREIGEBEN und wählen einen entsprechenden Namen.
4. Markieren Sie die Checkbox IM ACTIVE DIRECTORY VERÖFFENTLICHEN

5. Klicken Sie auf ÜBERNEHMEN.

Der Drucker ist nun im Active Directory veröffentlicht.

9.7 Drucker-Pooling

9.7.1 Allgemeines

Sie können einen Druckerpool erstellen, um Druckaufträge automatisch zum nächsten verfügbaren Drucker weiterzuleiten. Ein Druckerpool ist ein logischer Drucker, der durch mehrere Anschlüsse des Druckerservers mit mehreren Druckern verbunden ist. Der jeweils im Leerlauf befindliche Drucker erhält das nächste an den logischen Drucker gesendete Dokument. Dies ist in einem Netzwerk mit einem hohen Druckaufkommen nützlich, weil die Benutzer ihre Dokumente schneller erhalten. Ein Druckerpool vereinfacht auch die Verwaltung, da mehrere Drucker auf einem Server vom selben logischen Drucker aus verwaltet werden können.

Wenn ein Druckerpool eingerichtet ist, können Benutzer ein Dokument drucken, ohne nach einem verfügbaren Drucker suchen zu müssen. Der logische Drucker sucht einen freien Anschluss und sendet Dokumente in der Reihenfolge, in der sie hinzugefügt wurden, an die Anschlüsse. Wenn zuerst der Anschluss hinzugefügt wird, der mit dem schnellsten Drucker verbunden ist, ist gewährleistet, dass Dokumente zuerst an diesen schnellen Drucker gesendet werden, bevor sie an langsamere Drucker im Druckerpool gehen.

Beachten Sie vor dem Einrichten eines Druckerpools folgende Hinweise:

- Für das Drucker-Pooling müssen die Drucker vom gleichen Typ sein sowie den gleichen Druckertreiber verwenden.
- Weil die Benutzer nicht wissen können, auf welchem Drucker in einem Pool ihr Dokument ausgedruckt wird, sollten Sie alle Drucker an einem Standort versammeln.

9.7.2 Einrichten eines Druckerpools

So erstellen Sie einen Druckerpool

1. Wählen Sie START und klicken Sie auf DRUCKER UND FAXGERÄTE.
2. Klicken Sie mit der rechten Maustaste auf den verwendeten Drucker, und klicken Sie dann auf EIGENSCHAFTEN.
3. Aktivieren Sie auf der Registerkarte ANSCHLÜSSE das Kontrollkästchen AKTIVIEREN.
4. Wählen sie die Option DRUCKERPOOL AKTIVIEREN aus.
5. Klicken Sie auf die Anschlüsse, an denen Drucker angeschlossen sind, die zu einem Pool zusammengeführt werden sollen.
6. Klicken Sie auf ÜBERNEHMEN.

Die ausgewählten Drucker wurden zu einem Druckerpool zusammengefasst. Wenn ein Benutzer nun einen Druckauftrag an den Drucker sendet, wird der Auftrag an den nächsten freien Drucker weitergegeben und dort verarbeitet.

Die Drucker eines Druckerpools müssen vom gleichen Typ sein und denselben Druckertreiber verwenden.

Bei dem gerade beschriebenen Verfahren wird vorausgesetzt, dass die Drucker, die im Pool zusammengefasst werden sollen, sich bereits im Ordner **Drucker und Faxgeräte** befinden. Andernfalls müssen Sie die Drucker, die Sie zu einem Pool zusammenfassen wollen, erst als Drucker einrichten.

9.8 Ändern der Priorität von Druckaufträgen

9.8.1 Allgemeines

Mit Hilfe der Priorisierung kann man einzelnen Dokumenten, aber auch ganzen Benutzergruppen, eine bevorzugte Abarbeitung durch den Drucker und das Druckgerät ermöglichen.

Es hat keine Auswirkungen, wenn Sie eine Priorität lediglich für einen Drucker festlegen. Sie müssen mindestens zwei verschiedene logische Drucker für denselben physikalischen Drucker festlegen, um die Vorteile dieser Option nutzen zu können.

9.8.2 Ändern der Priorität einzelner Druckaufträge

So ändern Sie die Priorität für einzelne Dokumente

1. Öffnen Sie die Druckauftragsverwaltung, indem Sie auf das Symbol in der Taskleiste klicken.
2. Klicken Sie mit der rechten Maustaste auf das Dokument, für das Sie die Priorität ändern wollen.
3. Auf der Registerkarte ALLGEMEIN geben Sie die gewünschte Priorität für den ausgewählten Druckauftrag ein.

   Die Einstellungsmöglichkeiten reichen von 1, sehr niedrig, bis 99 sehr hoch.

Standardmäßig wird eine sehr niedrige Priorität für alle Druckaufträge verwendet.

9.8.3 Ändern der Priorität von Druckaufträgen für eine Benutzergruppe

Um für unterschiedliche Benutzergruppen unterschiedliche Prioritäten anwenden zu können, müssen Sie jeweils für ein Druckgerät mindestens zwei logische Drucker anlegen.

So ändern Sie die Priorität von Druckaufträgen für eine Benutzergruppe

1. Wählen Sie **Start** und klicken Sie auf **Drucker und Faxgeräte**
2. Klicken Sie mit der rechten Maustaste auf den verwendeten Drucker, und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie die Registerkarte ERWEITERT und vergeben Sie eine entsprechende Priorität für diesen logischen Drucker.
4. Klicken Sie auf ÜBERNEHMEN.
5. Klicken Sie auf DRUCKER HINZUFÜGEN.
6. Installieren Sie einen neuen logischen Drucker für dasselbe Druckgerät.
7. Vergeben Sie auf der Registerkarte ERWEITERT eine höhere oder geringere Priorität als beim vorherigen Drucker.
8. Vergeben Sie die entsprechenden Rechte auf den Druckern.
9. Stellen Sie sicher, dass die Benutzer die richtigen logischen Drucker verwenden.

© 2005, Microsoft Österreich GmbH

Sie haben nun einer Benutzergruppe eine höhere Priorität auf dem Druckgerät zugewiesen. Druckaufträge, die von der Benutzergruppe mit der höheren Priorität ausgehen, werden nun vorrangig behandelt.

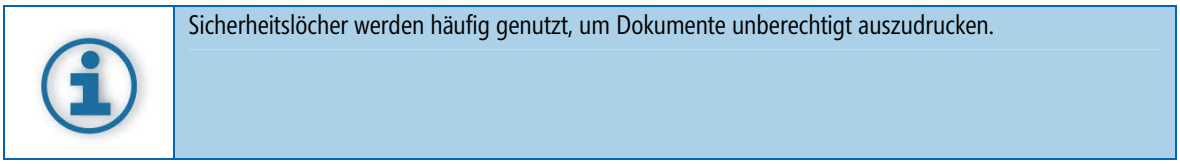
9.9 Verwaltung der Berechtigungen auf einem Drucker

9.9.1 Allgemeines

Ist in einem Netzwerk ein Drucker installiert, werden standardmäßige Druckerberechtigungen zugewiesen, die allen Benutzern das Drucken ermöglichen. Darüber hinaus können Gruppen für die Verwaltung des Druckers und der an den Drucker gesendeten Dokumente eingerichtet werden. Da der Drucker allen Benutzern im Netzwerk zur Verfügung steht, empfiehlt es sich, den Zugriff für bestimmte Benutzer durch das Zuweisen von Druckerberechtigungen zu beschränken. Sie können beispielsweise allen Schülern einer Klasse die Berechtigung DRUCKEN und allen Lehrkräften die Berechtigungen DRUCKEN und DOKUMENTE VERWALTEN zuweisen. Auf diese Weise können alle Benutzer Dokumente drucken, es ist jedoch nur den Lehrkräften möglich, den Status der an den Drucker gesendeten Dokumente zu ändern.

Grundsätzlich bietet es sich an, auch die Rechte über Drucker einzuschränken. Windows Server 2003 bietet Ihnen hier mehrere Möglichkeiten, die Verwaltung der Drucker von der reinen Benutzung zu trennen und so ein Maximum an Sicherheit zu gewährleisten.

Das Vergeben von Rechte kann möglicherweise verhindern, dass nicht berechtigte Benutzer Dokumente ausdrucken und so sensible Daten entwenden.



9.9.2 Verfügbare Rechte für das Drucken

In Windows stehen drei Ebenen von Sicherheitsberechtigungen für das Drucken zur Verfügung:

- Drucken
- Drucker verwalten
- Dokumente verwalten

Für Benutzergruppen, denen mehrere Berechtigungen zugewiesen sind, gelten die am wenigsten einschränkenden Berechtigungen. Wenn jedoch „Verweigern“ aktiviert ist, hat dies Vorrang vor jeder anderen Berechtigung. Nachfolgend finden Sie eine kurze Erläuterung der Aufgaben, die Benutzer auf der jeweiligen Berechtigungsebene ausführen können.

Drucken

Der Benutzer kann eine Verbindung zu einem Drucker herstellen und Druckaufträge an diesen Drucker senden. In der Standardeinstellung ist die Berechtigung „Drucken“ allen Mitgliedern der Gruppe JEDER zugewiesen.

Drucker verwalten

Der Benutzer kann die mit der Berechtigung „Drucken“ verbundenen Aufgaben ausführen und den Drucker darüber hinaus vollständig verwalten. Der Benutzer kann den Drucker anhalten und neu starten, die Spoolereinstellungen ändern, einen Drucker freigeben, Druckerberechtigungen anpassen und die Druckereigenschaften ändern. In der Standardeinstellung ist die Berechtigung „Drucker verwalten“ allen Mitgliedern der Gruppen „Administratoren“ und „Hauptbenutzer“ zugewiesen.

Die Mitglieder der Gruppen „Administratoren“ und „Hauptbenutzer“ verfügen standardmäßig über uneingeschränkten Zugriff, sie sind berechtigt zum „Drucken“, „Drucker verwalten“ und „Dokumente verwalten“.

Dokumente verwalten

Der Benutzer kann gesendete Dokumente aller anderen Benutzer anhalten, wieder aufnehmen, neu starten, abbrechen und deren Reihenfolge ändern. Das Senden von Dokumenten zum Drucker und die Steuerung des Druckerstatus sind jedoch nicht möglich. In der Standardeinstellung ist die Berechtigung „Dokumente verwalten“ den Mitgliedern der Gruppe „Ersteller-Besitzer“ zugewiesen.

Wenn einem Benutzer die Berechtigung „Dokumente verwalten“ zugewiesen wird, kann er nicht auf Dokumente zugreifen, die sich bereits in der Druckerwarteschlange befinden. Die Berechtigung gilt nur für Dokumente, die an den Drucker gesendet werden, nachdem dem Benutzer die Berechtigung zugewiesen wurde.

Verweigern

Für den Drucker werden alle vorangegangenen Berechtigungen verweigert. Wenn der Zugriff verweigert wird, kann der Benutzer den Drucker nicht verwenden oder verwalten und keine Berechtigungen anpassen.

9.9.3 Freigaben und Zugriffsberechtigungen

Sie können die Berechtigungen über Drucker direkt setzen, indem Sie einzelnen Benutzern oder Gruppen die Berechtigungen erteilen.

So geben Sie Benutzern unterschiedliche Rechte auf Drucker:

1. Wählen Sie START und DRUCKER UND FAXGERÄTE.
2. Klicken Sie mit der rechten Maustaste auf den entsprechenden Drucker und wählen Sie den Punkt EIGENSCHAFTEN aus.
3. Klicken Sie auf die Registerkarte SICHERHEIT.
4. Um gezielt einzelnen Benutzern oder Gruppen Rechte zu erteilen entfernen Sie die Gruppe „Jeder“ indem Sie darauf klicken und die Option ENTFERNEN wählen.

Das Belassen der Gruppe „Jeder“ im Active Directory und das Verweigern von gewissen Aktionen für diese Gruppe können zu schwerwiegenden Berechtigungsproblemen führen. Da die „Verweigern“-Richtlinien IMMER vor den „Zulassen“-Rechten ausgewertet werden, kann es passieren, dass zulässige Aktionen vorher verweigert wurden und dadurch nicht mehr zum Tragen kommen!

5. Fügen Sie die entsprechenden Benutzer oder Gruppen hinzu, indem Sie diese angeben beziehungsweise auswählen.
6. Vergeben Sie die entsprechenden Rechte.

Der Drucker steht den Benutzern ab sofort nur noch innerhalb der vergebenen Rechte zur Verfügung.

9.9.4 Gruppenrichtlinien und Drucker

Mit den Gruppenrichtlinien steht dem Administrator ein mächtiges Werkzeug zur Verfügung, um zu bestimmen, wie die Systemumgebung für einen Benutzer oder eine Benutzergruppe aussieht und welche Applikationen ihnen zur Verfügung stehen.

Gruppenrichtlinien können auch dazu dienen, die Nutzung eines Druckers zu regeln. Unter anderem können so gewisse Einstellungen gewissen Benutzern zugeordnet werden, aber auch die Berechtigungen zum Ändern, Löschen, Freigeben und Hinzufügen von Druckern geregelt werden.

© 2005, Microsoft Österreich GmbH

In Windows werden sechs Gruppen von Benutzern Druckerberechtigungen zugewiesen. Dabei handelt es sich um die Gruppen **Administratoren**, **Ersteller-Besitzer**, **Jeder**, **Hauptbenutzer**, **Druck-Operatoren** und **Server-Operatoren**.

In der Standardeinstellung ist jeder Gruppe eine Kombination der Berechtigungen **Drucken**, **Dokumente verwalten** und **Drucker verwalten** zugewiesen, wie in der folgenden Tabelle dargestellt ist.

Gruppe	Drucken	Dokumente verwalten	Drucker verwalten
Administratoren	X	X	X
Ersteller-Besitzer		X	
Jeder	X		
Hauptbenutzer	X	X	X
Druck-Operatoren	X	X	X
Server-Operatoren	X	X	X

Die Gruppen **Druck-Operatoren** und **Server-Operatoren** sind nur auf Domänencontrollern verfügbar.

Jede Berechtigung besteht aus einer Gruppe von Rechten, die dem Benutzer die Ausführung bestimmter Aufgaben ermöglicht. Die folgende Tabelle bietet eine Übersicht über die Zugriffsstufen, die den verschiedenen Sicherheitsberechtigungen für das Drucken zugeordnet sind.

Zugelassene Aufgaben	Dokumente verwalten	Drucker verwalten
Drucken		X
Drucker verwalten		X
Dokumente verwalten	X	
Berechtigungen lesen	X	X
Berechtigungen ändern	X	X
Besitz übernehmen	X	X

Nähere Informationen zum Anwenden von Gruppenrichtlinien erhalten Sie im entsprechenden Kapitel weiter vorn im Skriptum beziehungsweise im Hilfe & Support-Center!

© 2005, Microsoft Österreich GmbH

9.10 Überwachen von Druckvorgängen

Eine weitere, häufig auftretende Aufgabe ist das Überwachen von Druckaufträgen und das entsprechende Protokollieren derselben.

Windows Server 2003 bietet Ihnen mittels der bereits bekannten Gruppenrichtlinien die Möglichkeit, gewisse Druckaufträge von einzelnen Benutzern oder Gruppen aufzuzeichnen.

So aktivieren Sie die Protokollierung von Druckaufträgen:

1. Wählen Sie START und DRUCKER UND FAXGERÄTE.
2. Klicken Sie mit der rechten Maustaste auf den entsprechenden Drucker und wählen Sie den Punkt EIGENSCHAFTEN aus.
3. Klicken Sie auf die Registerkarte SICHERHEIT.
4. Klicken Sie auf die Schaltfläche ERWEITERT.
5. Klicken Sie auf die Registerkarte ÜBERWACHUNG.

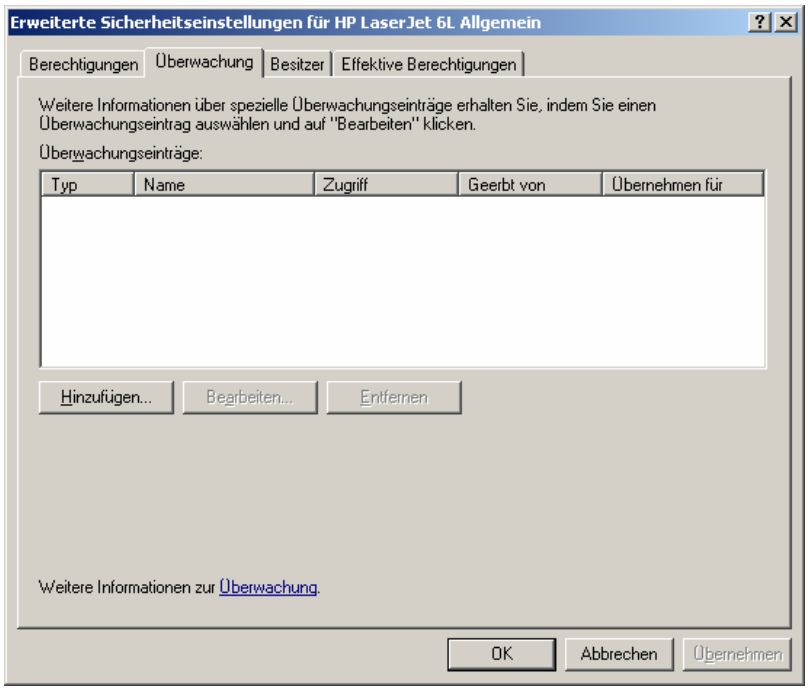


Abb. 93: Ansicht Überwachung für Drucker

6. Klicken Sie auf die Schaltfläche HINZUFÜGEN.
7. Wählen Sie die Benutzer oder Gruppen aus, für die Sie gewisse Protokolleinstellungen definieren wollen.

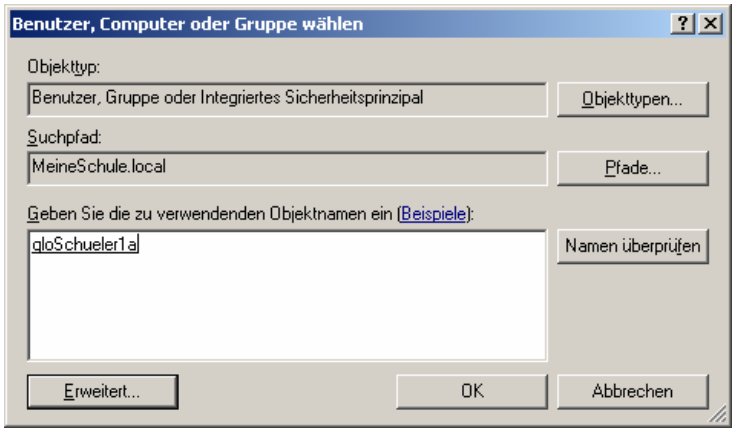


Abb. 94: Auswahl der Benutzer oder Gruppen

8. Definieren Sie nun die entsprechenden Aktionen aus, die protokolliert werden sollen, und bestätigen Sie die Auswahl mit OK.

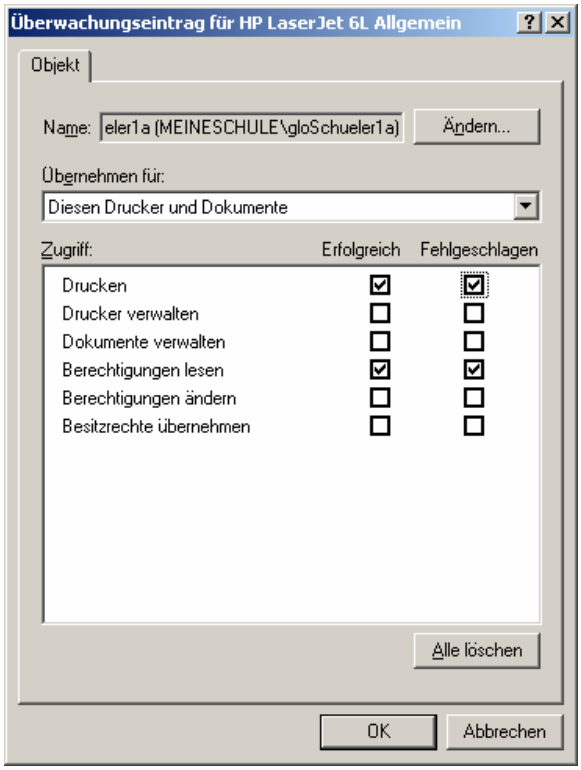


Abb. 95: Auswahl der Aktionen, die protokolliert werden

9. Sie sehen nun die erstellte Gruppenrichtlinie in der Liste auf der Registerkarte ÜBERWACHUNG.

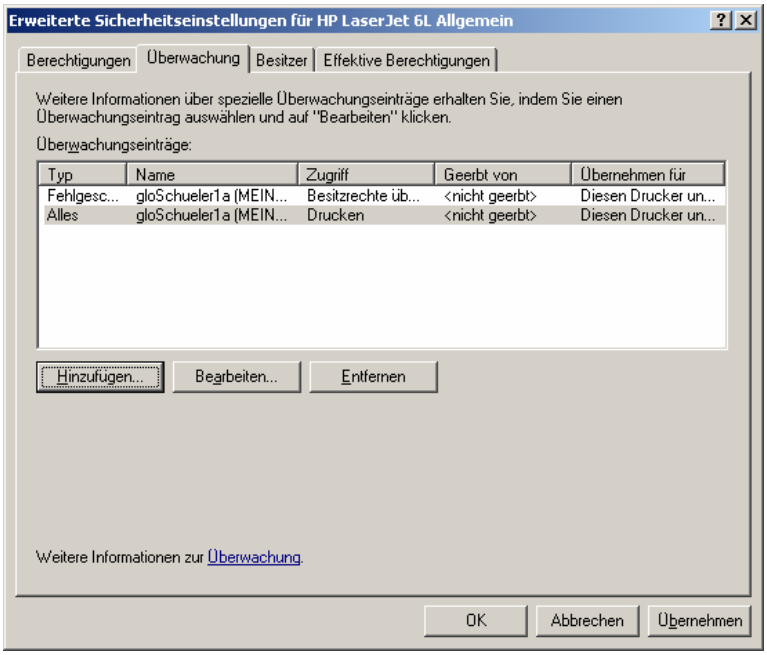


Abb. 96: Ansicht Überwachung für Drucker mit erstellter Gruppenrichtlinie

9.11 Internetdrucken

Das so genannte Internetdrucken ermöglicht Ihnen das Drucken, das Herstellen einer Verbindung zu einem Drucker und das Verwalten von Druckern über das Internet mittels eines Webbrowsers.

Nähere Informationen dazu erhalten sie im Anhang A *Internet Information Services 6.0*.

10 Datensicherung

Dieses Kapitel erläutert die Implementierung und Konfiguration der Datensicherung und eines Sicherungskonzepts unter Windows Server 2003

10.1 Basiswissen

Das Sicherungsprogramm in Windows Server 2003 bewahrt Sie vor dem Verlust Ihrer Daten. Ursache dafür könnten Hardwareausfälle (z. B. technische Defekte von Festplatten) oder (un)beabsichtigtes Löschen oder Überschreiben von Dateien sein.

Mit dem Sicherungsprogramm können Sie Ihre Daten auf verschiedene Speichermedien duplizieren und dort archivieren. Als Backup-Speichermedien können u. a. logische Laufwerke, andere Festplatten, Bandlaufwerke oder Speicher-Arrays (bestehend aus mehreren Festplatten oder mehreren Bandlaufwerken) genutzt werden.

10.1.1 Funktionalität des Sicherungsprogramms

Das Sicherungsprogramm kann auch die unter Windows Server 2003 neu eingeführten "Schattenkopien" von Laufwerken (engl. "Volume Shadow Copies") für Datensicherungen nutzen. Mit diesen wird es möglich, alle Dateien lückenlos zu sichern, selbst geöffnete. Benutzer können während der Sicherung mit den zu sichernden Daten weiterarbeiten.

Eine Schattenkopie ist ein Duplikat eines Original-Datenträgers zum Zeitpunkt der Erstellung der Kopie. Sie werden zyklisch (terminplangesteuert) vom "Volumeschattenkopie"-Dienst (engl. "Volume Shadow Copy Service") erstellt. Dabei werden jeweils nur die Veränderungen seit dem letzten Schattenkopie-Prozess gespeichert.

Das Sicherungsprogramm eröffnet Ihnen folgende Möglichkeiten:

- Duplizieren/Archivieren ausgewählter Dateien und Ordner auf einem Backup-Speichermedium
- Wiederherstellen archivierter Dateien und Ordner auf einem primären Speichermedium, z. B. auf der selben oder einer anderen Festplatte
- Nutzen der sog. "Automatischen Systemwiederherstellung" (engl. "Automated System Recovery - ASR") für das Sichern und Wiederherstellen von Systemdateien und der Systemkonfiguration nach einem vollständigen Systemausfall
- Kopieren von Daten auf entfernte (remote) Speichermedien (z. B. Remote Storage Services oder File Shares)
- Kopieren des "Systemzustands" (engl. "System State") des lokalen Systems
- Kopieren aller für den Bootvorgang erforderlichen (System-)Dateien auf der System-/Bootpartition
- Steuerung von Sicherungs- und Wiederherstellungsprozessen durch definierte Terminpläne
- Protokollieren von Sicherungs- und Wiederherstellungsprozessen
- Formatieren der sekundären (Ziel-)Speichermedien (z. B. Bänder)

10.1.2 Unterstützte Dateisysteme

Die auf den verwendeten Quell- und Zielspeichermedien unterstützten Dateisysteme sind FAT16, FAT32 und NTFS.

10.1.3 Sicherungsmethoden

Das Sicherungsprogramm in Windows Server 2003 unterstützt folgende fünf Methoden der Datensicherung:

- **Kopieren:** Kopiert alle ausgewählten Dateien, markiert sie jedoch nicht als "gesichert" (Archiv-Attribut wird nicht verändert). Diese Methode ist z. B. sinnvoll für Ad-hoc-Sicherungen zwischen geplanten Sicherungsprozessen.
- **Täglich:** Kopiert alle ausgewählten Dateien, die am Tag der täglichen Sicherung erstellt oder geändert wurden. Die gesicherten Dateien werden nicht als "gesichert" markiert (Archiv-Attribut wird nicht verändert).
- **Differenziell:** Kopiert jene Dateien, die seit der letzten normalen oder differenziellen Sicherung erstellt oder geändert wurden. Die gesicherten Dateien werden nicht als "gesichert" markiert (Archiv-Attribut wird nicht verändert).

Wenn die beiden Methoden "Normal" und "Differenziell" miteinander kombiniert werden, ist für das vollständige Wiederherstellen der Daten die letzte normale und die letzte differenzielle Sicherung erforderlich.

- **Inkrementell:** Kopiert jene Dateien, die seit der letzten normalen oder inkrementellen Sicherung erstellt oder geändert wurden. Die gesicherten Dateien werden als "gesichert "markiert (Archiv-Attribut wird verändert).

Wenn die Methoden "Normal " und "Inkrementell" miteinander kombiniert werden, ist für das vollständige Wiederherstellen der Daten die letzte normale und alle dazwischen liegenden inkrementellen Sicherungen – seit der letzten normalen Sicherung - erforderlich.

- **Normal:** Kopiert alle ausgewählten Dateien und markiert sie als "gesichert" (Archiv-Attribut wird verändert). Für das Wiederherstellen von Daten ist die letzte normale Sicherung erforderlich. Diese Sicherungsmethode wird üblicherweise beim erstmaligen Erstellen eines Sicherungs-Sets durchgeführt.

Weiter können Sie die Volumeschattenkopien für Sicherungsoperationen nutzen (siehe 10.1.1).

10.1.4 Erforderliche Berechtigungen für Datensicherungen

Administrative Berechtigungen

Um Sicherungen vornehmen zu dürfen, sind bestimmte Berechtigungen erforderlich. Als "Administrator" oder "Sicherungs-Operator" auf einem lokalen System können Daten dieses lokalen Systems gesichert werden.

Wenn man Mitglied in einer dieser Benutzergruppen in einer Domäne ist, können Daten auf allen Computern dieser Domäne gesichert werden bzw. auch Daten von Domänen, zu denen Vertrauensstellungen bestehen.

Minimalberechtigung, Datenträgerkontingente

Die Minimalberechtigung für Sicherungen verlangt es, Besitzer der betreffenden Dateien zu sein, wenn die o. g. Gruppenmitgliedschaften nicht gegeben sind.

© 2005, Microsoft Österreich GmbH

10.1.5 Systemzustand-Daten

Das Sicherungsprogramm ermöglicht das Sichern und Wiederherstellen aller Daten, die den aktuellen Zustand des Systems repräsentieren:

- Registry (immer)
- COM+ Class Registration Database (immer)
- Boot- und Systemdateien (immer)
- Certificate Services Database (auf einem Certificate Server)
- Active Directory (wenn Domäne vorhanden)
- SYSVOL Directory (auf einem Domänencontroller)
- Cluster Service Information (wenn Cluster vorhanden)
- IIS Metadirectory (wenn installiert)
- Geschützte Systemdateien (immer)

10.1.6 Spezielle Wiederherstellungsmethoden

Die Daten verteilter Dienste (z. B. Active Directory) sind Bestandteil der sog. "Systemzustand-Daten" (System State). Diese Daten können mit folgenden Methoden wiederhergestellt werden:

- Primäre Wiederherstellung
- Normale (nicht-autoritative) Wiederherstellung
- Autoritative Wiederherstellung

Welche der drei Methoden zur Wiederherstellung der Daten verteilter Dienste genutzt werden kann, ist von der Anzahl und der Konfiguration vorhandener Domänencontroller abhängig.

Primäre Wiederherstellung

Nutzen Sie diese Wiederherstellungsmethode, wenn der wiederherzustellende Server der einzige laufende Server mit replizierten Systemdaten ist und das erste Replikat von Systemdaten wiederhergestellt werden soll. Nutzen Sie diese Methode nicht, wenn eines oder mehrere Replikate von Systemdaten bereits wiederhergestellt worden sind. Ein typisches Anwendungsszenario für eine primäre Wiederherstellung ist jenes, wenn alle Domänencontroller ausgefallen sind und die Domäne auf einem Server von einer Sicherung wiederhergestellt werden soll.

Normale (nicht-autoritative) Wiederherstellung

Diese Methode wird im "nicht-autoritativen Wiederherstellungsmodus" (engl. "Nonauthoritative Restore Mode") durchgeführt. Alle wiederhergestellten Systemdaten (inkl. Active Directory-Objekte) haben die originale "Aktualisierungssequenz-Nummer" (engl. "Update Sequence Number"). Diese wird vom Active-Directory-Replikationssystem genutzt, um Veränderungen im Active Directory quer durch alle Server festzustellen.

Wenn durch eine normale Wiederherstellung (engl. "normal restore") wiederhergestellte Active-Directory-Daten zwischenzeitlich veraltet sind, werden diese nicht auf andere Server repliziert. Stattdessen werden die gesicherten Daten durch die aktuellen Daten (anderer Server) ersetzt.

Typische Anwendungsfälle für die Wiederherstellung von (verteilten) Systemdaten mittels normaler Wiederherstellung sind z. B.:

© 2005, Microsoft Österreich GmbH

Verteilte Daten	Grund für die Wiederherstellung
Active Directory	Wiederherstellen eines Single Domänencontrollers in einer replizierten Umgebung
SYSVOL	Wiederherstellen eines Single Domänencontrollers in einer replizierten Umgebung
Replica Sets	Wiederherstellen von Replikationssets mit Ausnahme des ersten Sets

Autoritative Wiederherstellung

Diese Methode arbeitet wie die normale Wiederherstellung, lediglich werden wiederhergestellte Systemdaten des Active Directory auf andere Server repliziert. Hierzu ist allerdings die Anwendung von "Ntdsutil" erforderlich. Mit Ntdsutil können Active-Directory-Objekte für eine autoritative Wiederherstellung markiert werden, was wiederum die Replikation auf andere Server zur Folge hat.

Ntdsutil ist ein Kommandozeilenprogramm, das Verwaltungsfunktionen für das Active Directory zur Verfügung stellt.

Anwendungsfälle für autoritative Wiederherstellungen sind:

Verteilte Daten	Grund für die Wiederherstellung
Active Directory	Rollback (unbeabsichtigter) Veränderungen
SYSVOL	Reset von Daten
Replica Sets	Rollback (unbeabsichtigter) Veränderungen

10.1.7 Recovery Console

Die Recovery Console ist ein Kommandozeilenprogramm, das zur Systemreparatur und -wiederherstellung genutzt werden kann. Die Nutzung dieses Werkzeugs ist z. B. dann erforderlich, wenn das Betriebssystem nicht mehr gestartet werden kann, auch nicht im "Sicheren Modus" (engl. "Safe Mode"). Die Recovery Console kann von der Setup-CD gestartet oder auf der Festplatte installiert werden. Im zweiten Fall kann beim Booten des Systems die Recovery Console als eigene Bootoption gewählt werden.

Die Recovery Console stellt alle für eine Reparatur eventuell erforderlichen Funktionen zur Verfügung (in Verzeichnisse wechseln bzw. deren Inhalte anzeigen, Dateien kopieren, Aktivieren einer bestimmten Installation auf einem Multiple-Boot-System etc.).

Um die Recovery Console benutzen zu können, benötigen Sie das Administrator-Konto der betreffenden Server-Installation.

10.1.8 Automatische Systemwiederherstellung

Mit dem Sicherungsprogramm ist es möglich, so genannte ASR-Sets für die automatische Systemwiederherstellung zu erstellen. ASR (Automated System Recovery) wird beispielsweise dann genutzt, wenn eine Server-Installation durch spezielle Startoptionen ("Sicherer Modus", "Letzte funktionierende Konfiguration") nicht mehr gestartet werden kann.

ASR besteht aus zwei Teilen:

- ASR-Sicherung
- ASR-Wiederherstellung

ASR-Sicherung

ASR-Sets werden mit dem "Assistent für die Vorbereitung der automatischen Systemwiederherstellung" erstellt, der vom Sicherungsprogramm aus gestartet werden kann.

Dieser Assistent sichert die Daten

- des Systemzustands (System State),
- der Systemdienste und
- aller Laufwerke, auf denen sich Komponenten des Betriebssystems befinden

und erstellt eine Diskette mit Informationen über

- die Sicherung,
- die Laufwerkskonfigurationen und
- die Wiederherstellung.

ASR-Restore

Auf den Wiederherstellungsteil von ASR kann zugegriffen werden, indem man im Textmodus des Windows-Setup die Taste **F2** drückt. ASR funktioniert dann wie folgt:

- Es liest die Laufwerkskonfiguration (Signaturen, Volumes, Partitionen) von der Diskette und stellt diese auf den betreffenden Laufwerken wieder her.
- Es installiert anschließend eine Minimalvariante des Betriebssystems und beginnt danach automatisch mit der Wiederherstellung der ASR-Sets.

10.2 Sichern/Wiederherstellen - Voraussetzungen

10.2.1 Daten sichern

Um effizient und zielgerichtet Sicherungen von Daten erstellen zu können, müssen bestimmte Voraussetzungen erfüllt werden. Diese sind in der folgenden Checkliste beschrieben:

- Aneignen von Basiswissen über Sicherungskonzepte und -methoden
- Überprüfen, ob die für eine Datensicherung erforderlichen Berechtigungen vorhanden sind. Diese sind gegeben, wenn man
  - Mitglied der Benutzergruppen "Administratoren" oder "Sicherungs-Operatoren" (am lokalen System oder in der Domäne)
  - oder Besitzer der zu sichernden Dateien

  ist.

- Überprüfen, ob der Zugriff auf die zu sichernden Dateien möglich ist:
  - Ist der Zugriff auf entfernte (remote) Daten möglich (File Shares)?

Es ist nicht möglich, den Systemzustand (System State) eines entfernten Systems zu sichern. Eine Alternative dazu wäre die Sicherung des Systemzustandes auf die lokale Platte des Servers. Diese Datei wird dann durch einen Remotezugriff über eine Datenfreigabe auf ein Band gesichert.

Eine weitere Möglichkeit wäre die Benutzung eines anderen, alternativen Sicherungsmediums wie z.B. USB-Disks.

- Bei der Verwendung externer Massenspeicher ist sicherzustellen, dass sie einwandfrei funktionieren, mit Windows Server 2003 kompatibel sind und direkt an den Computer angeschlossen sind, auf dem die Sicherung vorgenommen wird.
- Überprüfen, ob das Zielmedium (Band, Festplatte) ausreichend Speicherplatz für die zu sichernden Daten bietet.
- Überprüfen, ob das Zielmedium für die zu sichernden Daten verfügbar und einsatzbereit ist.
  - Bei Verwendung von Bandlaufwerken muss das entsprechende Band im Laufwerk eingelegt worden sein.
  - Wechselfestplatten müssen im Wechselschacht montiert sein und vom System erkannt werden.
- Beim Sichern verschlüsselter Dateisysteme muss zuerst der "private key" gesichert werden, um Daten wiederherstellen zu können.

10.2.2 Daten wiederherstellen

Beim Wiederherstellen von Daten sind – so wie beim Sichern auch – bestimmte Voraussetzungen zu erfüllen. Sie sind in der folgenden Checkliste beschrieben:

- Aneignen von Basiswissen über Wiederherstellungskonzepte und -methoden.
- Überprüfen, ob die für eine Datenwiederherstellung erforderlichen Berechtigungen vorhanden sind. Sie sind gegeben, wenn man Mitglied der Benutzergruppen "Administratoren" oder "Sicherungs-Operatoren" (am lokalen System oder in der Domäne) ist.
- Überprüfen, ob die Quellmedien mit den gesicherten Daten verfügbar sind (Bänder, Festplatten) und darauf zugegriffen werden kann.
- Überprüfen, ob das für die Wiederherstellung erforderliche Zielmedium verfügbar ist und darauf zugegriffen werden kann (File Shares, Wechselfestplatten etc.).
- Überprüfen, ob auf dem Zielmedium ausreichend Speicherplatz für die wiederherzustellenden Daten frei ist.
- Wenn der Systemzustand eines laufenden Domänencontrollers wiederhergestellt werden soll, muss dieser Server im "Verzeichnisdienste Wiederherstellungsmodus" (engl. "Directory Services Restore Mode") gestartet werden.

© 2005, Microsoft Österreich GmbH

10.3 Daten sichern

Zur Erstellung von Datensicherungen gibt es folgende Möglichkeiten:

- **Über die Windows-Benutzeroberfläche:** Die Windows-Benutzeroberfläche bietet die Möglichkeit der intuitiven Bedienung des Sicherungsprogramms, auch hier wieder in zwei Varianten:
  - **Der "Sicherungs- oder Wiederherstellungs-Assistent":** Wird das Sicherungsprogramm über die Benutzeroberfläche gestartet, zeigt es sich standardmäßig als Dialog in Form des "Sicherungs- oder Wiederherstellungs-Assistenten" (außer der Assistenten-Modus ist deaktiviert). Durch Klicken auf die Schaltfläche "Weiter" im Dialogfenster des Assistenten können nun sequenziell alle Einstellungen vorgenommen werden, die für die Erstellung eines Backup-Sets erforderlich sind. Sie reichen von der Auswahl der zu sichernden Dateien bis hin zur Definition von Aufträgen zur automatisierten Datensicherung.
  - **Die "Standard-Benutzeroberfläche":** Auf der Startseite des Assistenten gibt es aber auch die Möglichkeit, durch Klick auf den Link "Erweiterter Modus" in den erweiterten Modus zu wechseln, in dem die "Standard-Benutzeroberfläche" des Sicherungsprogramms geöffnet wird. Diese enthält die zur Erstellung einer Datensicherung erforderlichen Funktionen in Form eines tabellarischen Registers sowie in Form eines Menüs. Von diesem Dialogfenster kann durch Klicken auf die entsprechenden Schaltflächen (auf der Registerkarte "Willkommen") wieder zurück zu einzelnen Assistenten gewechselt werden (Sicherungs-, Wiederherstellungs-Assistent, Assistent für die automatische Systemwiederherstellung).
- **Über die Kommandozeile:** Das Sicherungsprogramm kann auch in einem Kommandozeilenfenster mit dem Kommando "ntbackup" gestartet werden. Alle für eine Datensicherung erforderlichen Einstellungen können diesem Kommando als Parameter übergeben werden.

Es ist allerdings nicht möglich mit "ntbackup" Daten wiederherzustellen.

Mit dem Aufruf von "ntbackup" über Batchdateien können auch komplexere Sicherungsoperationen realisiert werden. Der Aufruf der Batchdateien könnte wieder über Terminpläne gesteuert werden.

Wie erwähnt, beschreibt dieser Abschnitt lediglich die Methode der Nutzung des "Sicherungs- oder Wiederherstellungs-Assistenten". Die Benutzung der Standard-Benutzeroberfläche (Erweiterter Modus) oder des "ntbackup"-Befehls von der Kommandozeile aus wird in der Online-Hilfe und in der Technet-Bibliothek ausführlich beschrieben. Technet-Informationen zu Windows Server 2003 erhalten Sie via Internet unter

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/default.mspx

© 2005, Microsoft Österreich GmbH

10.3.1 Sicherungsprogramm starten

Das Sicherungsprogramm kann über die Benutzeroberfläche auf zwei verschiedene Arten gestartet werden:

- Über das Start-Menü
- Über den Eigenschaften-Dialog des zu sichernden Laufwerks

Beide Möglichkeiten des Startens sowie die Benutzung des Sicherungsprogramms sind in den folgenden Abschnitten beschrieben.

10.3.2 Sicherungsprogramm über das Start-Menü starten

Das Sicherungsprogramm rufen Sie über das Start-Menü wie folgt auf:

- Klicken Sie auf START – ALLE PROGRAMME – ZUBEHÖR und dann auf SYSTEMPROGRAMME. Hier wählen Sie den Eintrag SICHERUNG.

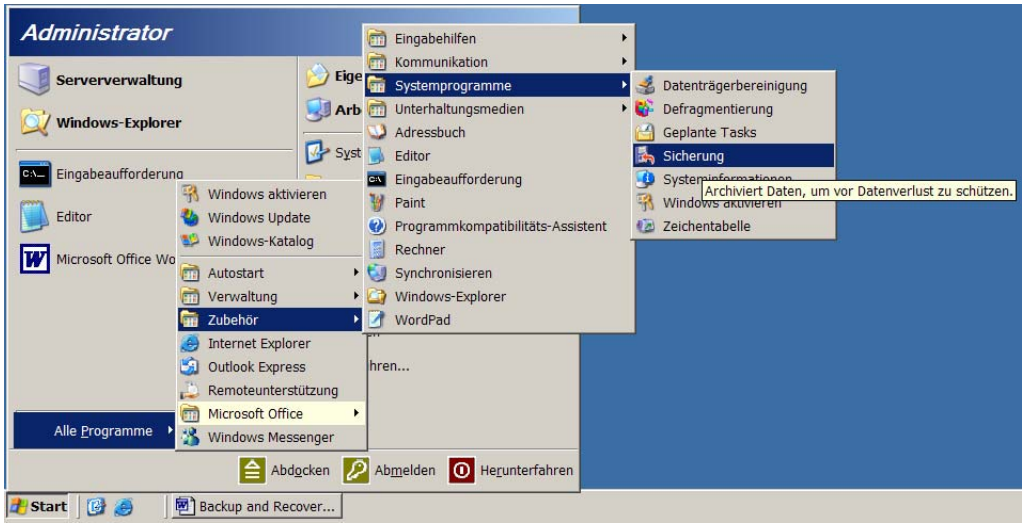


Abb. 97: Start-Menü - Sicherungsprogramm starten

- Das Dialogfenster "Sicherungs- oder Wiederherstellungs-Assistent" wird standardmäßig geöffnet (außer es ist deaktiviert, dann startet das Programm im "Erweiterten Modus" und zeigt die Standard-Benutzeroberfläche an).

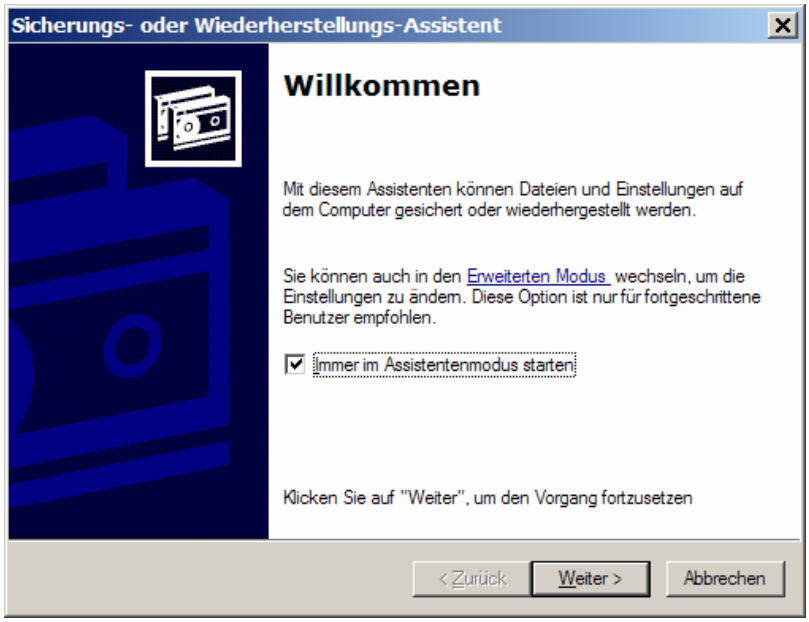


Abb. 98: Durchführen von Datensicherungen mit dem Assistent

Sicherungsprogramm über den Eigenschaften-Dialog des Laufwerks starten

Das Sicherungsprogramm kann auch über den Eigenschaften-Dialog des betreffenden Laufwerks gestartet werden. Dies funktioniert wie folgt:

- Klicken Sie im Start-Menü oder auf dem Windows-Desktop auf das Symbol ARBEITSPLATZ. Das Fenster ARBEITSPLATZ wird geöffnet.
- Klicken Sie dort mit der rechten Maustaste auf das Laufwerk mit den zu sichernden Daten (in der folgenden Abbildung ist dies beispielhaft das "Laufwerk E:").

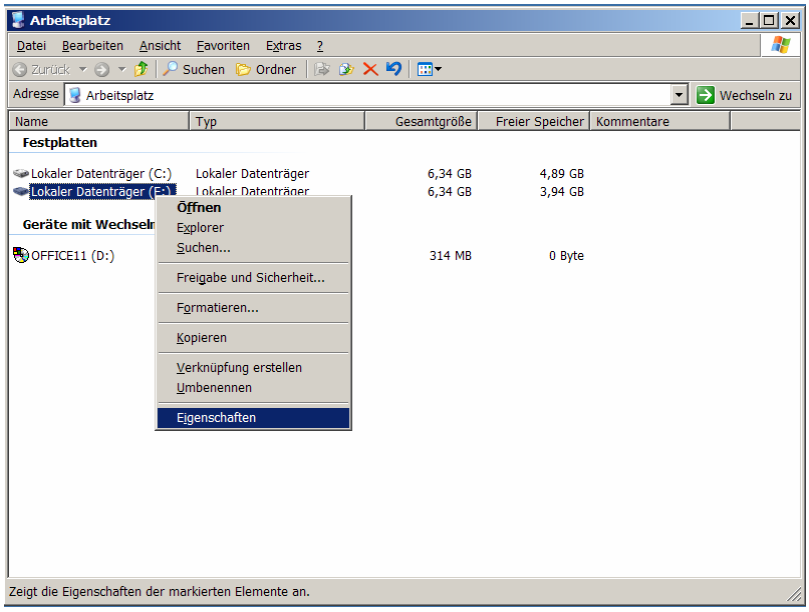


Abb. 99: Anzeige der Eigenschaften des Laufwerks mit den zu sichernden Daten

- Das Eigenschaften-Menü des ausgewählten Laufwerks wird geöffnet.
- Zeigen Sie im Eigenschaften-Menü auf den Eintrag EIGENSCHAFTEN und klicken Sie darauf.
- Der Eigenschaften-Dialog des ausgewählten Laufwerks wird geöffnet.

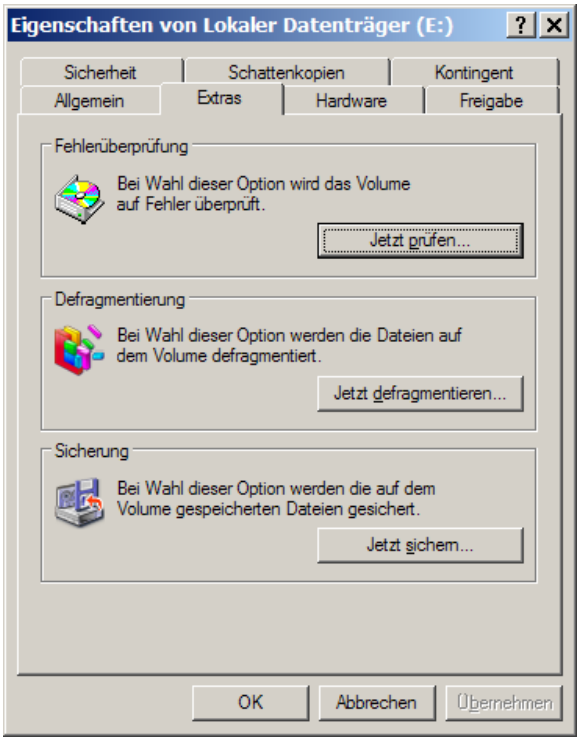


Abb. 100: Registerkarte "Extras" enthält die Schaltfläche "Jetzt sichern..."

- Klicken Sie im Eigenschaften-Dialog auf die Registerkarte EXTRAS und dort auf die Schaltfläche JETZT SICHERN...
- Das Dialogfenster "Sicherungs- oder Wiederherstellungs-Assistent" wird standardmäßig geöffnet (außer es ist deaktiviert).

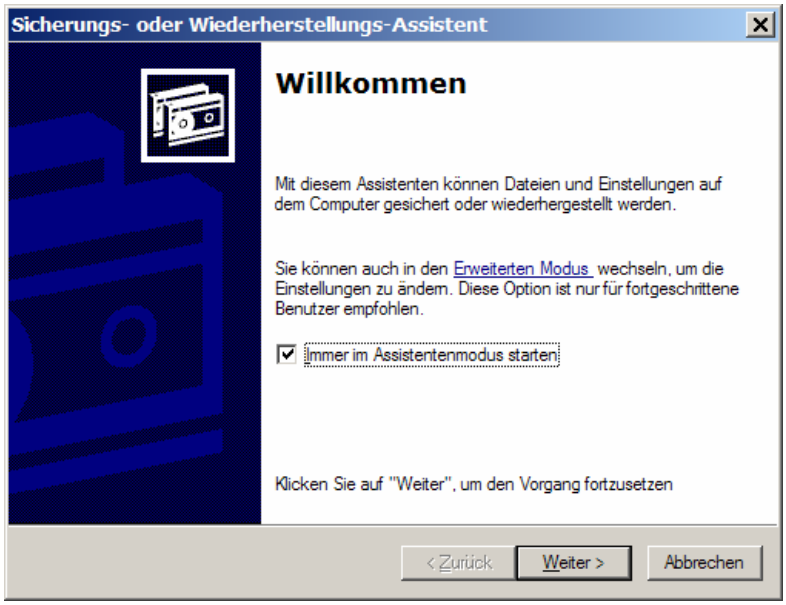


Abb. 101: Datensicherungen mit dem Assistenten

10.3.3 Datensicherung definieren

Das Sicherungsprogramm zeigt sich, wie erwähnt, normalerweise in Form des "Sicherungs- oder Wiederherstellungs-Assistenten" (siehe Kapitel 10.3.2).

Eine Datensicherung im "Assistenten-Modus" funktioniert wie folgt:

1. Klicken Sie auf der Startseite des "Sicherungs- oder Wiederherstellungs-Assistenten" auf die Schaltfläche WEITER.
2. Die Seite "Sichern oder wiederherstellen" wird angezeigt. Die Option DATEIEN UND EINSTELLUNGEN SICHERN ist standardmäßig ausgewählt. Klicken Sie auf die Schaltfläche WEITER.

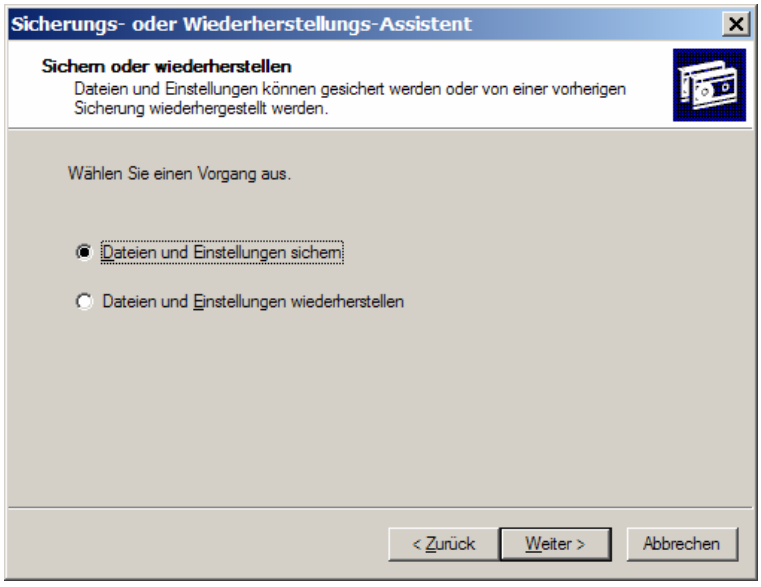


Abb. 102: Entscheidung über Datensicherung oder -wiederherstellung

3. Die Seite "Zu sichernde Daten" wird angezeigt. Auf dieser Seite wird über eine vollständige oder eine selektive Sicherung entschieden.

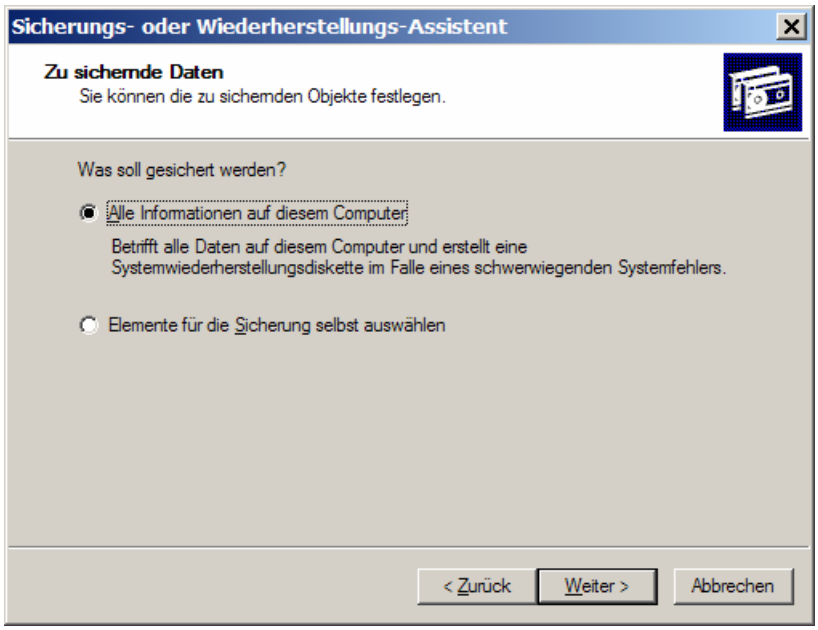


Abb. 103: Entscheidung für vollständige oder selektive Sicherung

4. Wenn Sie eine vollständige Sicherung wünschen, klicken Sie auf die Schaltfläche WEITER. Für eine selektive Sicherung, bei der Sie die zu sichernden Elemente selbst selektieren, klicken Sie dagegen auf die Option ELEMENTE FÜR DIE SICHERUNG SELBST AUSWÄHLEN und dann auf WEITER.

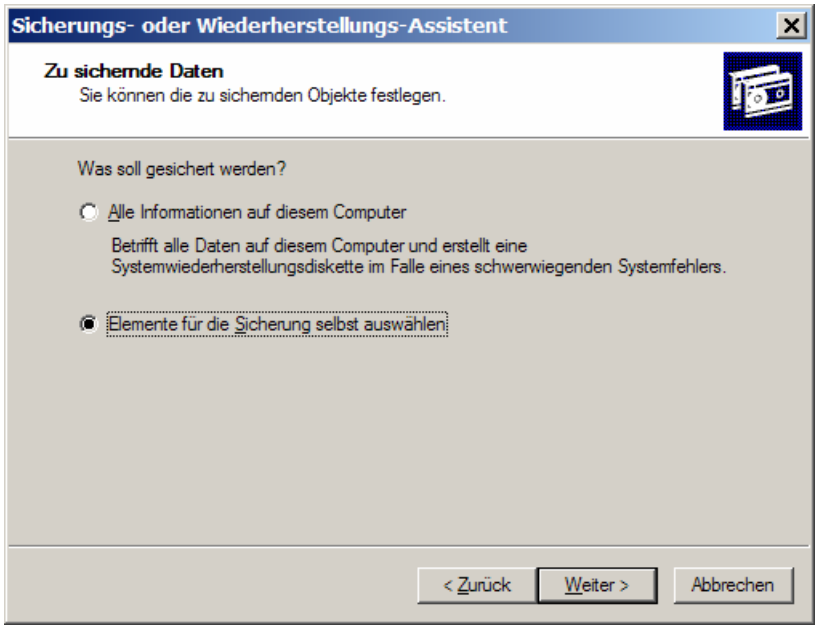


Abb. 104: Entscheidung für eine selektive Sicherung durch Auswahl der entsprechenden Option

5. Wenn Sie sich auf der Seite "Zu sichernde Daten" für eine selektive Sicherung entschieden haben, wird als nächste Seite "Zu sichernde Elemente" angezeigt, auf welcher Sie nun die zu sichernden Elemente bestimmen können. Bei Definition einer vollständigen Sicherung wird dieser Schritt übersprungen und gleich die Seite "Typ, Speicherort und Name der Sicherung" angezeigt.

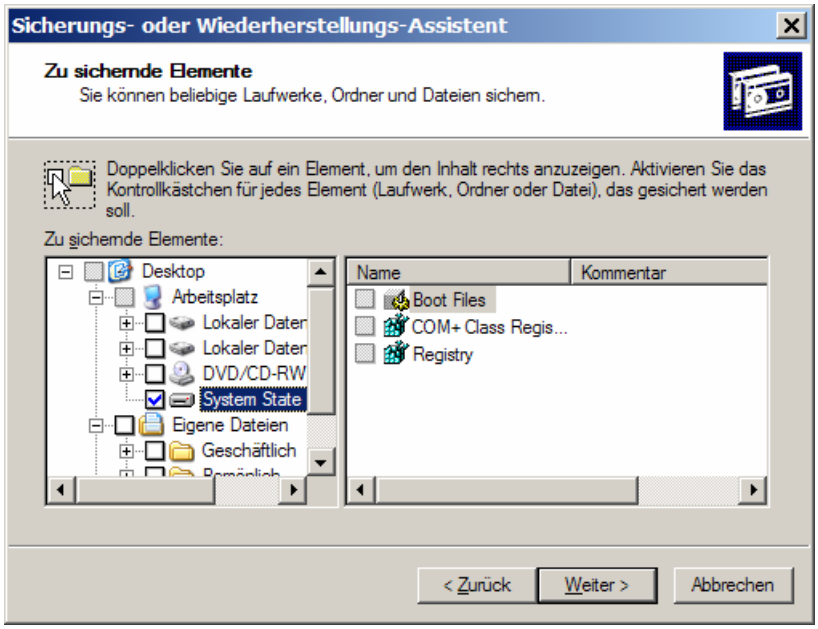


Abb. 105: Auswahl der zu sichernden Elemente

6. Die Seite "Typ, Speicherort und Name der Sicherung" wird angezeigt. Bei Definition einer selektiven Sicherung kommen Sie hierher von der Seite "Zu sichernde Elemente", bei einer vollständigen Sicherung kommen Sie von der Seite "Zu sichernde Daten". Auf dieser Seite müssen Sie folgendes angeben:
   - **Sicherungstyp:** Zielmedium für die zu sichernden Daten (Datei oder Band – "Datei" ist der Standardwert, "Band" steht nur zur Verfügung, wenn ein Bandlaufwerk vorhanden ist).
   - **Speicherort:** Speicherort des Zielmediums (Angabe des Pfads für die Sicherungsdatei bzw. des zu verwendenden Bandlaufwerks).

Anstatt den vollständigen Pfad einzugeben, ist es auch möglich, diesen mit dem "Speichern unter"-Dialog zu definieren. Klicken Sie auf die Schaltfläche DURCHSUCHEN... um diesen Dialog zu öffnen.

   - **Sicherungsname:** Name für die zu erstellende Sicherung. Der Name, den Sie hier eingeben, wird auch standardmäßig für die zu erstellende Sicherungsdatei verwendet.

   Sobald die Angaben auf dieser Seite vollständig sind, klicken Sie auf die Schaltfläche WEITER.

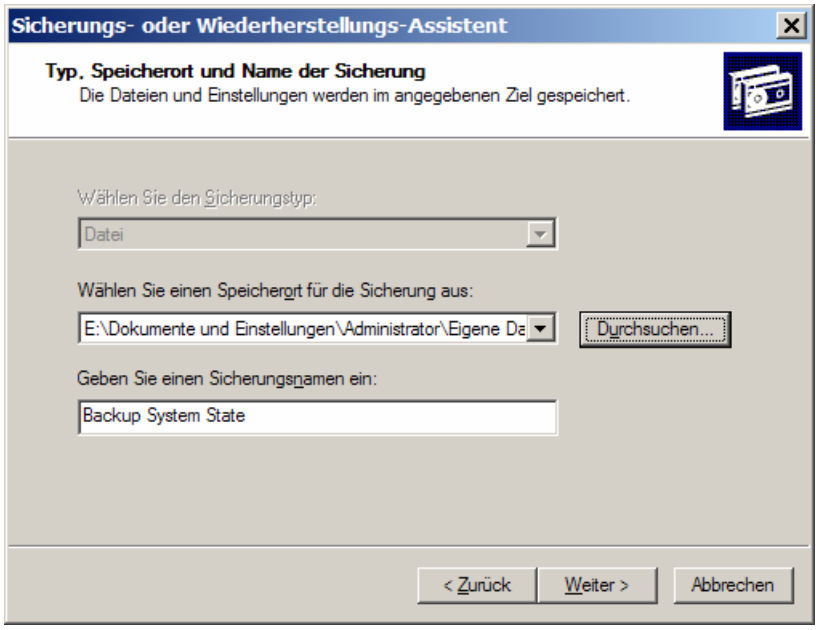


Abb. 106: Eingabe der Basisinformationen für die zu erstellende Sicherung

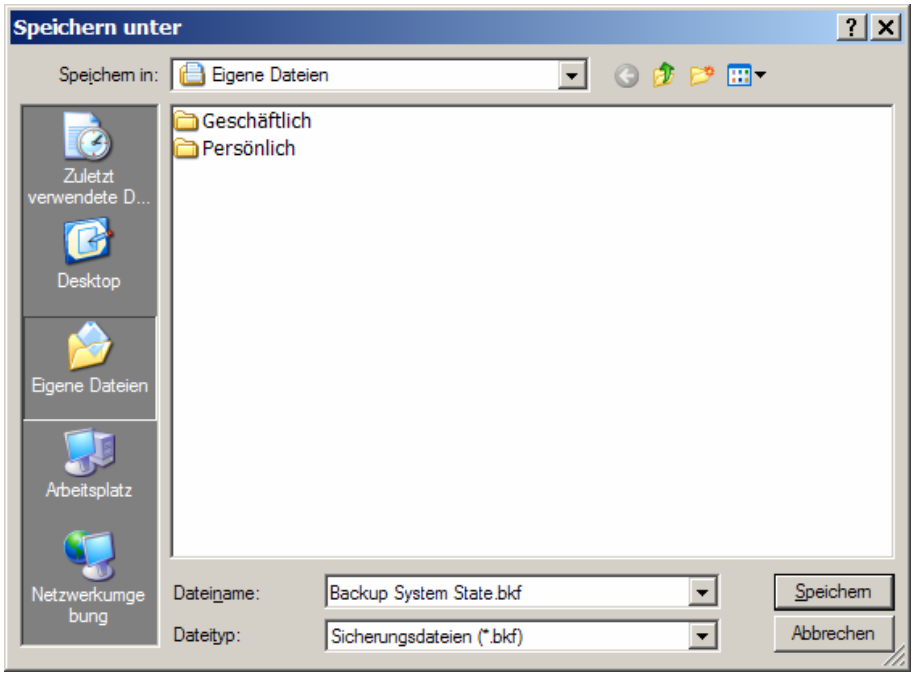


Abb. 107: Auswahl des Speicherorts mittels Dialog-Unterstützung (anstatt manueller Eingabe)

7. Die Seite "Fertigstellen des Assistenten" wird angezeigt. Wenn Sie sich für eine vollständige Sicherung entschieden haben, können Sie den Sicherungsvorgang nun mit Klicken auf die Schaltfläche `Fertig stellen` starten. Wenn Sie allerdings eine selektive Sicherung wünschen, haben Sie nun zwei Möglichkeiten:
   - Starten des Sicherungsvorgangs durch Klicken auf die Schaltfläche FERTIG STELLEN.
   - Angeben erweiterter Sicherungsoptionen durch Klicken auf die Schaltfläche ERWEITERT...

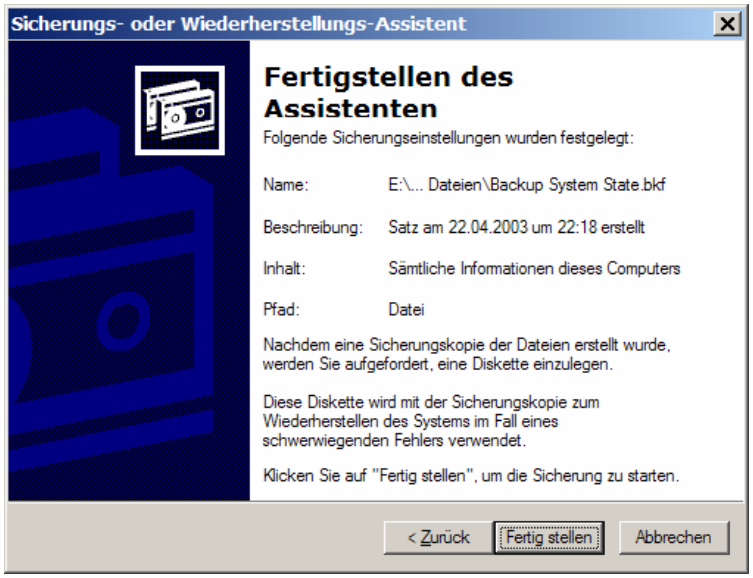


Abb. 108 "Fertigstellen des Assistenten" bei vollständiger Datensicherung

Die Sicherung kann jetzt gestartet werden, die Angabe erweiterter Sicherungsptionen ist bei einer vollständigen Sicherung im Assistenten-Modus nicht möglich.

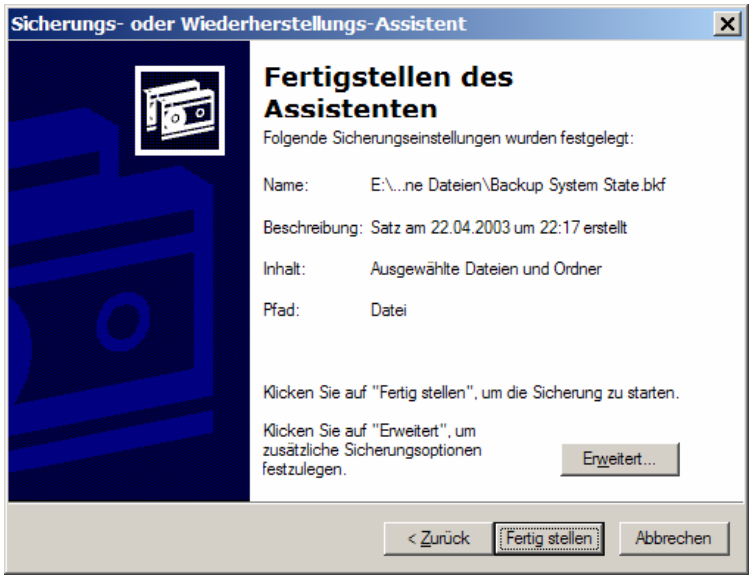


Abb. 109: "Fertigstellen des Assistenten" bei selektiver Datensicherung:

Die Sicherung kann jetzt gestartet werden, die Angabe erweiterter Sicherungsptionen ist bei einer selektiven Sicherung im Assistenten-Modus möglich.

Die Beschreibung der Datensicherung durch Klicken auf die Schaltfläche FERTIG STELLEN finden Sie im Kapitel 11.3.4 – "Daten sichern".

Die Beschreibung der Definition von erweiterten Sicherungsoptionen durch Klicken auf ERWEITERT finden Sie im nächsten Abschnitt.

Entsprechend Ihrer Entscheidung auf dieser Seite wird der begonnene Prozess an dieser Stelle anders fortgesetzt.

Erweiterte Sicherungsoptionen definieren

Im "Assistenten-Modus" können erweiterte Sicherungsoptionen nur bei der Erstellung selektiver Sicherungen definiert werden. Dazu müssen Sie auf der Seite "Fertigstellen des Assistenten" auf die Schaltfläche ERWEITERT... klicken (siehe Abb. 108).

1. Wenn Sie auf die Schaltfläche ERWEITERT... klicken wird die Seite "Typ der Sicherung" angezeigt. Auf dieser Seite können Sie definieren, welche von fünf möglichen Sicherungsmethoden angewendet werden soll. Eine Erklärung dieser Methoden finden Sie im Kapitel 11.1.3.
   Die Auswahl der Option MIGRIERTE REMOTESPEICHERDATEN SICHERN bewirkt, dass auch Daten gesichert werden, die in "Remote-Speicher" migriert worden sind und lokal durch so genannte Platzhalter-Dateien repräsentiert werden.
   Nachdem Sie Ihre Einstellungen auf dieser Seite gesetzt haben, klicken Sie auf die Schaltfläche WEITER.

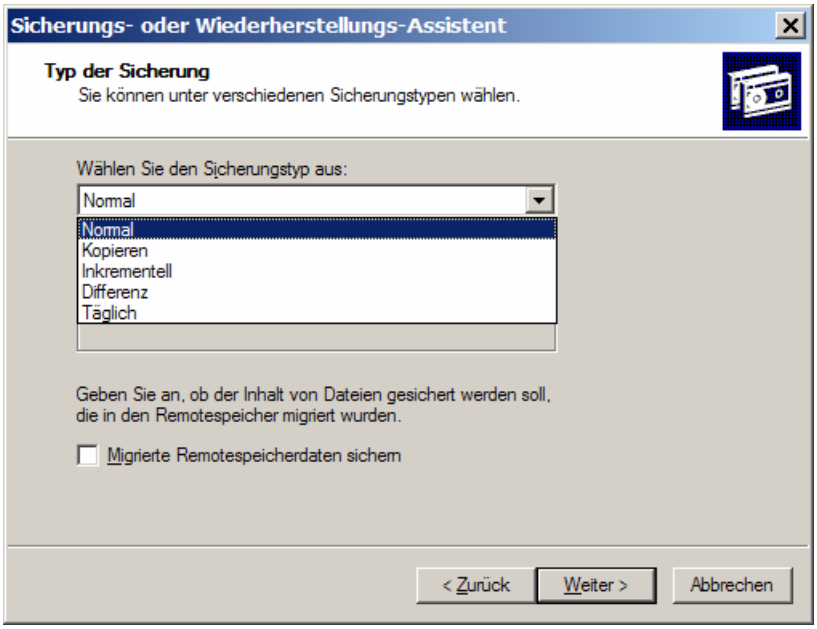


Abb. 110: Auswahl der Sicherungsmethode

2. Die Seite "Sicherungsoptionen" wird angezeigt. Auf dieser Seite stehen Ihnen folgende Optionen zur Verfügung, wobei keine standardmäßig ausgewählt ist:
   - **Daten nach der Sicherung überprüfen:** Wenn Sie diese Option auswählen, wird die Datensicherung nach dem Sicherungsvorgang mit den Originaldaten abgeglichen. Dies erfordert je nach Datenvolumen mehr Zeit, steigert dafür aber die Qualität der Datensicherung.
   - **Hardwarekomprimierung verwenden, wenn verfügbar:** Diese Option komprimiert die Sicherungsdateien auf dem Zielmedium und ist nur dann verfügbar, wenn die Hardware diese Funktion unterstützt. Dadurch verringert sich der Speicherplatzbedarf für Sicherungsdateien.
   - **Volumeschattenkopie deaktivieren:** Die Auswahl dieser Option bewirkt, dass die "Volumeschattenkopien" von Windows Server 2003 beim aktuellen Sicherungsvorgang nicht berücksichtigt werden. Dies verhindert allerdings, dass geöffnete Dateien mitgesichert werden. Diese Option ist nur dann verfügbar, wenn Volumeschattenkopien vorhanden sind. Details zum Thema "Volumeschattenkopien" finden Sie im Kapitel 10.1.1.

   Klicken Sie auf die Schaltfläche WEITER, sobald Sie die gewünschten Optionen ausgewählt haben.

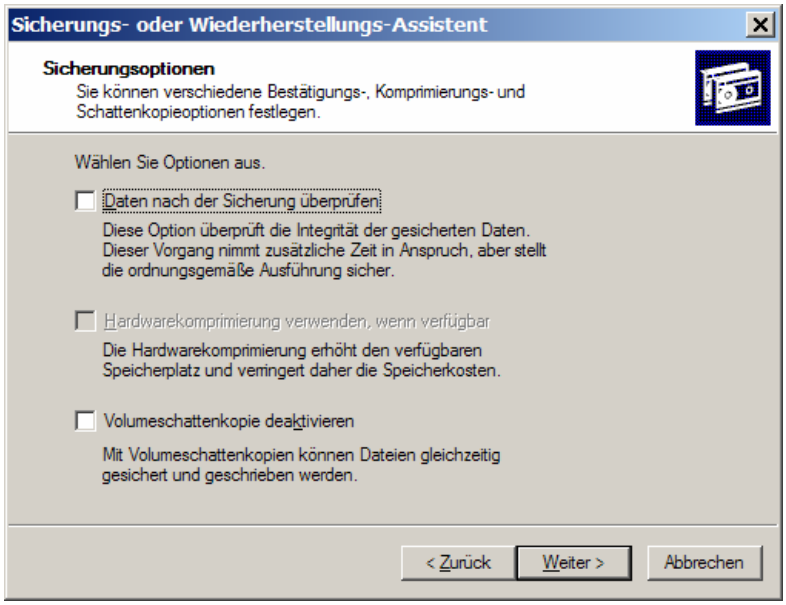
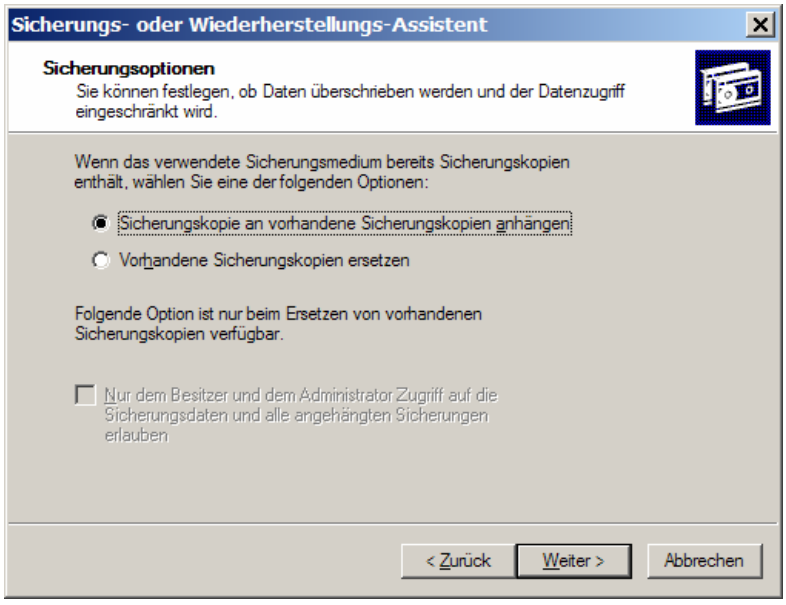


Abb. 111: Auswahl wichtiger Optionen

3. Die Seite "Sicherungsoptionen" wird angezeigt. Auf dieser Seite können Sie darüber entscheiden, ob die zu erstellende Datensicherung zu vorhandenen Sicherungsdateien hinzugefügt wird oder diese ersetzen soll. Die Standardauswahl ist das Hinzufügen zu vorhandenen Sicherungen. Wenn Sie sich für das Ersetzen vorhandener Sicherungen entscheiden, steht eine weitere Option zur Verfügung, die bei Auswahl festlegt, dass nur privilegierte Benutzer die zu erstellende Sicherung künftig verändern dürfen.
   Klicken Sie nach Auswahl der gewünschten Optionen auf die Schaltfläche WEITER.



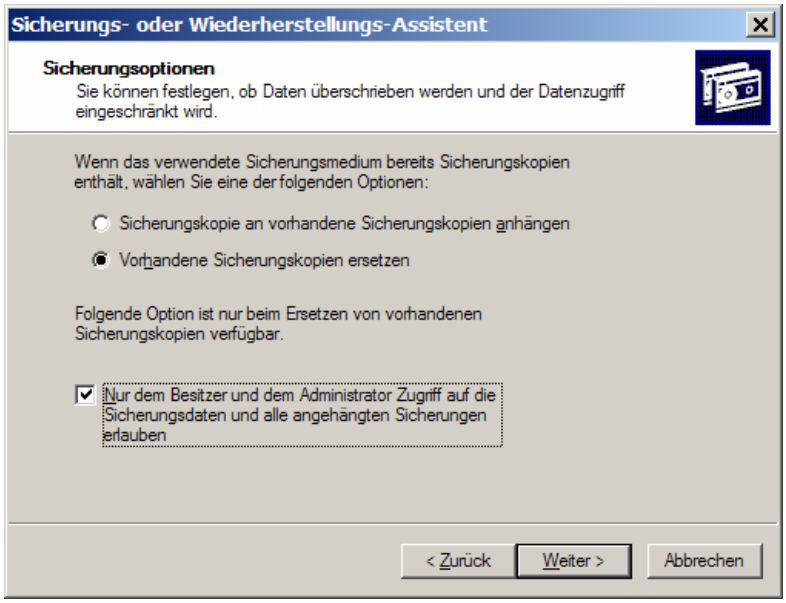


Abb. 112 und 113: Sicherung wird vorhandenen Sicherungen hinzugefügt oder ersetzt diese

4. Die Seite "Zeitpunkt der Sicherung" wird angezeigt. Standardmäßig ist die Option "Jetzt" aktiviert. Wenn Sie nun auf WEITER klicken, kommen Sie auf die Seite "Fertigstellen des Assistenten", auf der Sie den Sicherungsvorgang starten können (siehe Kapitel 10.3.3 „Datensicherung definieren“, Punkt 7) Damit wäre die Definition der erweiterten Sicherungsoptionen abgeschlossen.

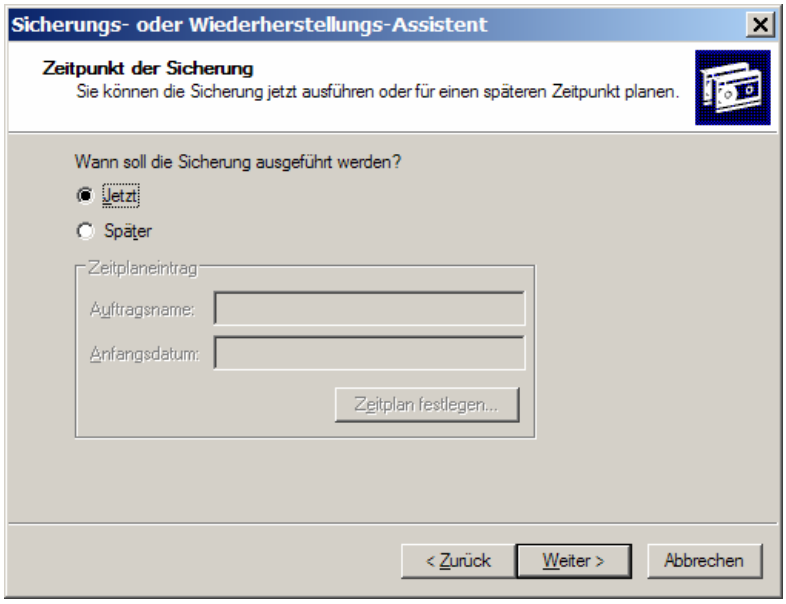


Abb. 114: Auswahl des Zeitpunkts der Sicherung - Jetzt

5. Sie haben auf dieser Seite aber auch die Möglichkeit, einen Sicherungsauftrag zu definieren, indem Sie die Option "Später" aktivieren. In diesem Fall wird die Sektion "Zeitplaneintrag" aktiviert, in der Sie jetzt den Sicherungsauftrag wie folgt definieren können:
   - **Auftragsname**: Direkte Eingabe eines Namens für den Sicherungsauftrag.

- **Anfangsdatum**: Angabe eines Startzeitpunkts und Möglichkeit der Definition eines Zeitplans über die Schaltfläche ZEITPLAN FESTLEGEN....Der Standardwert in ANFANGSDATUM ist der Erstellungszeitpunkt der aktuellen Datensicherung. Klicken Sie auf die Schaltfläche ZEITPLAN FESTLEGEN... um einen Startzeitpunkt und einen Zeitplan zu definieren.

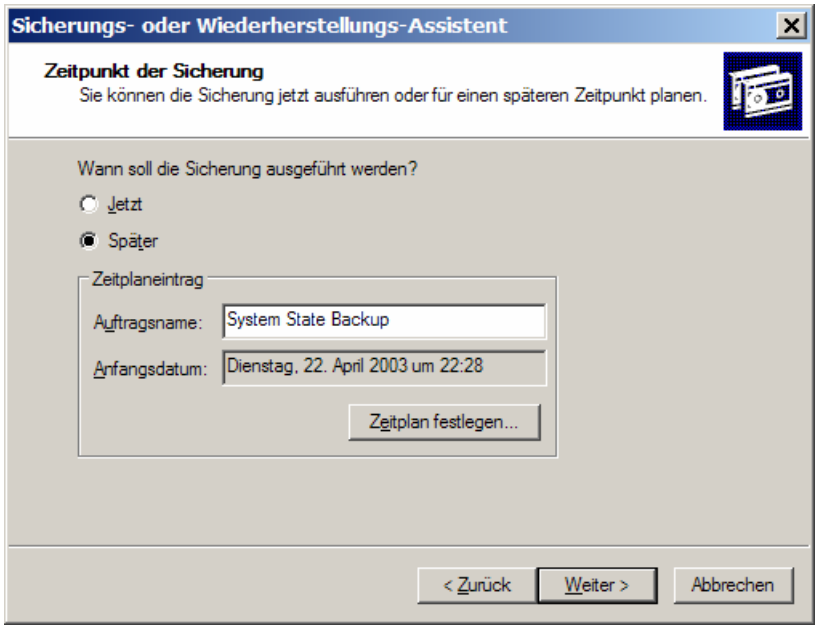


Abb. 115: Auswahl des Zeitpunkts der Sicherung – Später

Sicherungsauftrag definieren

Die Definition eines Sicherungsauftrags im Assistenten-Modus erfolgt über die Auswahl der erweiterten Sicherungsoptionen und dort auf der Seite "Zeitpunkt der Sicherung". Informationen zu den erweiterten Sicherungsoptionen finden Sie im Kapitel 11.3.3.

Falls Sie sich auf der Seite "Zeitpunkt der Sicherung" (siehe Punkt 5) für die Definition eines Sicherungsauftrags samt Terminplan entschieden haben, wird der Dialog "Auftrag planen" geöffnet.

Der Inhalt dieses Dialogs verteilt sich auf zwei Registerkarten:

1. **Zeitplan**: Diese Registerkarte beinhaltet jene Funktionen, die zur Erstellung eines Zeitplans für den Sicherungsauftrag erforderlich sind. Ist ein Zeitplan definiert, wird der Sicherungsauftrag in den darin definierten Intervallen automatisch erledigt. Es ist auch möglich, mehrere Zeitpläne für einen Sicherungsauftrag zu erstellen, so dass die Sicherung in unregelmäßigen Intervallen erfolgt. Die Optionen dieser Registerkarte sind folgende:
   - **Task ausführen:** In dieser Combobox können einfache Intervalle ausgewählt werden. Je nach Auswahl werden auf der Registerkarte dazu passende, leicht verständliche und selbsterklärende Optionen angeboten.

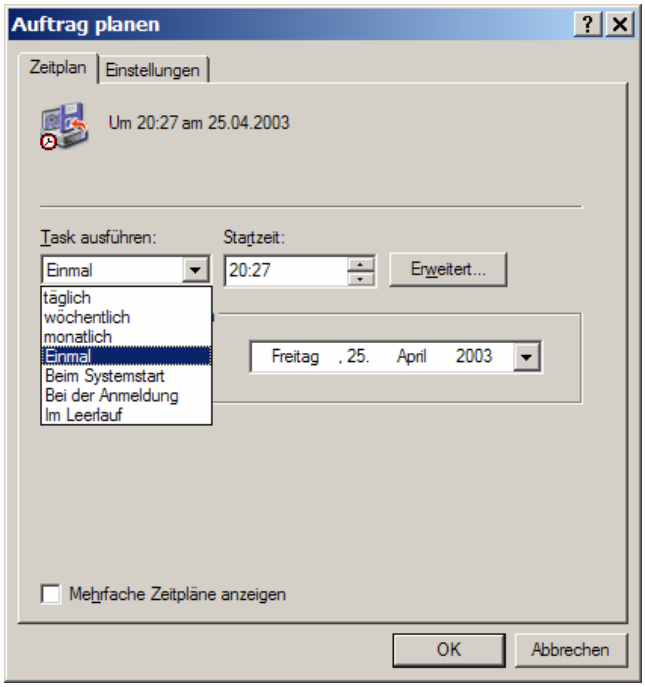


Abb. 116: Auswahl von Intervallen zur automatischen periodischen Ausführung eines Sicherungsauftrags

- **Startzeit:** Die Startzeit zum ausgewählten Intervall kann direkt eingegeben oder mit den Pfeil-Schaltflächen eingestellt werden.
- **Ausführen am:** In dieser Combobox kann das Startdatum eingestellt werden – direkt oder über ein Kalender-Steuerelement.

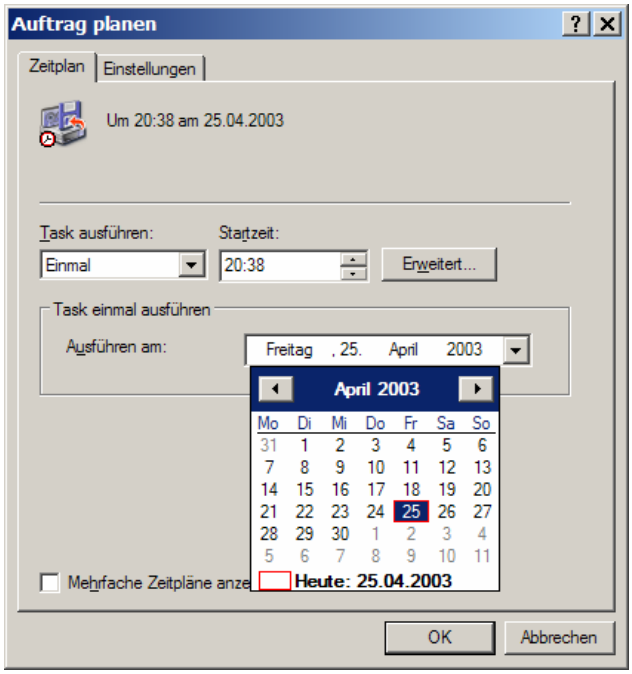


Abb. 117: Angabe des Tages, an dem das Ausführungsintervall beginnt

- **Erweitert:** Durch Klicken auf diese Schaltfläche wird der Dialog "Erweiterte Zeitplanoptionen" geöffnet, der erweiterte Optionen zur Zeitplandefinition anbietet. Diese Optionen sind leicht verständlich und selbsterklärend.

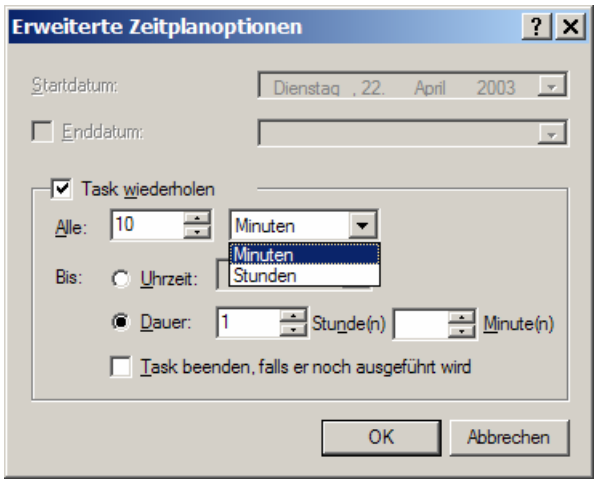


Abb. 118: Zusätzliche Optionen zur Zeitplandefinition

- **Mehrfache Zeitpläne anzeigen:** Durch Aktivieren dieser Option können mehrere Zeitpläne definiert – und somit unterschiedliche Intervalle miteinander kombiniert – werden. Die Registerkarte sieht dann wie folgt aus:

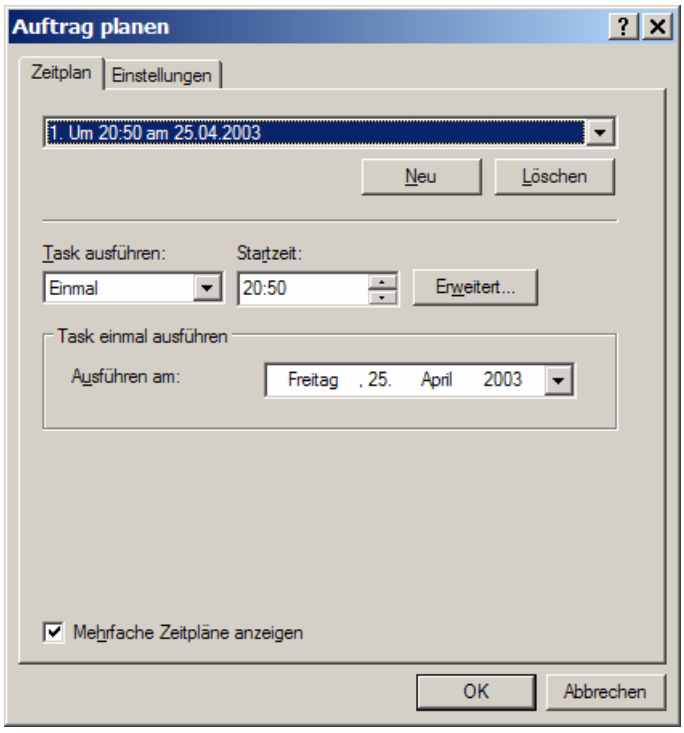


Abb. 119: Möglichkeit des Erstellens mehrerer miteinander kombinierter Zeitpläne

- **Combobox zur Zeitplanauswahl:** Anstelle der statischen Anzeige des Startzeitpunkts (ganz oben auf der Registerkarte), wird eine Combobox angezeigt, welche die Auswahl eines bestimmten Zeitplanes (zwecks Bearbeitung) ermöglicht.

- **Schaltfläche "Neu":** Auf diese Schaltfläche können weitere Zeitpläne durch Anklicken hinzugefügt werden.
- **Schaltfläche "Löschen":** Hier kann ein in der Combobox ausgewählter Zeitplan gelöscht werden.

2. **Einstellungen:** Diese Registerkarte bietet in verschiedenen Optionsgruppen folgende Einstellungen an, die den Ablauf von Sicherungsaufträgen beeinflussen und modifizieren (quasi als Feintuning):

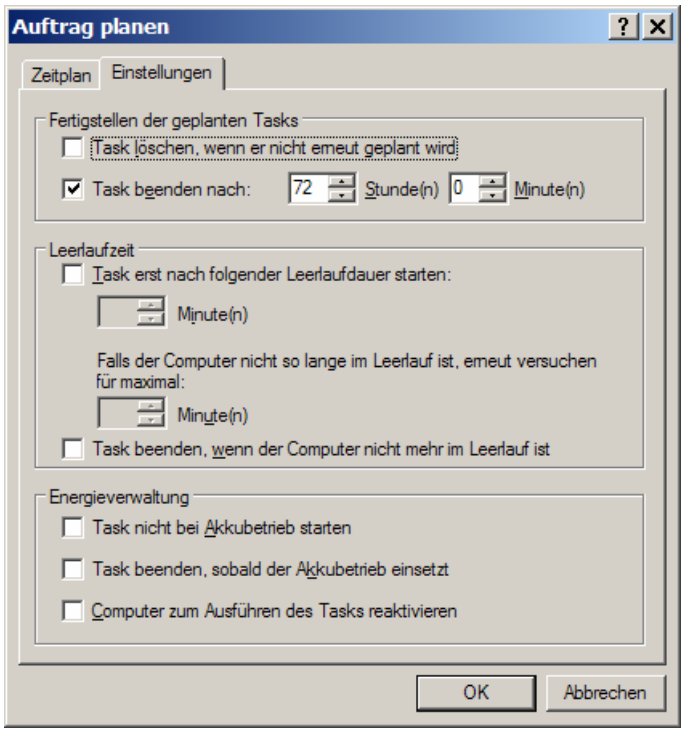


Abb. 120: Feintuning eines Sicherungsauftrags

- **Task löschen, wenn er nicht erneut geplant wird:** Ist diese Option aktiviert, wird der Sicherungsjob gelöscht, nachdem er ein Mal ausgeführt ist.
- **Task beenden nach [nn] Stunden [nn] Minuten:** Diese Option ermöglicht die Angabe einer Maximallaufzeit des Sicherungsauftrags in Stunden und Minuten.
- **Task erst nach folgender Leerlaufdauer starten:** Wird diese Option aktiviert, kann durch die Angabe von [nn] Minuten die Leerlaufzeit des Computers definiert werden. Wenn der Benutzer innerhalb dieser Zeitspanne nicht aktiv wird (durch Maus und Tastatur), tritt der Zustand der "Leerlaufzeit" ein.
- **Falls der Computer nicht so lange im Leerlauf ist, erneut versuchen für maximal [nn] Minuten:** Wenn der Computer zur angegeben Zeit nicht den Zustand der "Leerlaufzeit" erreicht, kann hier angegeben werden, dass das Erreichen der Leerlaufzeit nochmals für die angegebene Zeitspanne überwacht wird.
- **Task beenden, wenn der Computer nicht mehr im Leerlauf ist:** Ist diese Option aktiviert, wird ein laufender Sicherungsauftrag beendet, sobald die Leerlaufzeit beendet wird (durch Benutzeraktivitäten am Computer).
- **Task nicht bei Akkubetrieb starten:** Aktivieren Sie diese Option, um zu verhindern, dass Sicherungsaufträge im Akkubetrieb gestartet werden.
- **Task beenden, sobald der Akkubetrieb einsetzt:** Ein laufender Sicherungsauftrag wird bei Einsetzen des Akkubetriebs beendet, wenn diese Option aktiviert ist.

- **Computer zum Ausführen des Tasks reaktivieren:** Bei Aktivierung dieser Option wird der Computer "aufgeweckt", d. h. der momentan aktive "Sleep Modus" wird beendet.

3. Klicken Sie im Dialog "Auftrag planen" auf die Schaltfläche OK, um die Erstellung des aktuellen Sicherungsauftrags abzuschließen. Danach erscheint der Dialog KONTOINFORMATIONEN FESTLEGEN:

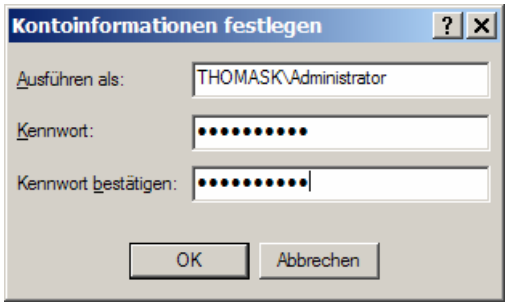


Abb. 121: Anmeldung des Taskplaners zum Start des Sicherungsauftrag

Hier müssen Sie ein Benutzerkonto angeben, mit dem der Taskplaner sich zum Start des Sicherungsauftrags am System anmelden kann. Bei wiederholten Ausführungen desselben Auftrags wird immer wieder dieses Konto verwendet.

10.3.4 Daten sichern

Wenn Sie alle Schritte absolviert und eine Datensicherung (einmalig oder regelmäßig) eingerichtet haben, gelangen Sie auf die letzte Seite des Sicherungs- und Wiederherstellungs-Assistenten:

Abb. 122: Wichtige Informationen zur aktuellen Datensicherung

Klicken Sie auf die Schaltfläche FERTIG STELLEN, um die Definition der aktuellen Datensicherung abzuschließen. Die Datensicherung wird zum gewünschten Zeitpunkt starten: sofort oder später, einmalig oder zyklisch. Dass sie läuft, zeigt der Dialog "Status: Sicherungsvorgang" an.

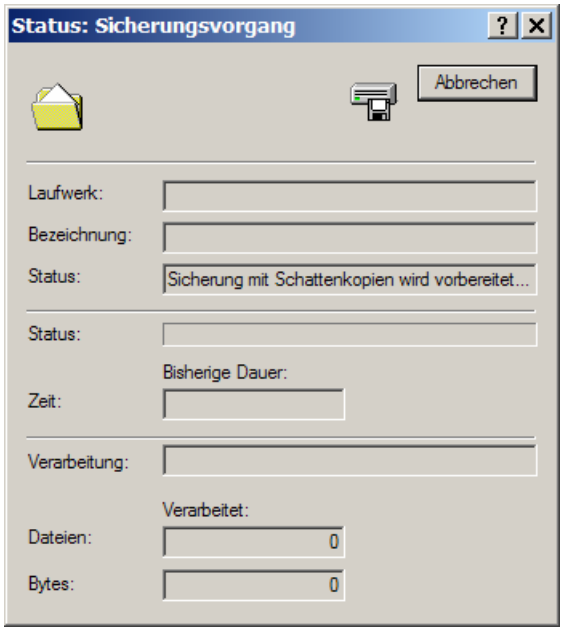


Abb. 123: Anzeige der Vorbereitung für die Datensicherung

Die Datensicherung ist gestartet, der Sicherungsvorgang vorbereitet. Anschließend werden die zu sichernden Elemente selektiert. Dieser Vorgang wird mit dem Dialog "Auswahlinformationen" angezeigt, der über dem aktuellen Dialog angezeigt wird.

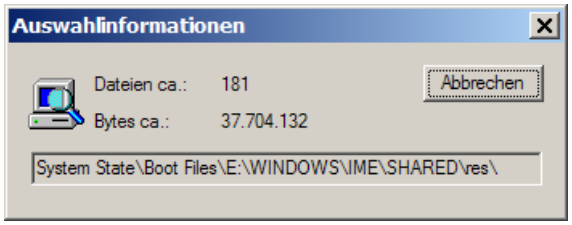


Abb. 124: Anzeige der Auswahl zu sichernder Elemente

Sobald die Auswahl der zu sichernden Elemente beendet ist, wird der Dialog "Auswahlinformationen" geschlossen und der weitere Verlauf der Datensicherung – das Sichern der ausgewählten Elemente – angezeigt:

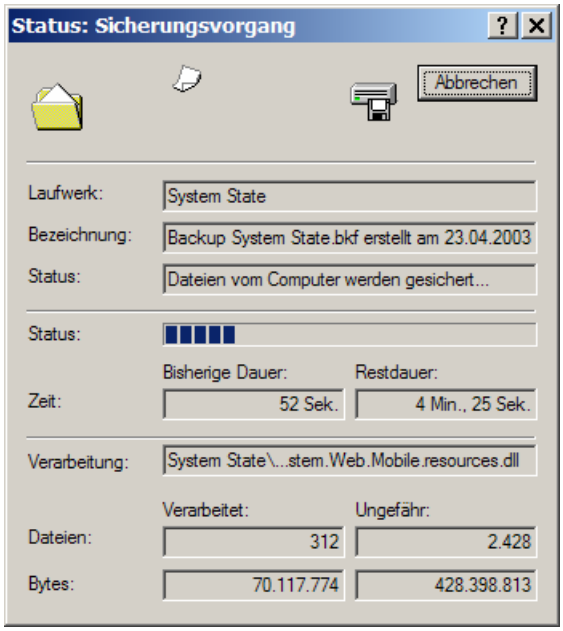


Abb. 125: Anzeige der eben gesicherten Elemente

Das Ende der Sicherung wird im selben Dialog angezeigt. Im Feld "Status" steht "Abgeschlossen".

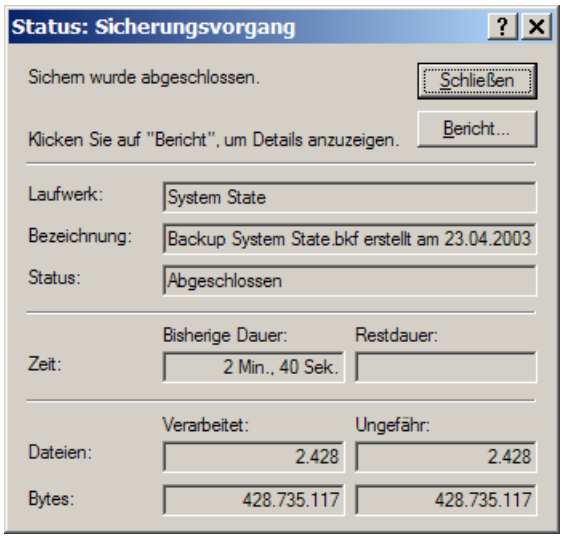


Abb. 126: Das Ende der Datensicherung wird angezeigt

Zusätzlich wird nun die Schaltfläche BERICHT... angezeigt, die Sie anklicken, um im Windows Texteditor einen Bericht über den Verlauf der Sicherung abzurufen:

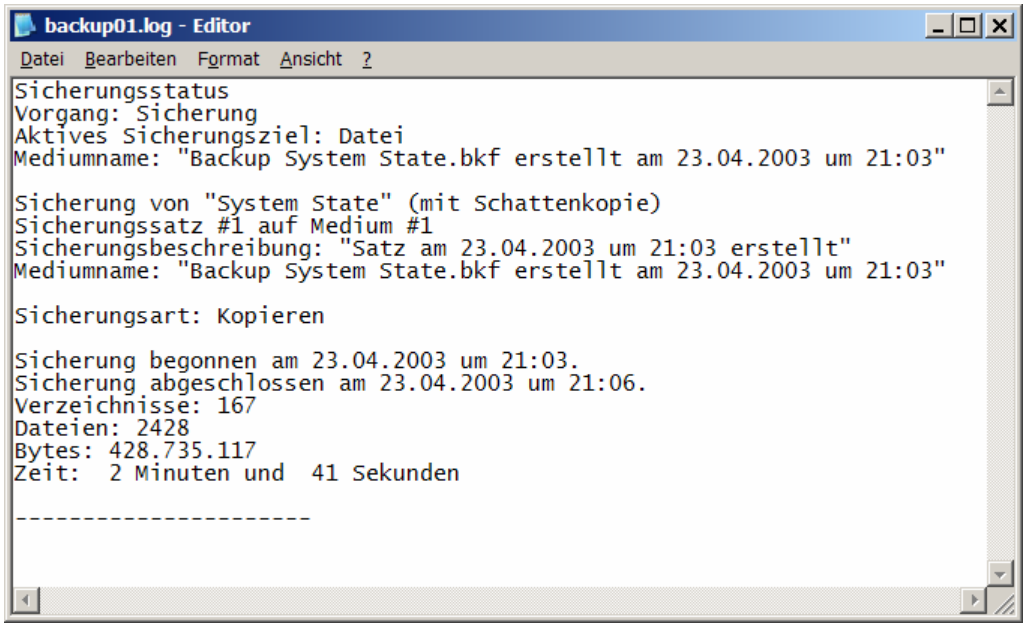


Abb. 127: Datensicherungsbericht

Diese Protokolldateien heißen standardmäßig "backupNN.log", wobei NN eine fortlaufende Zahl ist. Sie werden in folgendem Verzeichnis gespeichert:

"\Dokumente und Einstellungen\BENUTZERNAME\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows NT\NTBackup\data"

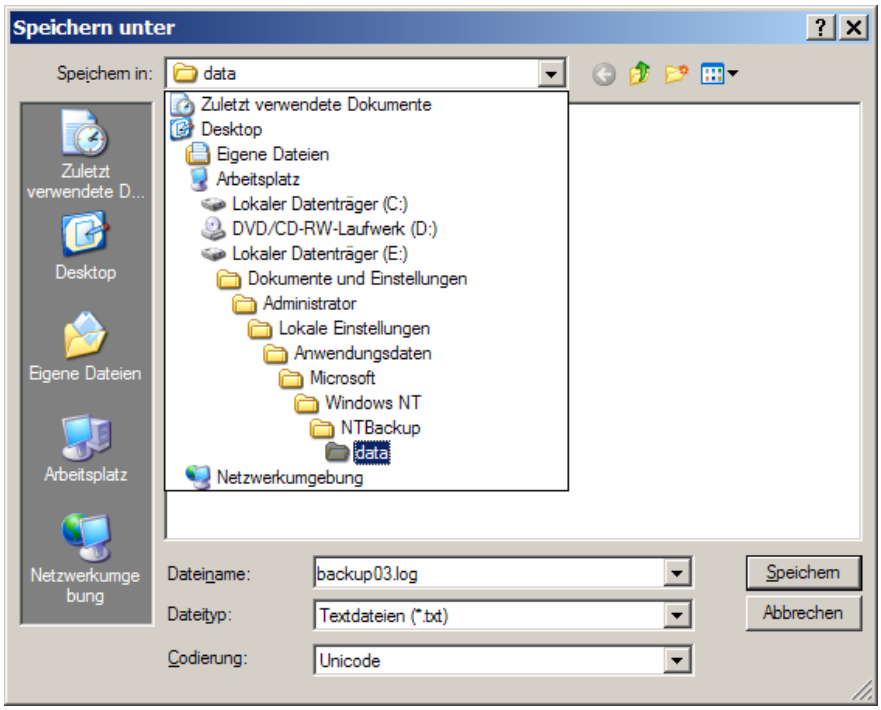


Abb. 128: Speicherort der Protokolldateien für Sicherungsvorgänge

10.4 Daten wiederherstellen

Um Daten wiederherzustellen, nutzen Sie unter Windows Server 2003 dieselben Möglichkeiten wie beim Sichern von Daten (mit Ausnahme des Kommandos "ntbackup", das nicht zum Wiederherstellen von Daten verwendet werden kann).

Sie können den "Sicherungs- und Wiederherstellungs-Assistenten" benutzen, indem Sie auf der Startseite des Assistenten auf den Link "Erweitert" klicken oder die "Standard-Benutzeroberfläche".

Wie schon bei der Datensicherung wird auch bei der Wiederherstellung nur die Nutzung des Assistenten beschrieben.

Die Benutzung des Sicherungsprogramms im "Assistenten-Modus" erfolgt genau gleich wie bei der Datensicherung. Das Starten des Programms ist daher hier nicht mehr gesondert beschrieben, dies steht im Kapitel 11.3.1.

10.4.1 Datenwiederherstellung definieren

Wenn Sie Daten wiederherstellen möchten, gehen Sie wie folgt vor:

1. Starten Sie das Sicherungsprogramm im Assistenten-Modus und klicken Sie auf der Startseite des Assistenten auf die Schaltfläche WEITER.
2. Die Seite "Sichern oder wiederherstellen" wird angezeigt. Wählen Sie die Option DATEIEN UND EINSTELLUNGEN WIEDERHERSTELLEN und klicken Sie WEITER.

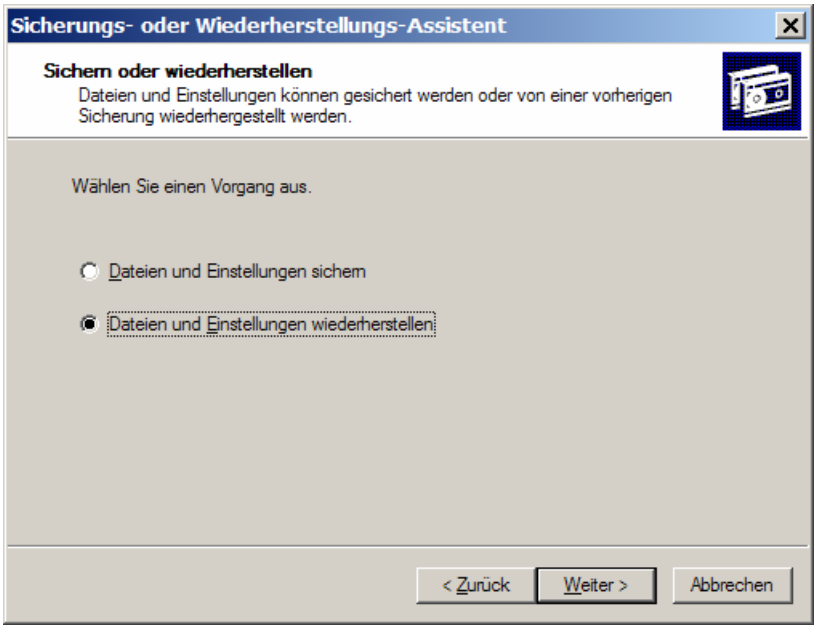


Abb. 129: Entscheidung über Datensicherung oder -wiederherstellung

3. Die Seite "Wiederherzustellendes Objekt" wird angezeigt. Auf dieser Seite können Sie unter den vorhandenen Datensicherungen jenes Sicherungsmedium auswählen, das die wiederherzustellenden Daten enthält.

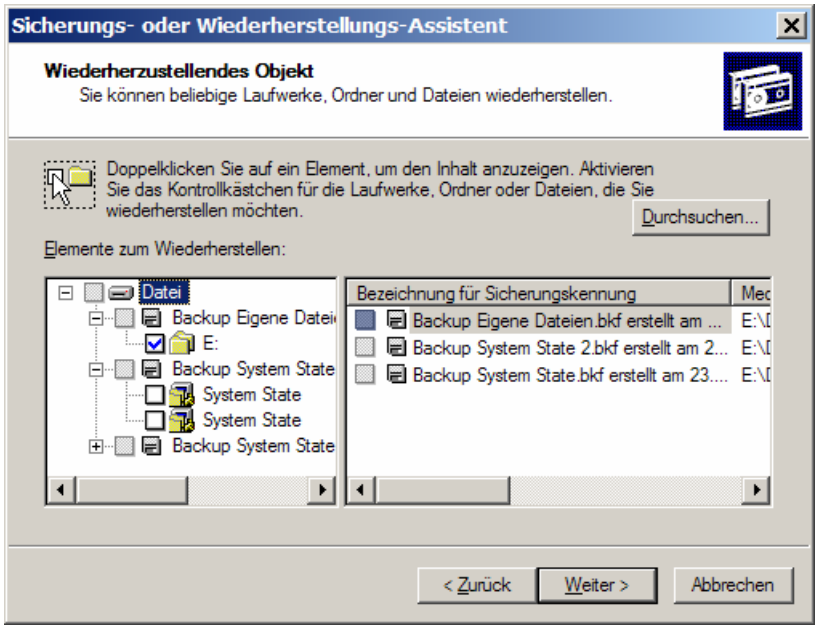


Abb. 130: Auswahl des Sicherungsmedium

Sie können auch gezielt nach weiteren Sicherungsmedien suchen, indem Sie auf die Schaltfläche DURCHSUCHEN... klicken. Es wird dann der Dialog "Sicherungsdatei öffnen" angezeigt, in dem Sie die Sicherungsdatei durch direkte Eingabe des Pfads auswählen können bzw. durch Klicken auf die Schaltfläche DURCHSUCHEN.

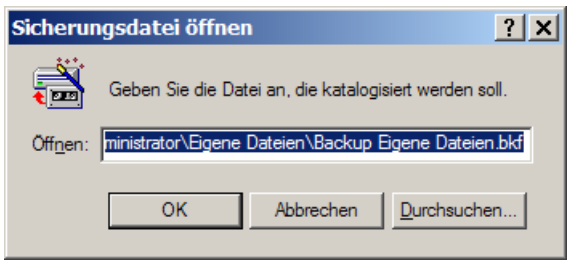


Abb. 131: Auswahl einer Sicherungsdatei

Wenn Sie im Dialog "Sicherungsdatei öffnen" auf "Durchsuchen" klicken, öffnen Sie den Dialog "Wählen Sie die zu katalogisierende Datei.". Hier können Sie das Sicherungsmedium für die Wiederherstellung auswählen.

© 2005, Microsoft Österreich GmbH

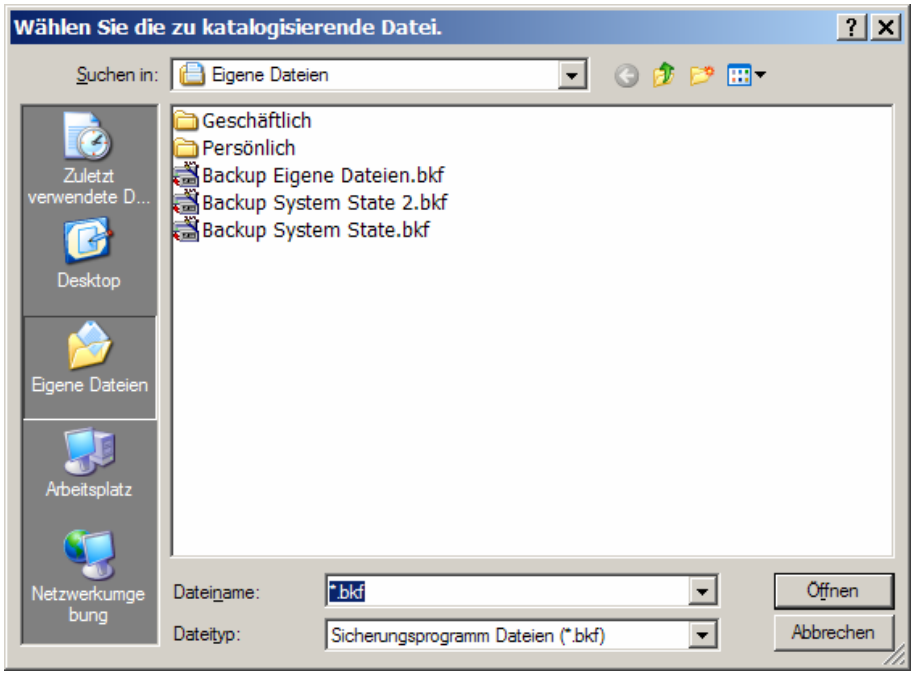


Abb. 132: Auswahl des Sicherungsmediums für die Wiederherstellung

4. Sobald Sie das für die Wiederherstellung zu verwendende Sicherungsmedium ausgewählt haben, klicken Sie auf die Schaltfläche "Weiter". Die Seite "Fertigstellen des Assistenten" wird angezeigt.

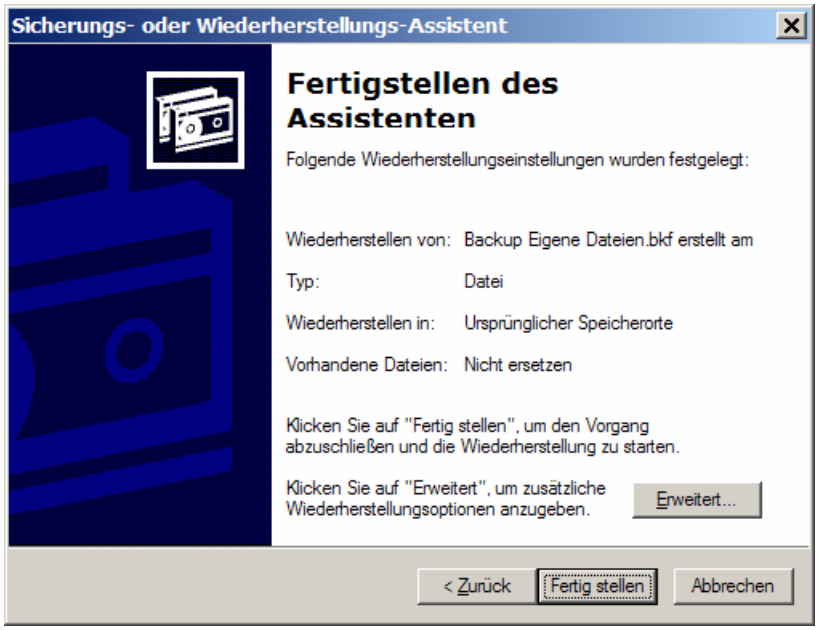


Abb. 133: Fertigstellen des Assistenten

Sie haben nun zwei Möglichkeiten:

- Wiederherstellung mit den Standardoptionen
- Wiederherstellung mit speziellen Optionen

Wenn Sie eine Standard-Wiederherstellung wünschen, klicken Sie auf die Schaltfläche FERTIGSTELLEN. Wollen Sie spezielle Optionen einstellen, klicken Sie auf die Schaltfläche ERWEITERT.

Die Beschreibung der Datenwiederherstellung finden Sie im Kapitel 11.4.2, die Definition erweiterter Optionen finden Sie im folgenden Abschnitt.

Das Wiederherstellen des Systemzustands (System State) mit allen erforderlichen Systemdaten ist mit der Wiederherstellung von Benutzerdaten völlig identisch. Einziger Unterschied ist, dass Sie das entsprechende Sicherungsmedium, das die Systemzustandssicherung enthält, auswählen und dann auf das Kontrollkästchen "System State" klicken. Die Funktionalität erweiterter Wiederherstellungsoptionen, wie z. B. Herstellen von Daten am ursprünglichen oder am alternativen Zielort, hat dieselben Auswirkungen wie beim Wiederherstellen von Benutzerdaten.

Erweiterte Wiederherstellungsoptionen definieren

Um die Standardwerte der Wiederherstellungsoptionen zu verändern bzw. um spezielle Optionen auszuwählen, klicken Sie auf der Seite "Fertigstellen des Assistenten" auf die Schaltfläche "Erweitert".

1. Auf der Seite "Zielort der Wiederherstellung" können Sie nun festlegen, wo die Daten wiederhergestellt werden. Sie haben folgende Optionen:
   - **Daten wiederherstellen in:** Der Standardwert in dieser Combobox ist "Ursprünglicher Bereich" und selbsterklärend (die Daten werden am Original-Herkunftsort wiederhergestellt). Wenn Sie einen der beiden Werte "Alternativer Bereich" oder "Einzelner Ordner" auswählen, wird zusätzlich eine weitere Option angezeigt (siehe b).

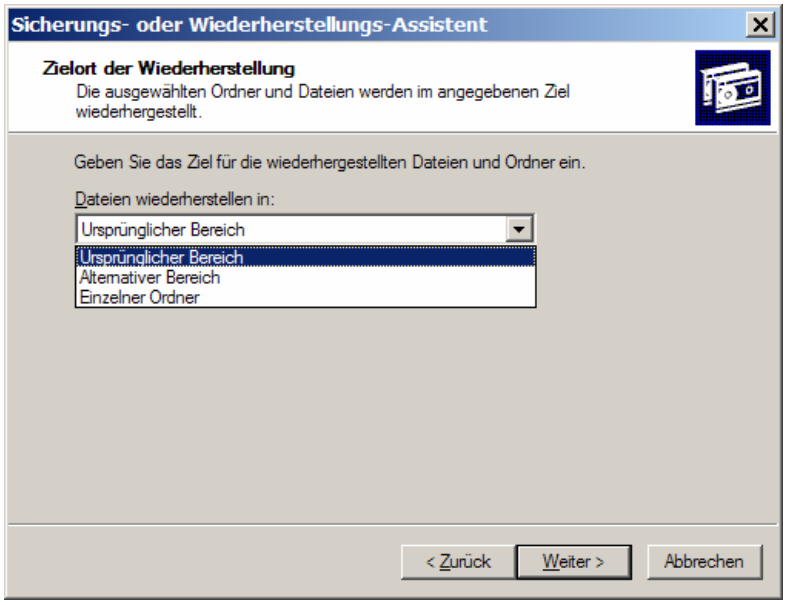


Abb. 134: Auswahl der Zielorte für Wiederherstellung

   - **"Alternativer Bereich"** oder **"Einzelner Ordner":** Wenn Sie in der Combobox DATEN WIEDERHERSTELLEN IN nicht den Standardwert ausgewählt haben, sondern ALTERNATIVER BEREICH oder EINZELNER ORDNER, können Sie in einer weiteren Textbox einen alternativen Zielort für die Datenwiederherstellung auswählen. Wenn Sie Daten mit der Option ALTERNATIVER BEREICH wiederherstellen, werden die Daten am angegebenen Zielort und unter Beibehaltung der Ordnerstruktur der gesicherten Daten wiederhergestellt.

Bei der Option EINZELNER ORDNER werden die Daten am Zielort wiederhergestellt, allerdings nicht in der Original-Ordnerstruktur.

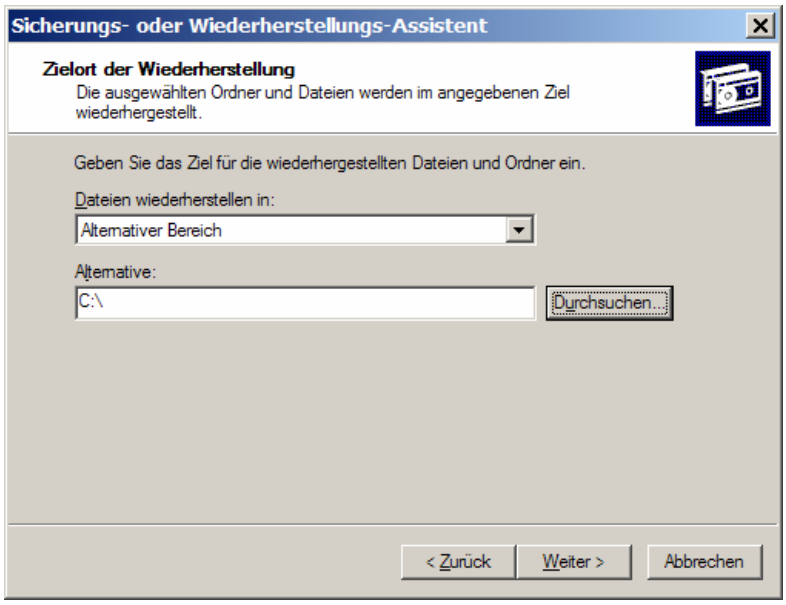


Abb. 135: Zielort der Wiederherstellung

Daten können alternativ auch an anderen Orten wiederhergestellt werden, mit oder ohne Beibehaltung der Original-Ordnerstruktur.

Der Zielort kann in der entsprechenden Textbox manuell eingegeben oder durch Klicken auf die Schaltfläche "Durchsuchen" gesucht und festgelegt werden.

Es wird dann der Dialog "Wiederherstellungspfad" angezeigt, in dem der Zielort per Mausklick ausgewählt werden kann. Mit einem Klick auf die Schaltfläche "OK" wird der Dialog beendet. Der ausgewählte Zielort wird als Pfad in die Textbox der Assistenten-Seite "Zielort der Wiederherstellung" eingetragen.

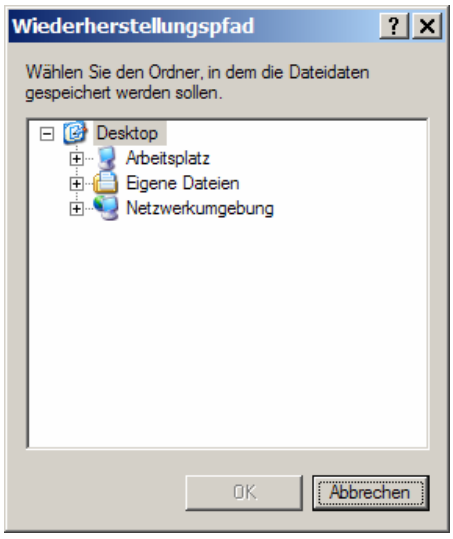


Abb. 136: Wiederherstellungspfad - Auswahl eines alternativen Zielorts für die wiederherzustellenden Daten.

2. Klicken Sie auf die Schaltfläche WEITER, um die Seite "Optionen der Wiederherstellung" anzuzeigen. Auf dieser Seite haben Sie folgende Optionen:
   - **Vorhandene Dateien beibehalten (empfohlen):** Diese Option ist der Standardwert auf dieser Seite. Behalten Sie sie bei, wenn die vorhandenen nicht durch die (identischen) Dateien der Datensicherung ersetzt werden sollen.
   - **Dateien nur ersetzen, wenn sie älter sind als die Sicherungsdateien:** Wählen Sie diese Option, um vorhandene ältere durch neuere Dateien aus der Datensicherung zu ersetzen.
   - **Vorhandene Dateien ersetzen:** Wenn Sie diese Option wählen, werden vorhandene Dateien durch die Wiederherstellung überschrieben.

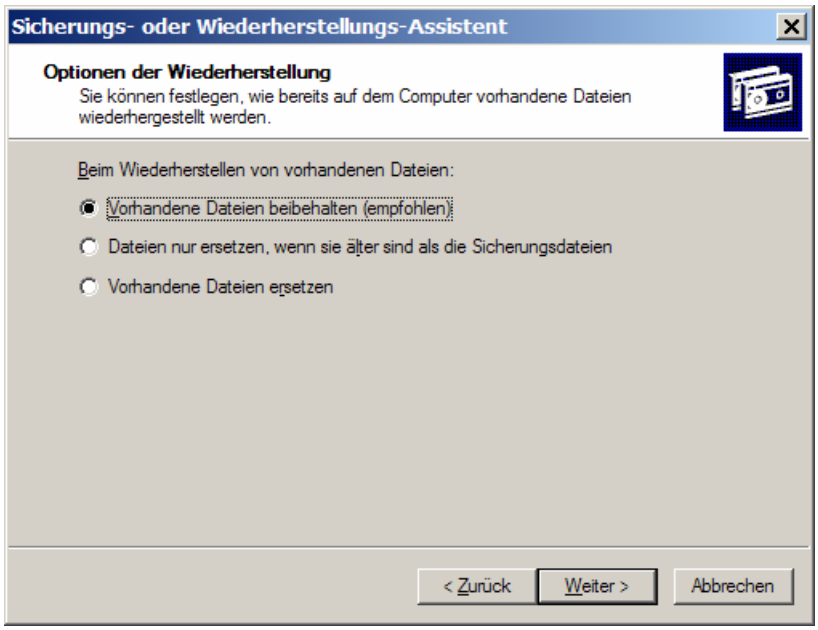


Abb. 137: Optionen der Wiederherstellung

3. Die Seite "Erweiterte Wiederherstellungsoptionen" wird angezeigt. Auf dieser Seite stehen folgende Optionen zur Auswahl, die kombiniert miteinander aktiviert werden können:
   - **Sicherheitseinstellungen wiederherstellen:** Diese Option ist ein Standardwert auf dieser Seite und bewirkt, dass für jede einzelne Datei die Sicherheitseinstellungen wiederhergestellt werden, also die Zugriffsrechte auf die Objekte, die Einträge im Sicherheitsprotokoll und die Besitzer der Objekte. Diese Wiederherstellung ist aber nur dann möglich, wenn die Daten auf einem NTFS-Laufwerk der Windows Server 2003-Familie gesichert sind und auf einem solchen wiederhergestellt werden sollen.
   - **Nur Abzweigungspunkte wiederherstellen, nicht die Ordner und Dateidaten, auf die verwiesen wird:** Je nach Art der Wiederherstellung ist diese Option standardmäßig aktiviert oder nicht. Wenn Sie diese Option aktivieren, werden nur die sog. "NTFS-Abzweigungspunkte" wiederhergestellt, nicht jedoch die Daten, auf die verwiesen wird.

Ein Abzweigungspunkt ist eine Verknüpfung in Form eines NTFS-Ordners (ab Windows 2000), der auf einen Zielordner auf demselben oder einem anderen Datenträger verweisen kann. Soll auf einen anderen Datenträger verwiesen werden, muss dieser zuvor als "bereitgestelltes Laufwerk" (mounted drive) konfiguriert werden. Dies erfolgt durch die Erstellung eines so genannten Bereitstellungspunkts (mount point). Dadurch kann die Limitierung auf 26 Laufwerksbuchstaben umgangen werden.

- **Vorhandene Bereitstellungspunkte beibehalten:** Diese Option ist ein Standardwert auf dieser Seite und verhindert, dass bei der Wiederherstellung Bereitstellungspunkte auf der Partition oder dem Volume überschrieben werden, auf denen Daten wiederhergestellt werden. Diese Option sollte immer dann aktiviert werden, wenn Sie die Daten eines vollständigen Laufwerks oder einer vollständigen Partition wiederherstellen. Wenn Sie beispielsweise Daten auf einem Austauschlaufwerk wiederherstellen und Sie das Laufwerk partitioniert und formatiert sowie die Bereitstellungspunkte wiederhergestellt haben, müssen Sie diese Option wählen, damit die Bereitstellungspunkte nicht überschrieben werden. Wenn Sie Daten auf einer Partition oder einem Laufwerk wiederherstellen, das unmittelbar vorher neu formatiert wurde, und Sie die bisherigen Bereitstellungspunkte wiederherstellen möchten, dürfen Sie diese Option nicht aktivieren.
- **Clusterregistrierung auf dem Quorum-Datenträger und allen anderen Knoten wiederherstellen:** Stellt sicher, dass die Quorumdatenbank des Clusters auf allen Knoten eines Serverclusters wiederhergestellt und repliziert wird. Wenn Sie diese Option auswählen, hält das Sicherungsprogramm den Clusterdienst auf allen anderen Knoten des Serverclusters an, nachdem der wiederhergestellte Knoten neu gestartet wurde. Aus diesem Grund ist das gesamte Servercluster während einer autorisierenden Wiederherstellung der Daten auf dem Quorum-Datenträger des Clusters nicht verfügbar.
- **Wiederhergestellte Daten in replizierten Datensätzen als primäre Daten für alle Replikate markieren:** Diese Option ist bei einer Wiederherstellung des Systemzustands (System State) verfügbar. Wenn Sie diese Option aktivieren, wird eine primäre Wiederherstellung vorgenommen (siehe Kapitel 10.1.6) und sichergestellt, dass wiederhergestellte Daten des Dateireplikationsdiensts auf Ihre anderen Server repliziert werden. Wählen Sie diese Option nur dann aus, wenn Sie den *ersten* Replikatsatz im Netzwerk wiederherstellen. Diese Option sollte nicht verwendet werden, wenn bereits ein oder mehr Replikatsätze wiederhergestellt worden sind.

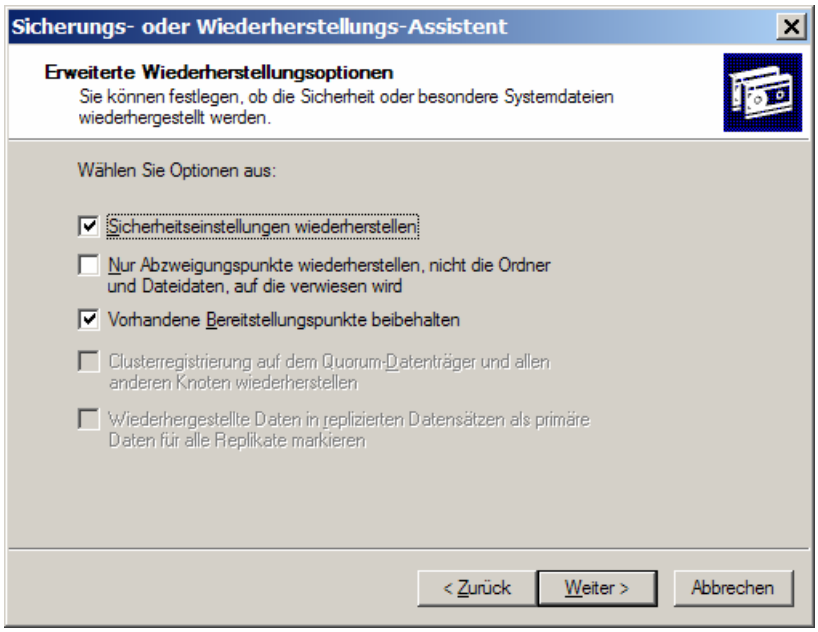


Abb. 138: Festlegen besonderer Wiederherstellungsoptionen

10.4.2 Daten wiederherstellen

Wenn Sie mit der Definition der Datenwiederherstellung fertig sind und eventuell erweiterte Wiederherstellungsoptionen gesetzt haben, wird die Seite "Fertigstellen des Assistenten" angezeigt.

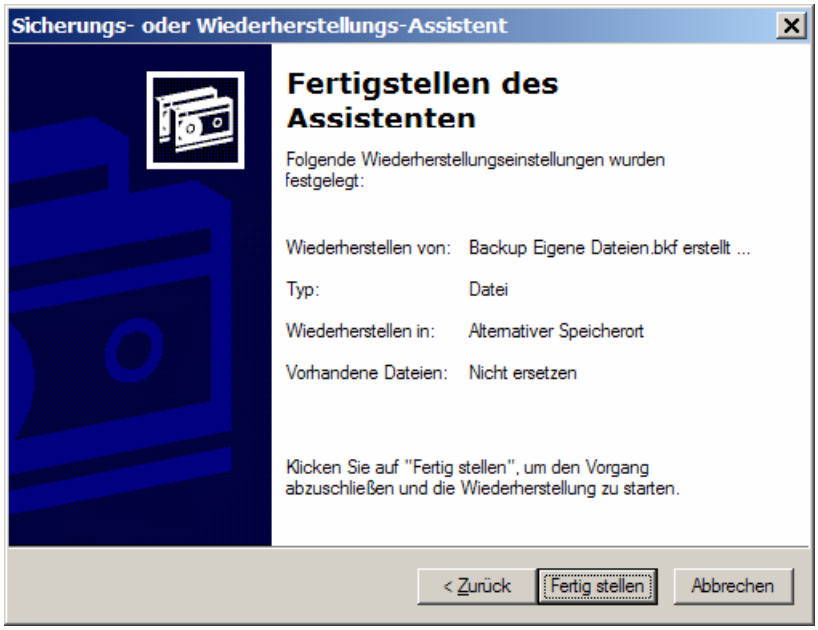


Abb. 139: Zusammenfassung der Datensicherung

Klicken Sie auf die Schaltfläche FERTIG STELLEN, um die Wiederherstellung zu starten. Es wird sofort der Dialog "Status: Wiederherstellen" angezeigt, der im Verlauf der Wiederherstellung den aktuellen Zustand anzeigt, wie die folgenden beiden Abbildungen zeigen.

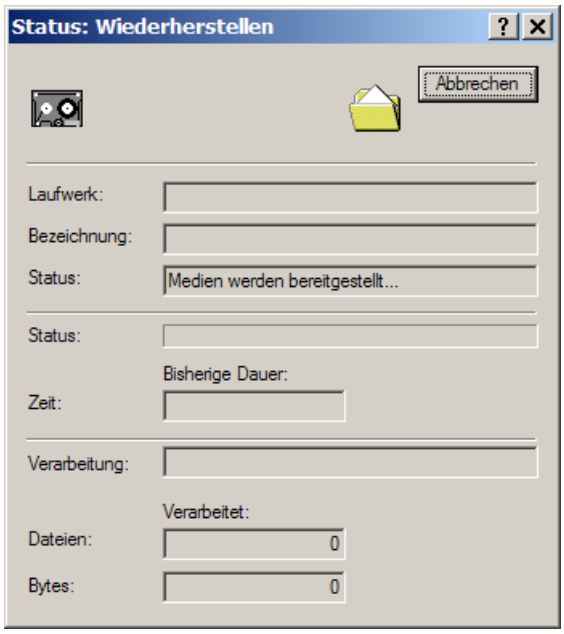


Abb. 140: Die Wiederherstellung läuft, der Zugriff auf die Sicherungsmedien erfolgt

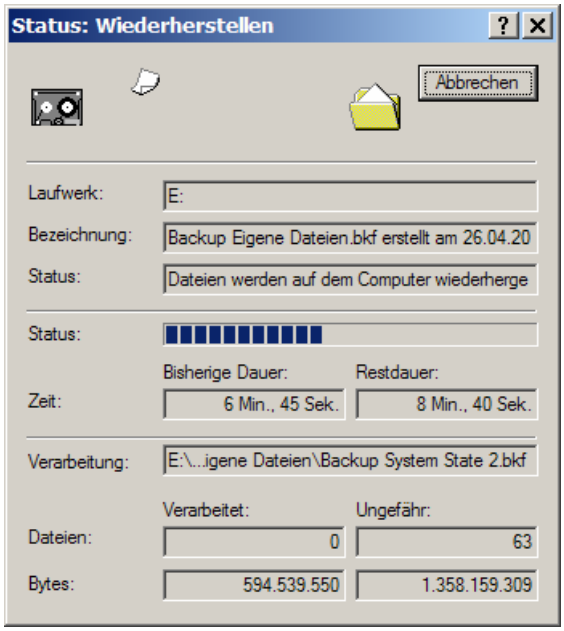


Abb. 141: Anzeige des Verlaufs der Wiederherstellung

Das Ende der Wiederherstellung wird im selben Dialog angezeigt, im Feld "Status" steht "Abgeschlossen". Zusätzlich erscheint die Schaltfläche BERICHT..., klicken Sie darauf, wenn Sie einen Bericht (als Textdatei) über den aktuellen Wiederherstellungsvorgang wünschen.

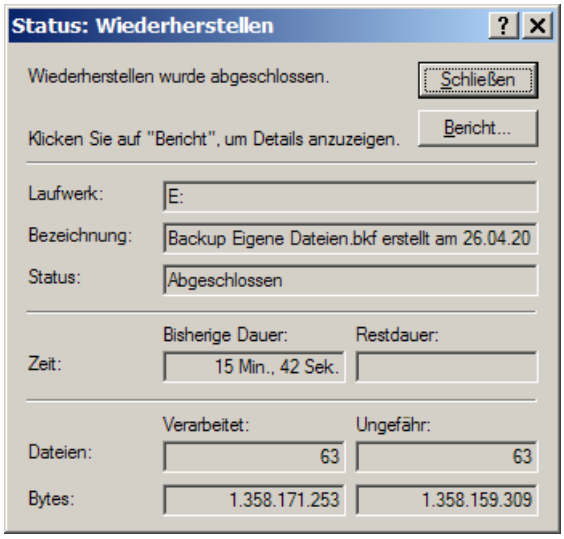


Abb. 142: Die Wiederherstellung ist beendet, optional kann ein Bericht angezeigt werden

Wenn Sie auf BERICHT... klicken, wird im Texteditor der Bericht zur aktuellen Wiederherstellung angezeigt.

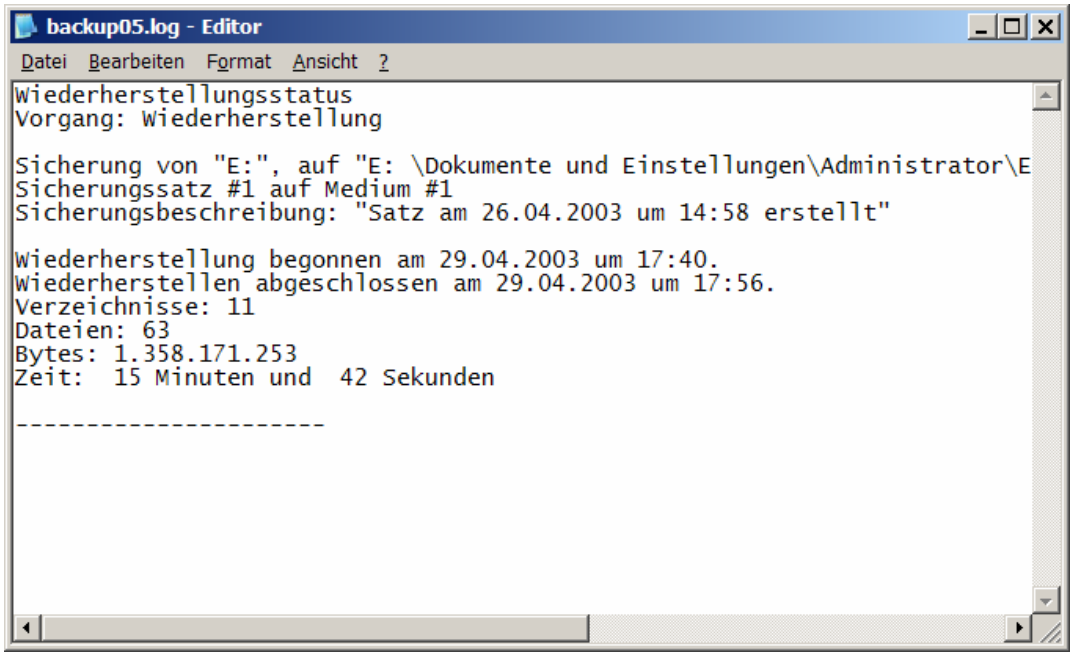


Abb. 143: Datenwiederherstellungsbericht

Diese Protokolldateien heißen standardmäßig "backupNN.log" (bei "Backup" und "Restore", NN ist eine fortlaufende Zahl), und werden in folgendem Verzeichnis gespeichert:

\Dokumente und Einstellungen\BENUTZERNAME\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows NT\NTBackup\data

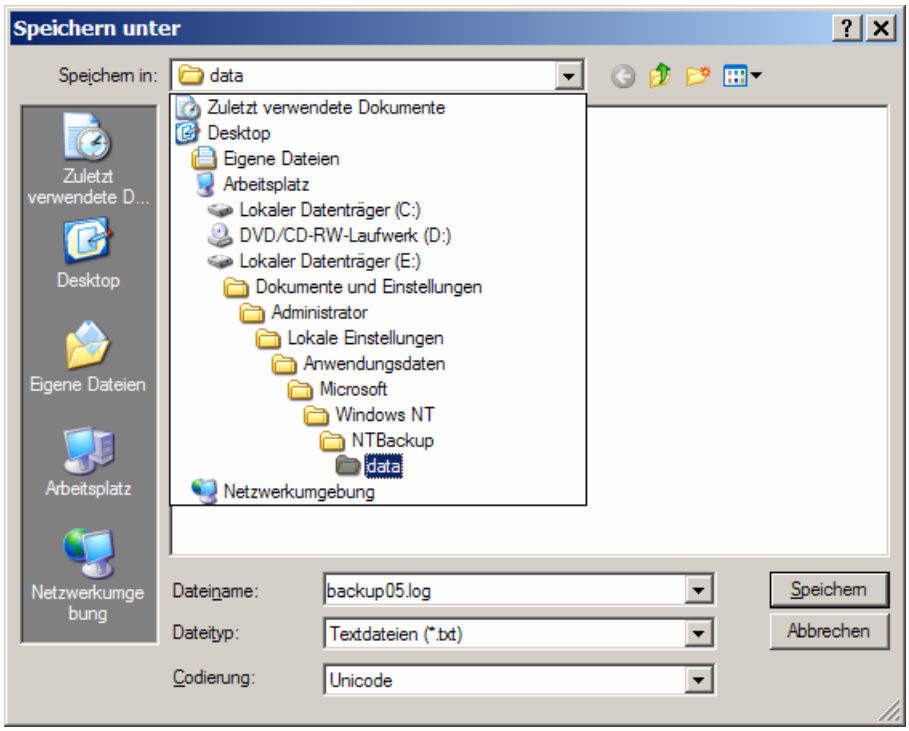


Abb. 144: Speicherort der Protokolldateien für Wiederherstellung

11 Software Update Services (SUS)

Microsoft Software Update Services (SUS) ist eine kostenlose Add-In-Komponente für Server, die auf Windows 2000 und Windows Server 2003 basieren, sowie für Desktopcomputer, auf denen Windows 2000 Professional und Windows XP Professional ausgeführt wird.

Ziel von SUS ist es, den Zugang zu den neuesten Updates, Sicherheitsupdates und Service Packs zu erleichtern bzw. zu beschleunigen.

11.1 Allgemeines

SUS stellen Client-PCs mit speziellen Microsoft-Betriebssystemen über das Netzwerk so genannte "Wichtige Updates" bereit. Allgemeine Updates oder Treiberupdates müssen weiterhin über die Microsoft-Updatewebseite abgerufen werden. Mit SUS behält der Netzwerkadministrator die Kontrolle darüber, wann welche Updates auf welche PCs verteilt werden.

11.1.1 Problemstellung

Bei der standardmäßigen Verwendung der SUS im Schulbetrieb fallen zwei Punkte auf:

- Updates werden aus dem Internet geladen, d. h. alle Clients mit aktiviertem SUS laden die identischen Patches von der Microsoft-Updateseite. Dies führt zu einer unnötig hohen Netzwerklast an der Internetverbindung der Schule.
- Es ist keine Vorauswahl der zu installierenden Patches möglich.

11.1.2 Lösung

Installation und Konfiguration eines lokalen SUS-Servers innerhalb des Schulnetzwerks:

- Client-PCs beziehen ihre Updates zukünftig automatisch vom SUS-Server innerhalb des Schulnetzwerks. Er wird so konfiguriert, dass er die in Frage kommenden Patches während der Nacht vom Microsoft-Updateserver holt und damit die Internetverbindung der Schule während der Unterrichtszeit nicht belastet.
- Der Netzwerkadministrator kann festlegen, dass er Updates/Patches aus vom SUS-Server prüft und bestätigt, bevor Client-PCs sie abrufen dürfen. Mit dieser Vorfilterung kann er beispielsweise bekanntermaßen fehlerhafte Patches vom Update-Prozess ausgrenzen.

Einschränkungen von SUS

- Benötigt mindestens Windows 2000
- Keine Unterstützung für Microsoft Office
- Zentralisierte Deinstallation von automatisch verteilten Updates ist nicht möglich

Funktionsweise von SUS

1. „Windows Update Synchronsiation"-Dienst synchronisiert den SUS-Server in regelmäßigen Zeitabständen über Port 80 (http) mit einem Microsoft Windows Updateserver.
2. Ein Client prüft eine gewisse Zeitspanne nach dem Hochfahren den SUS-Server auf neue genehmigte Updates.
3. Falls der Client ein erforderliches Update erkennt und entsprechend konfiguriert ist, beginnt er über Port 80 (http) mit dem Download des Updates vom SUS-Server und der anschließenden Installation.

© 2005, Microsoft Österreich GmbH

4. Falls der Client entsprechend konfiguriert ist, unterdrückt er einen eventuell notwendigen Reboot des Systems, d. h. die Updates werden erst dann aktiv, wenn der Benutzer selbst den Client neu startet.

Die aktuelle Version des SUS-Servers kann auch Servicepacks (ab Windows 2000 SP4 und ab Windows XP SP1a) verteilen. Von den unter http://v4.windowsupdate.microsoft.com/de/ angebotenen Hotfixes, Patches und Updates können damit keine Dateien unter „Empfohlen" bzw. „Treiberupdates" installiert werden.

11.2 Systemvoraussetzungen für die Schule

11.2.1 SUS-Server

Für die Installation des SUS-Servers müssen folgende Voraussetzungen gegeben sein:

- P3 700 MHz mit 256MB RAM und 8 GB freiem Plattenplatz
- Mindestens Windows 2000 Server mit aktuellem SP
- Installierter IIS
- Dienst „Software Update Service Synchronisation Service" muss auf „Automatisch" gestellt sein

Die aktuelle Version des SUS-Servers kann auch auf einem Domänencontroller installiert werden.

11.2.2 Client

Die Voraussetzungen auf dem Client sind mindestens Windows 2000 SP3 oder Windows XP SP1.

11.3 Installation und Konfiguration eines SUS-Servers

- Erstellen Sie am künftigen SUS-Server eine eigene NTFS-Partition mit ca. 5 GB Größe und weisen Sie ihr den Laufwerksbuchstaben S: zu.
- Laden Sie sich kostenlos die aktuelle Version des SUS-Servers von folgender Adresse: http://www.microsoft.com/windowsserversystem/sus
- Rufen Sie die Installationsdatei des SUS-Servers auf.

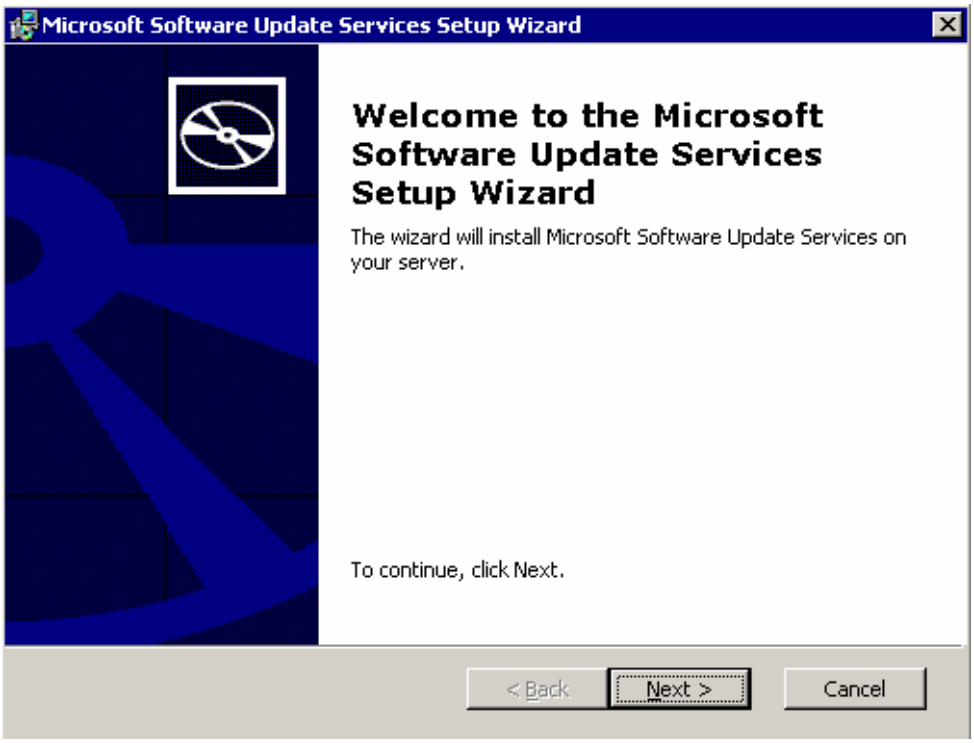


Abb. 145: Willkommensbildschirm

- Gehen Sie mit NEXT zur nächsten Seite.

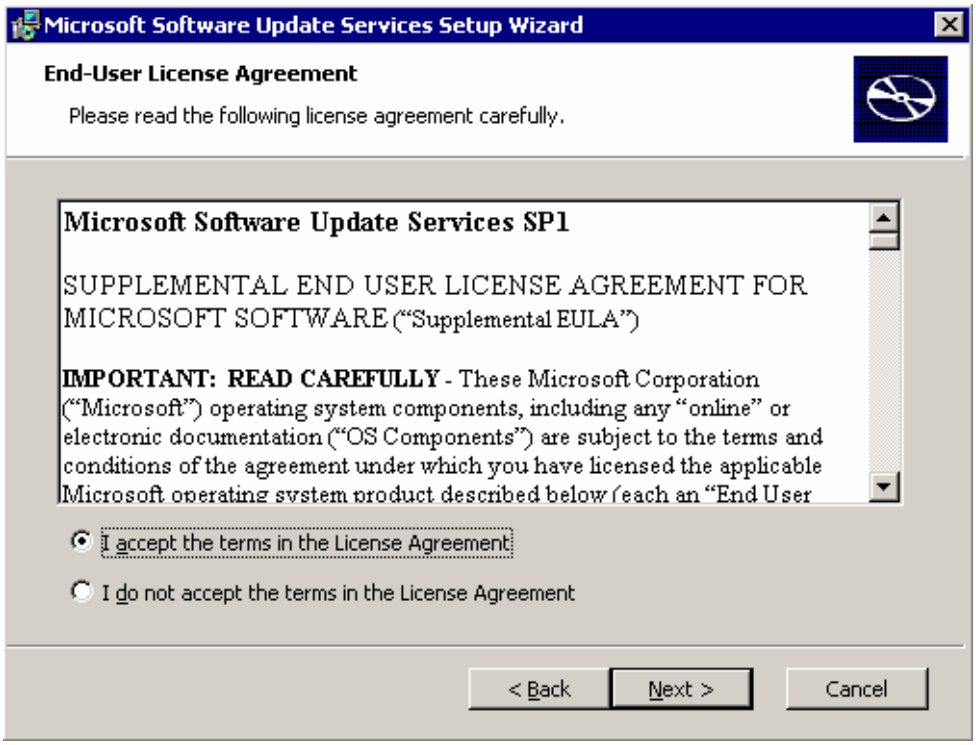


Abb. 146: Bestätigung der Lizenzvereinbarung

- Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Next.**

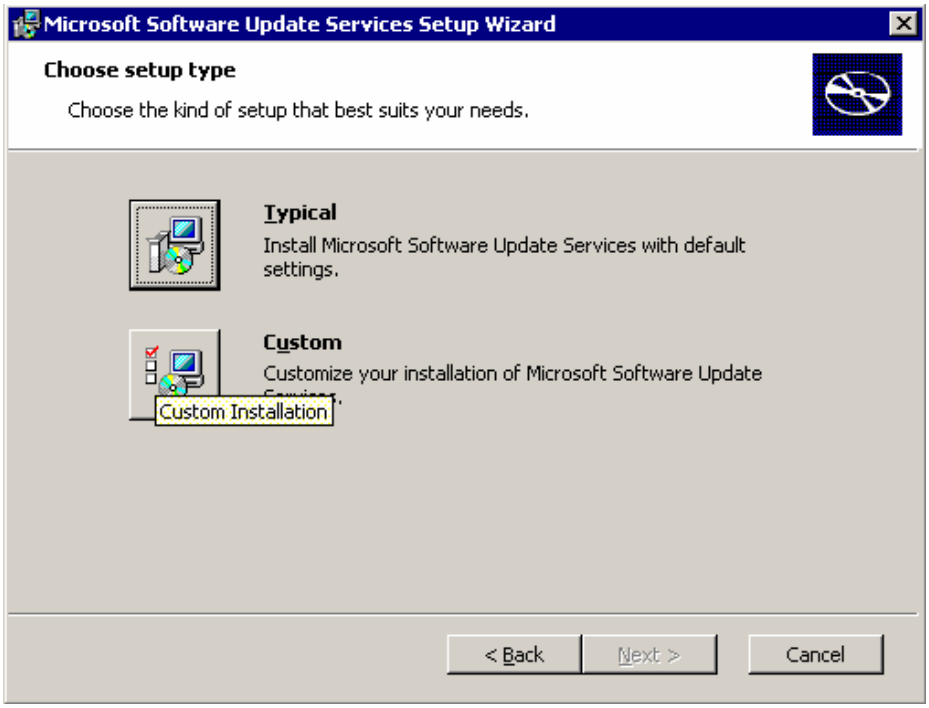


Abb. 147: Auswahl der Installationsart

- Wählen Sie hier CUSTOM aus.

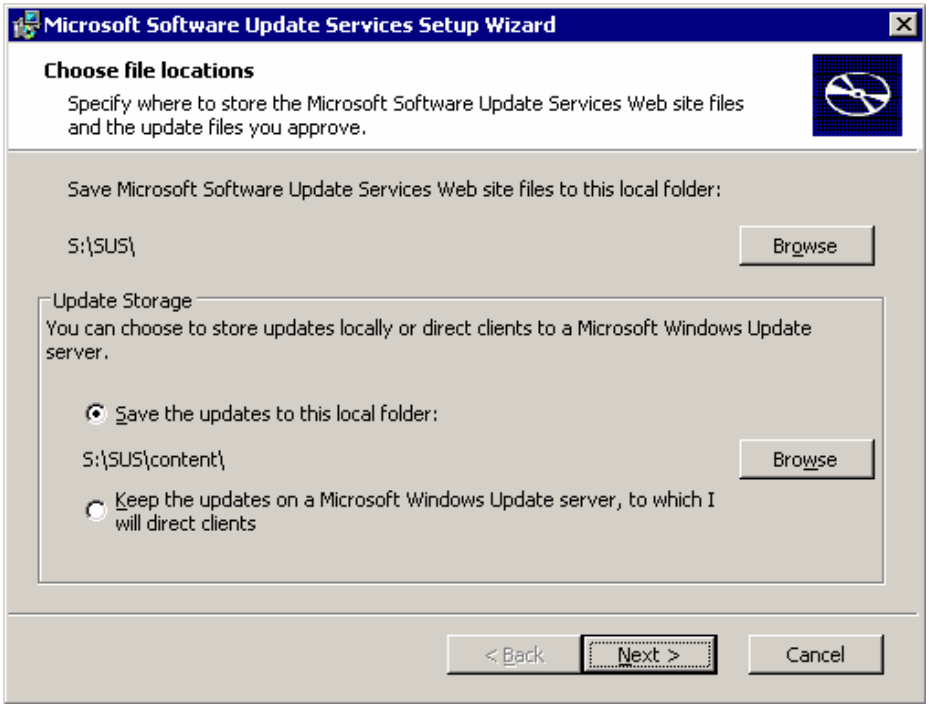


Abb. 148: Speicherpfad angeben

- Definieren Sie als Installationspfad S:\SUS und klicken auf NEXT.

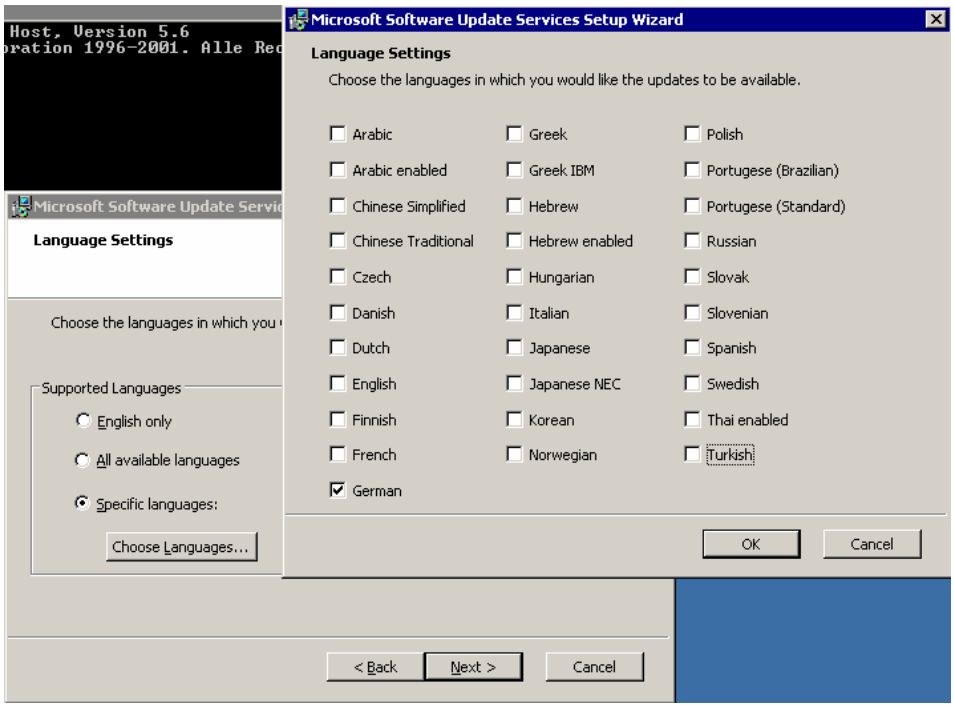


Abb. 149: Auswahl der Sprache

- Wählen Sie als Sprache GERMAN aus, wenn Sie an den Clients nur deutsche Versionen des MS-Betriebssystems verwenden (ansonsten weitere Sprachen wählen). Bestätigen Sie das Fenster mit OK und klicken auf NEXT.

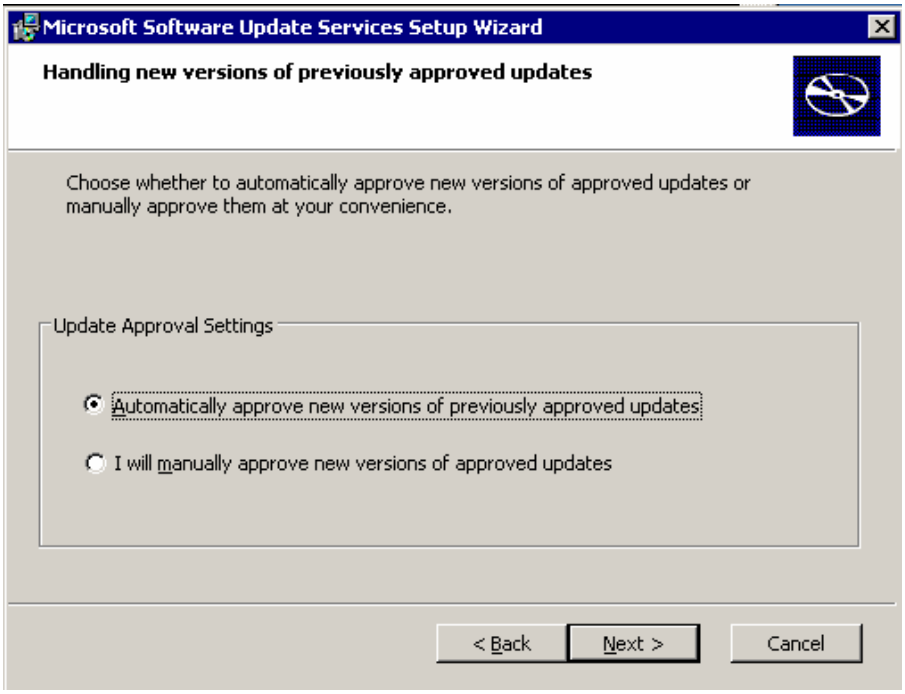


Abb. 150: Automatisches oder manuelles Bestätigen der Updates

- Wählen Sie hier AUTOMATICALLY APPROVE NEW VERSIONS OF PREVIOUS APPROVED UPDATES aus, damit Sie nicht jedes von Microsoft zur Verfügung gestellte Update vor der Auslieferung an die Clients von Hand bestätigen müssen, und klicken Sie auf NEXT.

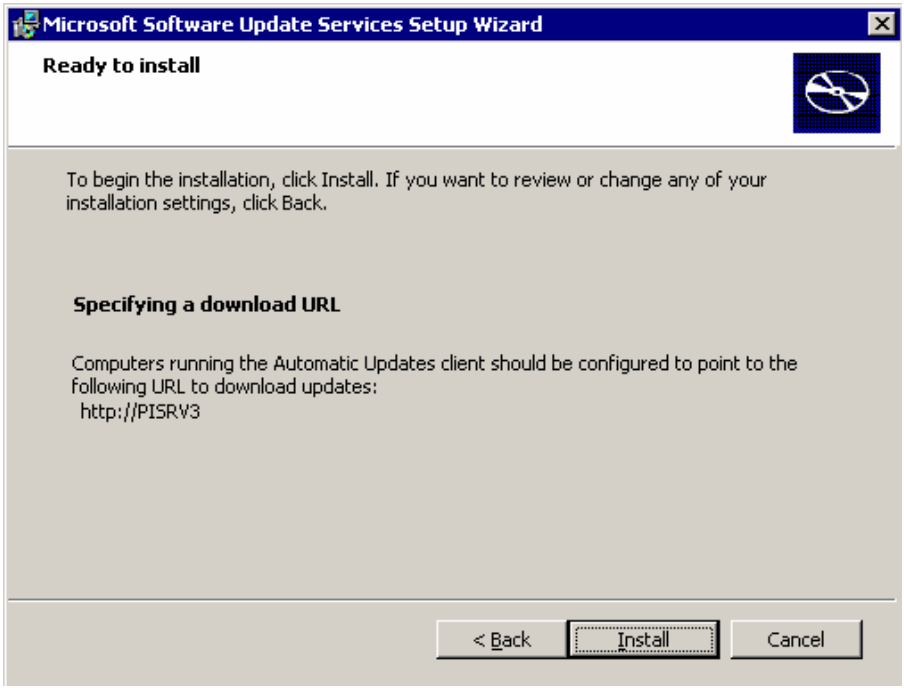


Abb. 151: Installation starten

- Nach dem Klick auf INSTALL wird der SUS-Server installiert.

11.4 Konfiguration des SUS-Servers

Nach erfolgreicher Installation kann der SUS-Server am Server selber über http://localhost/susadmin/ bzw. über den DNS-Namen (z. B. http://srv01.meineschule.local/susadmin/) verwaltet werden.

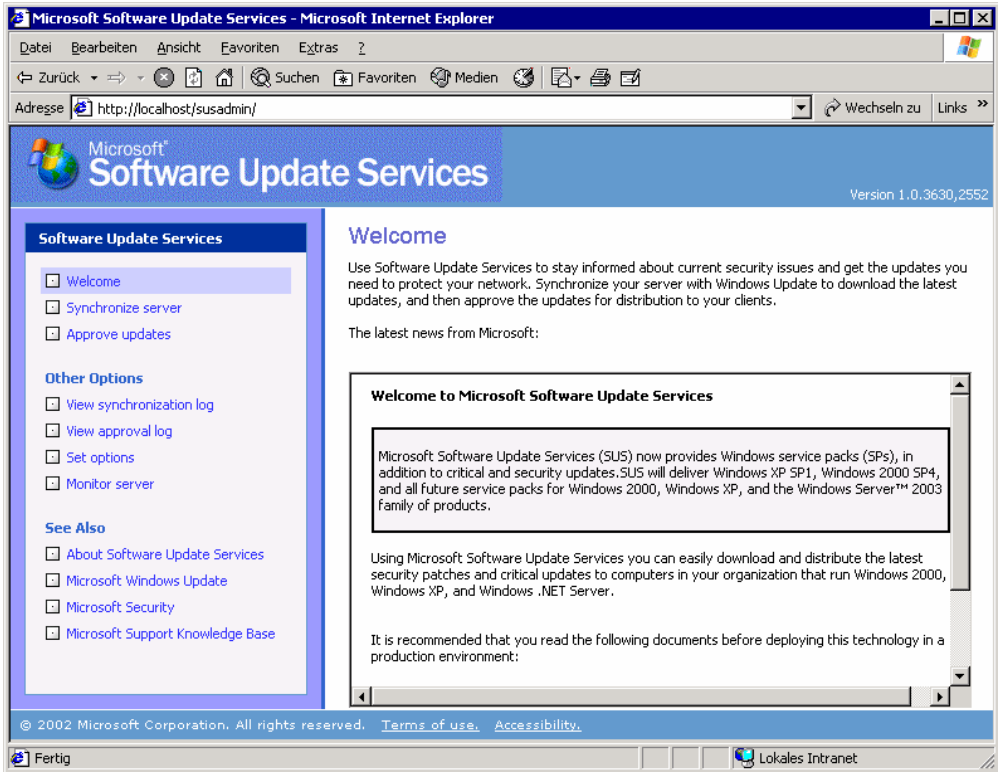


Abb. 152: Willkommensbildschirm des SUS-Servers

Über den Link SET OPTIONS auf der linken Seite, können Sie nun die Einstellungen des SUS-Servers festlegen:

- SELECT A PROXY SERVER CONFIGURATION: Sollte in Ihrem Netzwerk eine Internetverbindung nur über einen Proxyserver erlaubt sein, muss dieser hier angegeben werden. Eine eventuell notwendige Proxyauthentifizierung kann hier ebenfalls erledigt werden.
- SPECIFY THE NAME YOUR CLIENTS USE TO LOCATE THIS UPDATE SERVER: Hier könne Sie den Namen Ihres SUS-Servers ändern. Als Voreinstellung steht hier der NetBIOS Name des SUS-Servers.

	Eine Änderung dieser Einstellung muss auch bei der Clientkonfiguration berücksichtigt werden.

- SELECT WHICH SERVER TO SYNCHRONIZE CONTENT FROM: Hier geben Sie die Quelle an, mit der der SUS-Server sich synchronisieren soll. Für den Einsatz in der Schule sollte die Voreinstellung „Synchronize directly from the Microsoft Windows Update Servers" beibehalten werden.
- SELECT HOW YOU WANT TO HANDLE NEW VERSIONS OF PREVIOUSLY APPROVED UPDATES: Damit definieren Sie die Vorgehensweise bei neuen Updates.

- Falls ein bereits am Client installiertes Update durch eine neuere Version ersetzt werden soll, wählen Sie die Option AUTOMATICALLY APPROVE NEW VERSIONS OF PREVIOUSLY APPROVED UPDATES.
- Soll SUS jedoch bei einer neuen Version eines Updates warten, bis sie vom Administrator freigegeben wurde, dann wählen Sie DO NOT AUTOMATICALLY APPROVE NEW VERSIONS OF PREVIOUSLY APPROVED UPDATES. I WILL MANUALLY APPROVE THESE LATER.

◆ SELECT WHERE YOU WANT TO STORE UPDATES: Hier definieren Sie, wo die Updates gespeichert werden sollen. Da der Update-Katalog immer von der Microsoft-Updateseite heruntergeladen wird, könnten auch die Updates am Windows Update Server belassen werden, anstatt sie auf den SUS-Server herunterzuladen. Für den Schulbetrieb ist allerdings die Einstellung SAVE THE UPDATES TO A LOCAL FOLDER zu bevorzugen. Legen Sie dafür die gewünschte Sprache(n) fest, in der/denen Sie die Windowsupdates wünschen.

Übernehmen Sie Ihre Einstellungen mit dem Button APPLY.

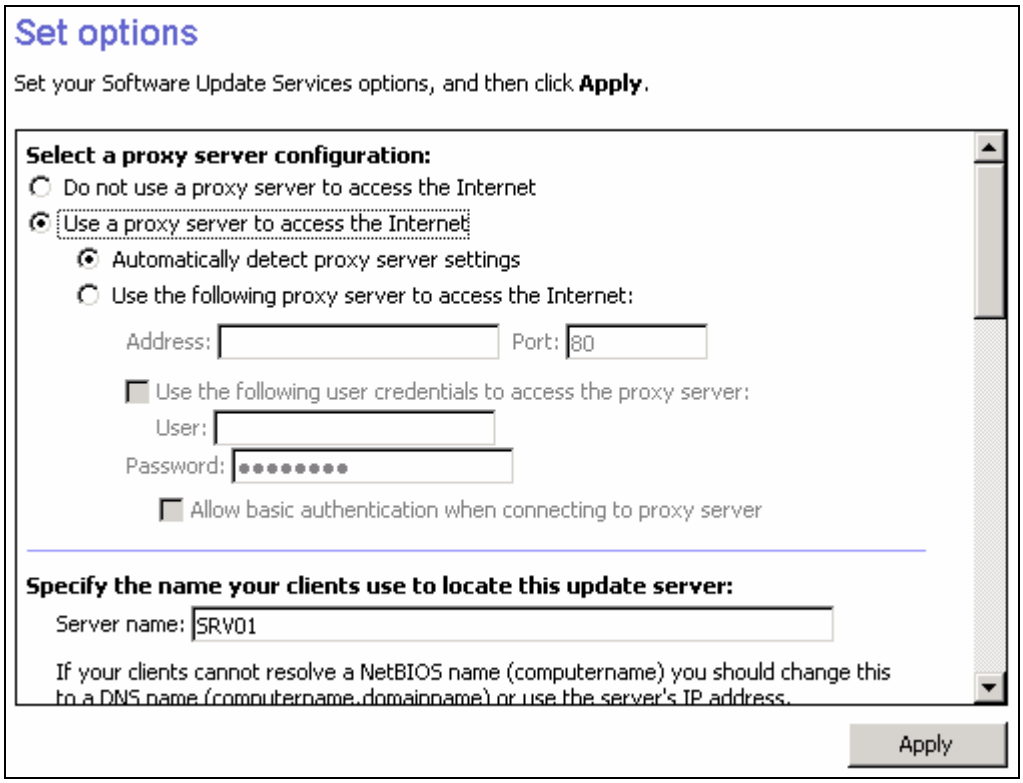


Abb. 153: Einstellungen des SUS-Servers

Die Einstellung unter SPECIFY THE NAME YOUR CLIENTS USE TO LOCATE THIS UPDATE SERVER sollte die IP oder den FQDN (Full Qualified Domain Name) des SUS-Servers aufweisen, falls die Clients diesen nicht über seinen NetBIOS-Namen auflösen können.

Als nächstes klicken Sie im Menü links auf SYNCHRONIZE SERVER und wählen SYNCHRONIZE SCHEDULE aus, um einen Zeitplan für den automatischen Download der Updates von der Microsoft-Updateseite einzurichten.

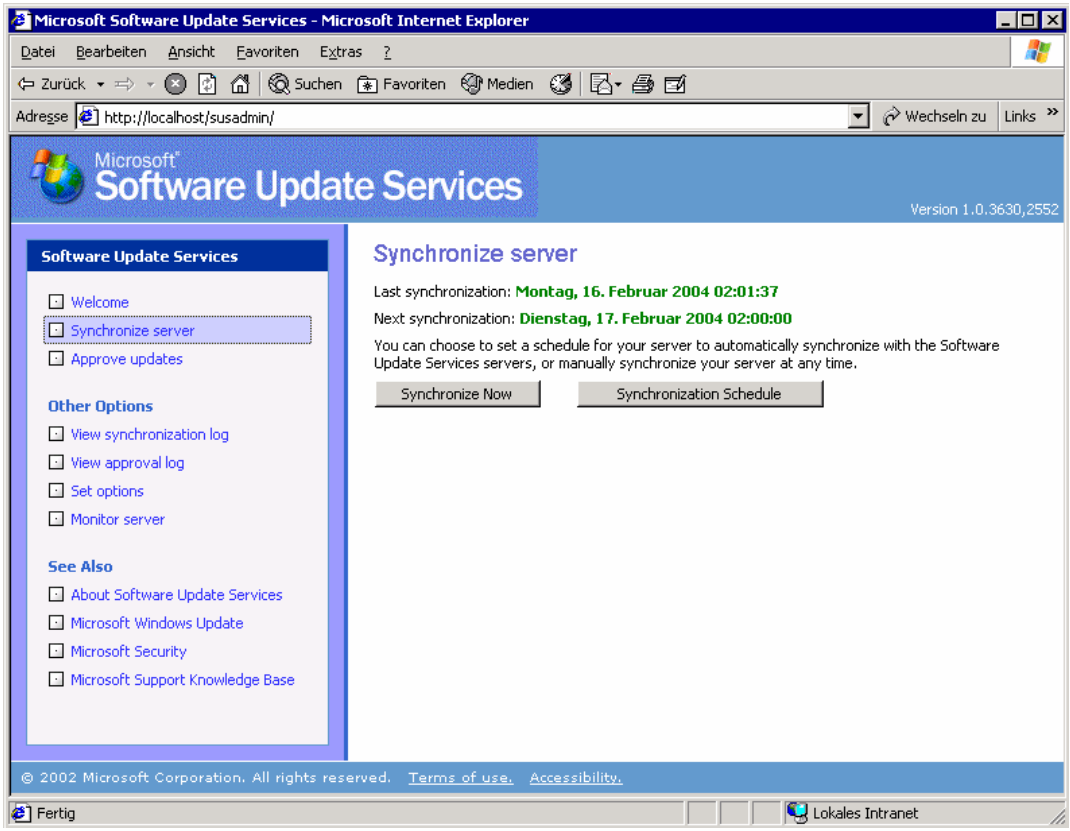


Abb. 154: Auswahl einer sofortigen oder geplanten Synchronisation

Definieren Sie nun die Synchronisationseinstellungen Ihres SUS-Servers und klicken Sie anschließend OK.

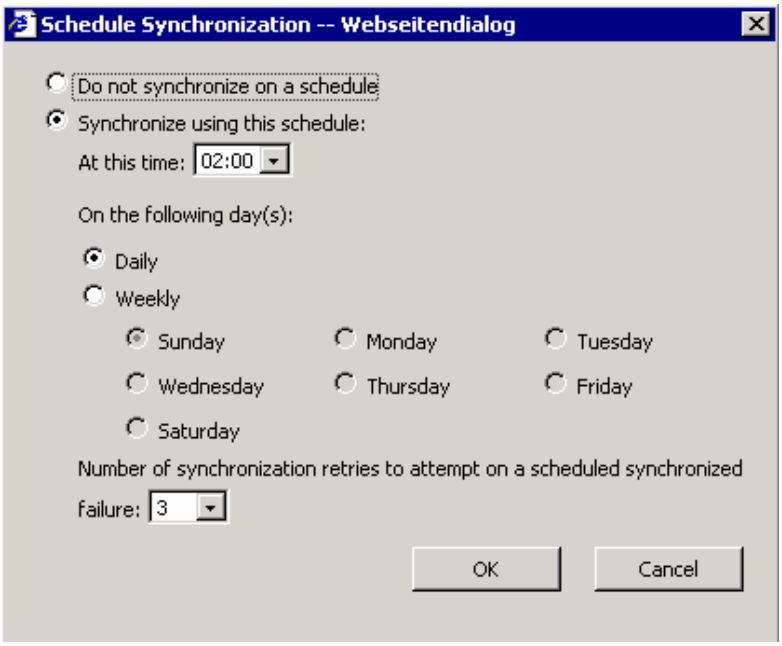


Abb. 155: Einstellungen der geplanten Synchronisation

Ändern Sie die Uhrzeit für die Synchronisation (z. B. auf 05:00 Uhr), da es mit den Defaulteinstellungen leicht vorkommen kann, dass die Microsoft Update Server überlastet sind.

Einem erfolglosen Versuch der Synchronisation wiederholt der SUS-Server nach 30 Minuten.

Klicken Sie anschließend auf den Button SYNCHRONIZE NOW um die Synchronisation erstmalig zu starten. Der Vorgang nimmt einige Zeit in Anspruch.

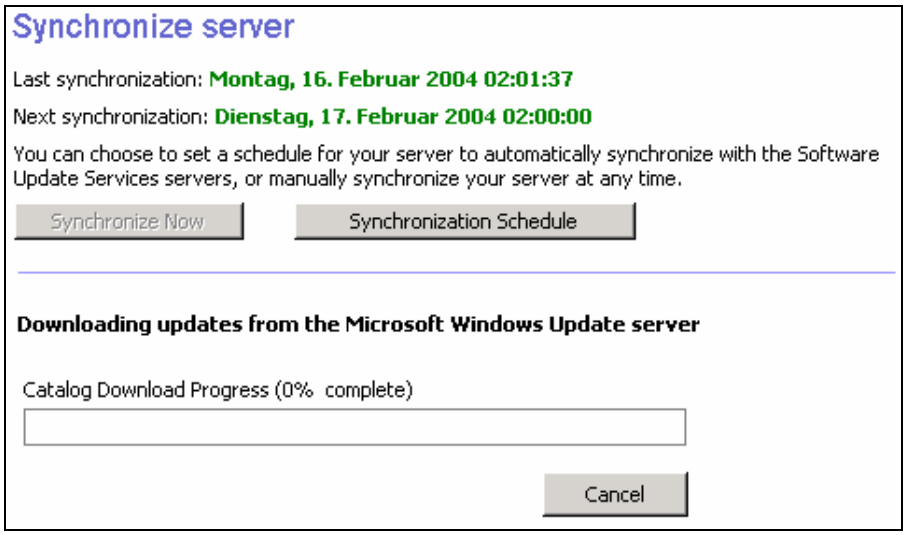


Abb. 156: Synchronisation

Nun ist der SUS-Server eingerichtet und kann für die automatische zentrale Verteilung an die Clients verwendet werden.

Über den Link APPROVE UPDATES kann man sich eine Liste aller Updates ausgeben lassen – geordnet nach Updatedatum, Titel, Plattform und Status.

Mögliche Statuswerte sind:

- approved: Update ist für die Verteilung an die Clients freigegeben
- not approved, new: Update wurde für die Verteilung noch nicht freigegeben
- updated: Update ist eine neue Version eines bereits veröffentlichten Updates
- unavailable: Update kann derzeit nicht heruntergeladen werden

11.5 Konfiguration der Clients für die Verwendung von SUS

Es gibt mehrere Möglichkeiten, den Client für die Verwendung von SUS zu konfigurieren:

- Über die lokale Gruppenrichtlinie
- Über die Registrierung
- Über eine Active-Directory-Gruppenrichtlinie

Für den Einsatz in der Schule ist die Konfiguration über einer Active-Directory-Gruppenrichtlinie zu bevorzugen.

11.5.1 Vorgehensweise:

- Klicken Sie auf einem Active-Directory-Domänencontroller auf START und anschließend auf AUSFÜHREN.
- Geben Sie ***dsa.msc*** ein, um das Snap-In "Active Directory-Benutzer und -Computer" zu laden.
- Klicken Sie mit der rechten Maustaste auf die Organisationseinheit oder Domäne, in der Sie die Richtlinie erstellen möchten, und klicken Sie auf EIGENSCHAFTEN.
- Klicken Sie auf die Registerkarte GRUPPENRICHTLINIE und anschließend auf NEU.
- Geben Sie einen Namen für die Richtlinie ein, und klicken Sie auf BEARBEITEN.
- Klicken Sie auf COMPUTERKONFIGURATION – ADMINISTRATIVE VORLAGEN – WINDOWS-KOMPONENTEN – WINDOWS UPDATE

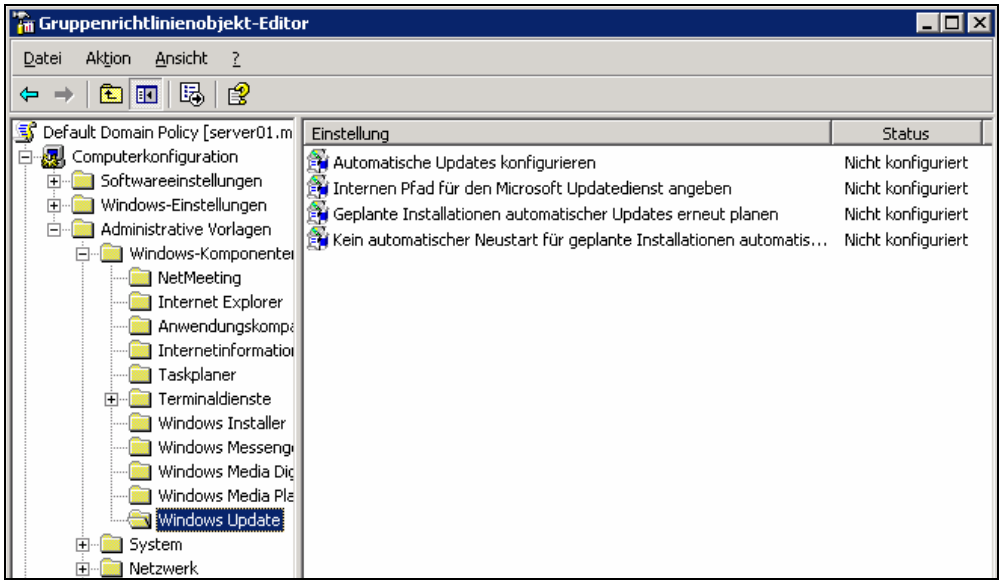


Abb. 157: Bearbeiten der Gruppenrichtlinien

11.5.2 Einstellung: Automatische Updates konfigurieren

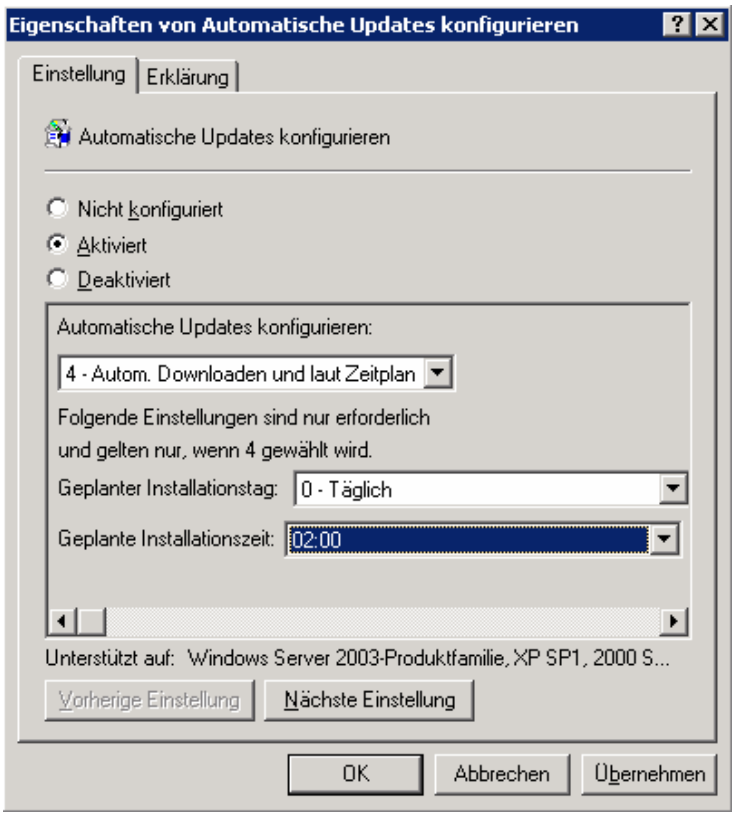


Abb. 158: Eigenschaften der automatischen Updates

Es gibt verschiedenen Einstellungsmöglichkeiten:

1. NICHT VERWENDET
2. VOR DEM DOWNLOAD VON UPDATES BENACHRICHTIGEN UND VOR DEREN INSTALLATION ERNEUT BENACHRICHTIGEN: Wenn Windows Updates ermittelt, die für diesen Computer geeignet sind, wird ein Statusbereichssymbol mit einer Meldung angezeigt, dass Updates zum Download bereitstehen. Durch Klicken auf das Symbol oder die Meldung können Sie Updates zum Downloaden auswählen.
   Die ausgewählten Updates werden im Hintergrund übertragen. Nach dem Download zeigt der Statusbereich erneut ein Symbol, das Sie darüber informiert, dass die Updates installiert werden können. Wenn Sie auf das Symbol oder die Meldung klicken, können Sie die Updates auswählen, die installiert werden sollen.
3. (STANDARDEINSTELLUNG) UPDATES AUTOMATISCH DOWNLOADEN UND ÜBER INSTALLIERBARE UPDATES BENACHRICHTIGEN: Windows sucht nach anwendbaren Updates für den Computer und überträgt sie im Hintergrund automatisch (der Benutzer wird während dieses Vorgangs nicht benachrichtigt oder gestört). Nach dem Download benachrichtigt Sie ein Symbol im Statusbereich, dass die Updates installationsbereit sind. Durch klicken auf das Symbol oder die Meldung können Sie die Updates auswählen, die Sie installieren möchten.
4. UPDATES AUTOMATISCH DOWNLOADEN UND LAUT ANGEGEBENEM ZEITPLAN INSTALLIEREN: Legen Sie den Zeitplan mit den Optionen in der Gruppenrichtlinieneinstellung fest. Standardmäßig sind Installationen um 03:00 Uhr morgens geplant, falls kein Zeitplan etwas anderes festlegt. Falls für Updates ein Neustart erforderlich ist, startet Windows den Computer automatisch neu. (Falls ein Benutzer am Computer angemeldet ist, wenn Windows neu gestartet werden soll, wird der Benutzer benachrichtigt und kann den Neustart verzögern.)

Für den Schulbereich wird Einstellung 4 dringend empfohlen.

11.5.3 Einstellung: Internen Pfad für den Microsoft-Updatedienst angeben

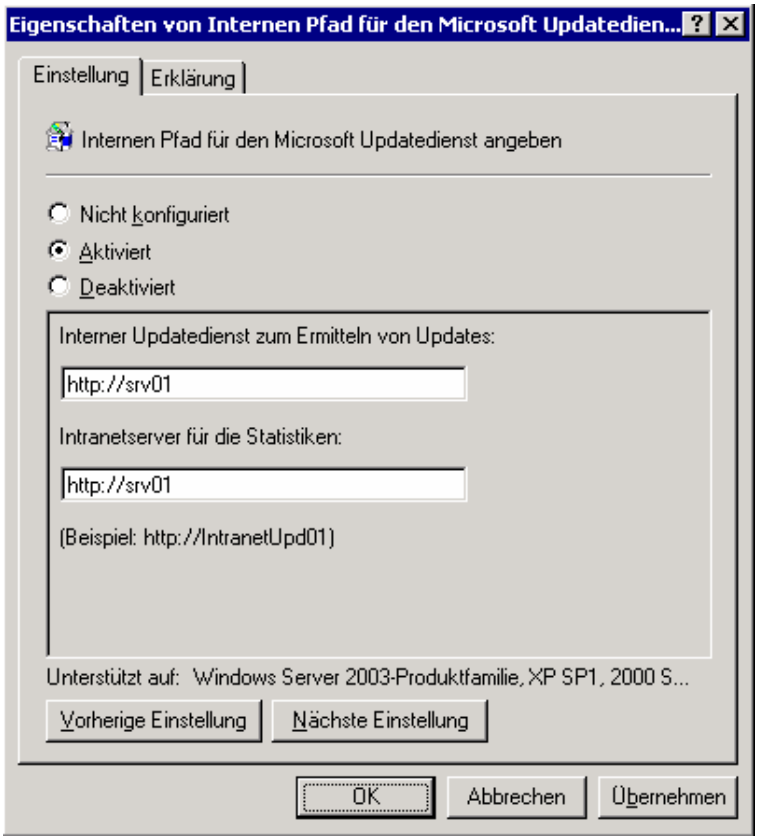


Abb. 159: Eigenschaften von internen Pfaden des SUS-Servers

Aktivieren Sie zunächst diese Einstellung und geben dann in beiden Eingabefeldern den NetBios-Namen bzw. den FQDN des SUS-Servers an.

11.5.4 Einstellung: Geplante Installationen automatischer Updates erneut planen

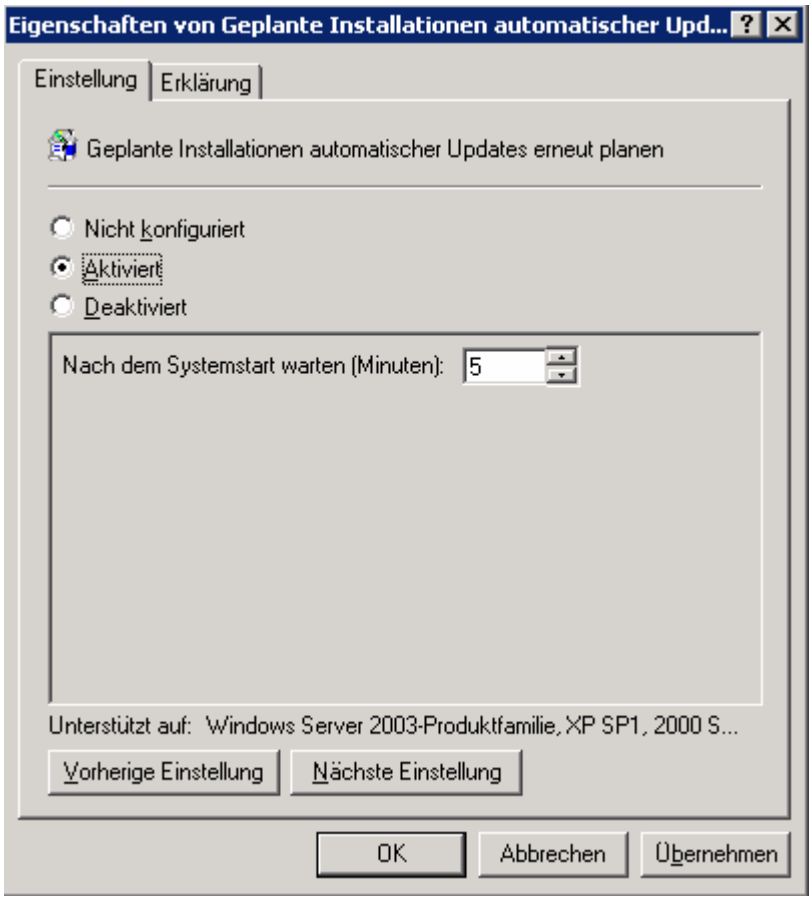


Abb. 160: Planung der Installation von automatischen Updates

Hier können Sie einstellen, ob und wann der Rechner das automatische Update erneut versuchen soll, falls er zur Zeit des geplanten Updates nicht eingeschaltet war.

11.5.5 Einstellung: Kein automatischer Neustart für geplante Installationen

Ist diese Einstellung nicht konfiguriert oder deaktiviert, wird fünf Minuten nach der Installation der Updates ein automatischer Neustart ausgeführt, wenn eines der installierten Updates oder mehrere dies erfordern. Ist diese Einstellung aktiviert, so werden Sie bei Bedarf aufgefordert den Neustart manuell vorzunehmen. Beachten Sie bitte, dass ein Neustart in jedem Fall früher oder später ausgeführt werden muss, da ansonsten künftige Update nicht entdeckt und damit nicht heruntergeladen und installiert werden.

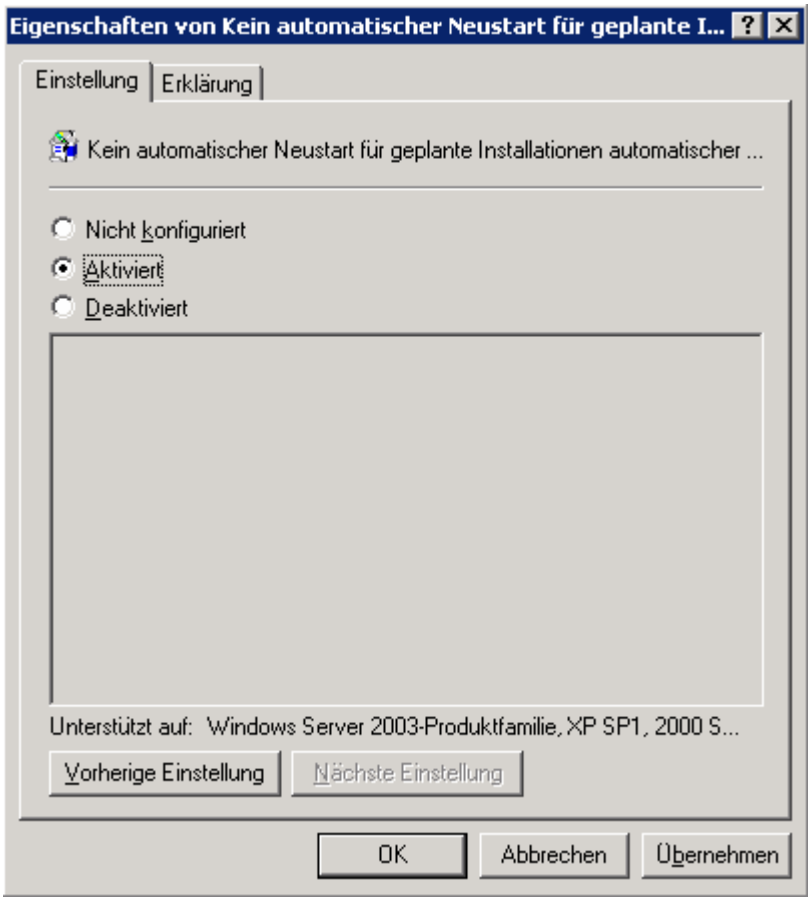


Abb. 161: Kein automatischer Neustart für geplante Installationen

Als nächstes muss der Updatedienst am Client gestartet werden. Auch dies kann über Einstellungen in einer Gruppenrichtlinie realisiert werden. Klicken Sie auf COMPUTERKONFIGURATION – WINDOWS-EINSTELLUNGEN – SICHERHEITSEINSTELLUNGEN – SYSTEMDIENSTE – AUTOMATISCHE UPDATES.

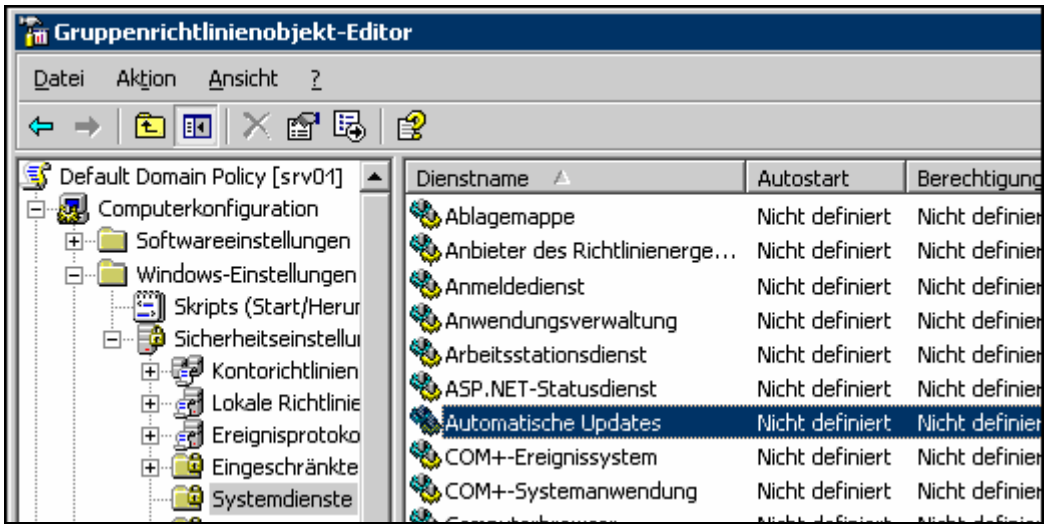


Abb. 162: Gruppenrichtlinienobjekt-Editor

Nach einem Doppelklick auf AUTOMATISCHE UPDATES aktivieren Sie diese Richtlinie und stellen als Startmodus AUTOMATISCH ein.

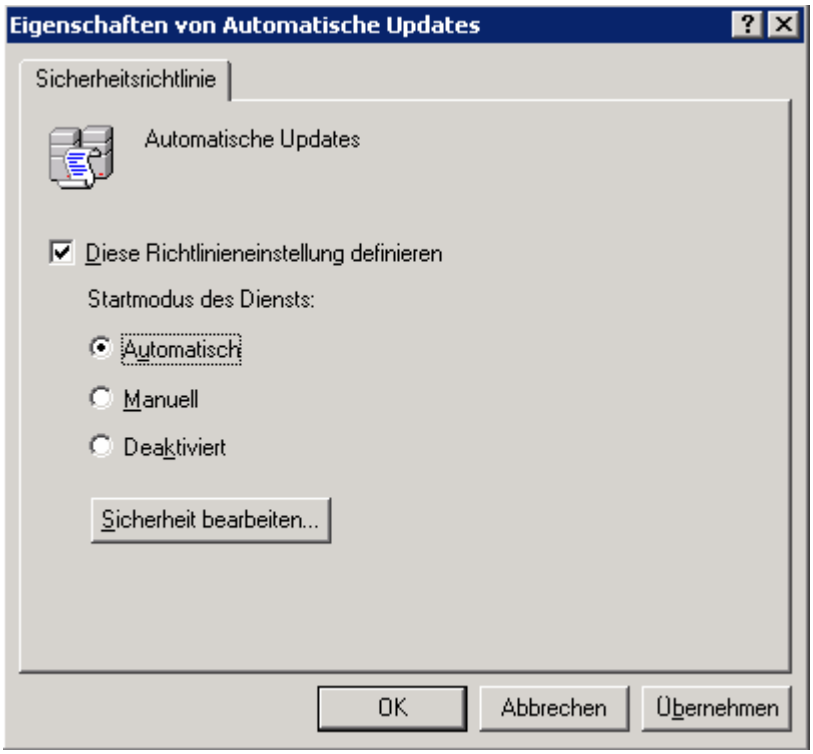


Abb. 163: Eigenschaften von automatischen Updates

11.6 Überprüfung der Aktivitäten und Fehlersuche

Im Windows-Ordner befindet sich die Datei "Windows update.log", die die Kommunikation mit dem SUS-Server protokolliert.

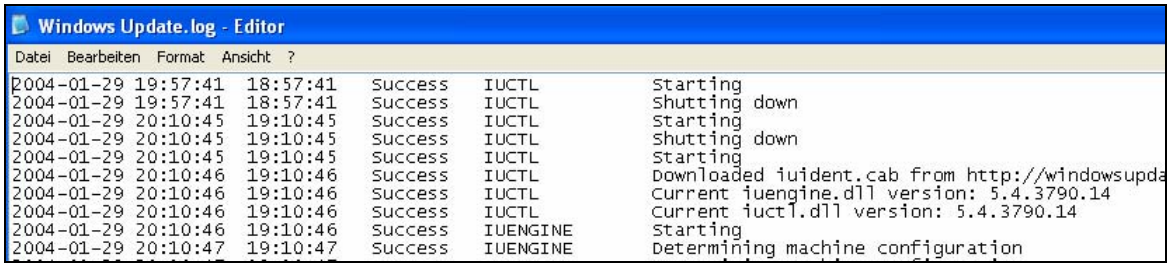


Abb. 164: Windows Update.log

Ebenso werden die Updatevorgänge in der Ereignisanzeige im Bereich "System" protokolliert, um fehlerhafte oder erfolgreiche Updatevorgänge nachzulesen:

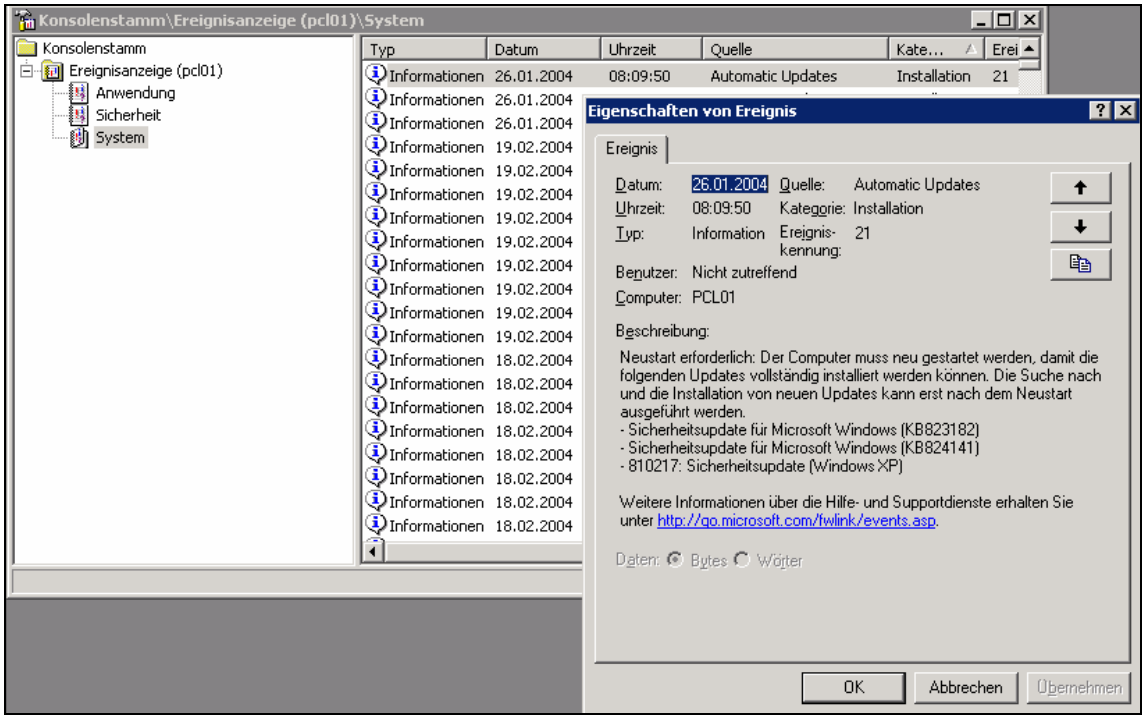


Abb. 165: Ereignisanzeige im Bereich „System“

12 Anhang A - Internet Information Services 6.0

Dieses Kapitel erläutert Installation und Konfiguration der Internet Information Services 6.0 (IIS) unter Windows Server 2003.

12.1 Überblick – Definition

Die Einführung der Windows Server 2003-Familie bedeutete gleichzeitig die Einführung der Anwendungsserver und einer neuen Serverfunktion. Damit wird eine einheitliche und durchgängige Konfiguration bestimmter Technologien erreicht. Die Bestandteile dieser neuen Serverrolle sind:

- Internetinformationsdienste
- ASP.NET
- ASP
- COM+
- Microsoft Message Queuing (MSMQ)
- Microsoft Data Engine (MSDE)

Die Kombination dieser Technologien auf einem Server hat für Webanwendungsentwickler und Administratoren den Vorteil, dynamische Inhalte wie z. B. von Datenbanken gesteuerte ASP.NET-Anwendungen ohne zusätzliche Software auf dem Server hosten zu können.

Dieser Abschnitt beschreibt die grundlegenden Funktionen und Features, die Ihnen die neuen „Internet-Informations-Services" (IIS) bieten.

Die Produkte der Windows Server 2003-Familie bietet mit der neuen, gegenüber den Vorgängern stark verbesserten, Version 6.0 der Internetinformationsdienste eine verlässliche und sichere Basis für Internetanwendungen und XML Web-Services. Nachdem man vor allem auch im Bereich der Skalierbarkeit einiges an Potenzial freigesetzt hat, findet man nun auch die ideale Plattform für Webanwendungen aller Art und aller Größe.

In diesem Kapitel erhalten Sie folgende Informationen:

- Neuerungen in IIS 6.0
- Installation des Anwendungsservers
- Konfiguration des Anwendungsservers
- Verwalten von Websites
- Verwalten von FTP-Sites
- Grundlagen der SMTP-Server-Verwaltung
- IIS 5.0 Isolation Modus

12.2 Neuerung in IIS 6.0

In IIS 6.0 wurden zahlreiche Neuerungen und Verbesserungen gegenüber den Vorgängerversionen erzielt. Die wichtigsten Features fasst die nachfolgende Aufstellung zusammen:

Einige dieser Neuerungen werden weiter unten in diesem Kapitel ausführlicher erläutert. Die nachfolgende Auflistung soll nur einen groben Überblick für erfahrene Benutzer darstellen.

12.2.1 Verbesserte Leistung

- IIS 6.0 führt einen neuen Kernelmodustreiber ein, wodurch der Durchsatz erhöht wird.
- IIS 6.0 benutzt erweiterte Techniken um die Caching-Leistung zu verbessern. Das heißt, dass IIS 6.0 nur die Teile einer Anwendung zwischenspeichert und vorhält, die wirklich gebraucht werden ohne schon beim Initialisieren einer Anwendung den gesamten Inhalt zwischenzuspeichern.
- IIS 6.0 unterstützt nun auch bis 64 GB Arbeitsspeicher, den es für Caching verwenden kann.
- Verschiedene Anwendungen können nun in eigenständigen Prozessen ablaufen, was dazu führt, dass Anwendungen durch einen Ausfall oder Fehler einer anderen Anwendung nicht versagen oder beeinträchtigt werden.

12.2.2 Verbesserte Sicherheit

- IIS 6.0 wird nun standardmäßig im „LockDown"-Modus ausgeliefert. Das heißt, dass IIS 6.0 nach der Installation nur statische Inhalte (.html, .gif) wiedergeben können. Weitere Freigaben muss der Administrator verfügen.
- IIS 6.0 wird standardmäßig als Konto mit sehr niedrigen Privilegien ausgeführt. Dies reduziert den maximal möglichen Schaden drastisch.
- Funktionen in ASP/ASP.NET laufen in einem eigenen Konto mit sehr niedrigen Privilegien ab.
- IIS 6.0 besitzt zahlreiche Verbesserungen im Bereich der SSL-Verschlüsselung. Dazu gehören unter anderem Fernverwaltung der Zertifikate, Steigerung der Leistung und zusätzliche Unterstützung von auf Hardware basierenden Verschlüsselungstechnologien.

12.2.3 Verbesserte Verwaltung

- Die Verwaltungsoberfläche wurde stark verbessert und enthält nun alle Einstellungsmöglichkeiten, um den Anwendungsserver zu konfigurieren.
- Zusätzlich gibt es eine neue Weboberfläche für die Fernwartung.
- Die Administration wird durch die Einführung der XML-METABASE stark vereinfacht, da sämtliche Konfigurationsdaten als XML-Datei vorliegen und nicht mehr umständlich mittels Tools aus einem proprietären Format gelesen werden müssen.
- Die Administration und Veränderung von Applikationseinstellungen kann im laufenden Betrieb erfolgen.
- Unterstützung für automatische Updates, welche jedoch standardmäßig aus Sicherheitsgründen deaktiviert ist.

12.2.4 WMI-Unterstützung

- IIS 6.0 besitzt nun einen eigenen WMI-Anbieter, der es dem Administrator ermöglicht, die Verwaltung auch programmgesteuert abzuwickeln.
- IIS 6.0 bringt bereits einen vorgefertigten Satz an WMI-Skripten mit, die als VB-Scripts vorliegen, abgelegt Windows}System32.

12.2.5 Authentifizierung und Berechtigungsverwaltung

- Standardmäßige Integration der Passport-Technologie.

12.3 Installation des Anwendungsservers

12.3.1 Allgemeines

Um den Anwendungsserver zu installieren gibt es zwei grundlegende Möglichkeiten: die Serververwaltungsanwendung, die standardmäßig immer beim Systemstart angezeigt wird, und die Auswahl „Windows-Komponenten hinzufügen/entfernen".

Da IIS ein mächtiges Programm darstellt, wird Windows Server 2003 immer ohne IIS installiert. Nachfolgend erfahren Sie, wie man die Anwendungsserverrolle unter Windows Server 2003 installiert.

12.3.2 Installation von IIS 6.0 unter Windows Server 2003

So installieren Sie IIS 6.0 unter Windows Server 2003

1. Legen Sie die Setup-CD in das CD-ROM-Laufwerk. Schließen Sie gegebenenfalls das Setup-Startmenü.
2. Öffnen Sie das Fenster SERVERVERWALTUNG, sofern es nicht bereits geöffnet ist. Ansonsten wählen Sie unter START – VERWALTUNG den Menüpunkt SERVERVERWALTUNG.
3. Wählen Sie in der Ansicht den Punkt FUNKTION HINZUFÜGEN ODER ENTFERNEN.
   Es erscheint der Serverkonfigurationsassistent.
4. Wählen Sie den Punkt WEITER.
   Der Assistent analysiert daraufhin das System.
5. Falls Sie diesem Server bei der Installation noch keine Serverrollen zugeordnet haben, müssen Sie sich entscheiden, ob Sie eine vorgeschlagene Standardkonfiguration einrichten oder die Einstellungen und Serverrollen selbst definieren möchten.
6. Wählen Sie in diesem Fall hier die zweite Option BENUTZERDEFINIERTE KONFIGURATION.
7. In der nächsten Ansicht wählen Sie die gewünschte Funktion/Serverrolle aus und bestätigen die Auswahl mit einem Klick auf den Button WEITER. Falls Sie Fragen haben sollten, hilft Ihnen die integrierte Hilfe. Betätigen Sie den entsprechenden Link, rechts von der Auswahlliste. Wählen Sie hier auf jeden Fall den Punkt Anwendungsserver.
8. In der Ansicht ANWENDUNGSSERVEROPTIONEN wählen Sie beide Punkte, also „FrontPage-Erweiterungen" und „ASP.NET aktivieren". Bestätigen Sie mit dem Button WEITER.

© 2005, Microsoft Österreich GmbH

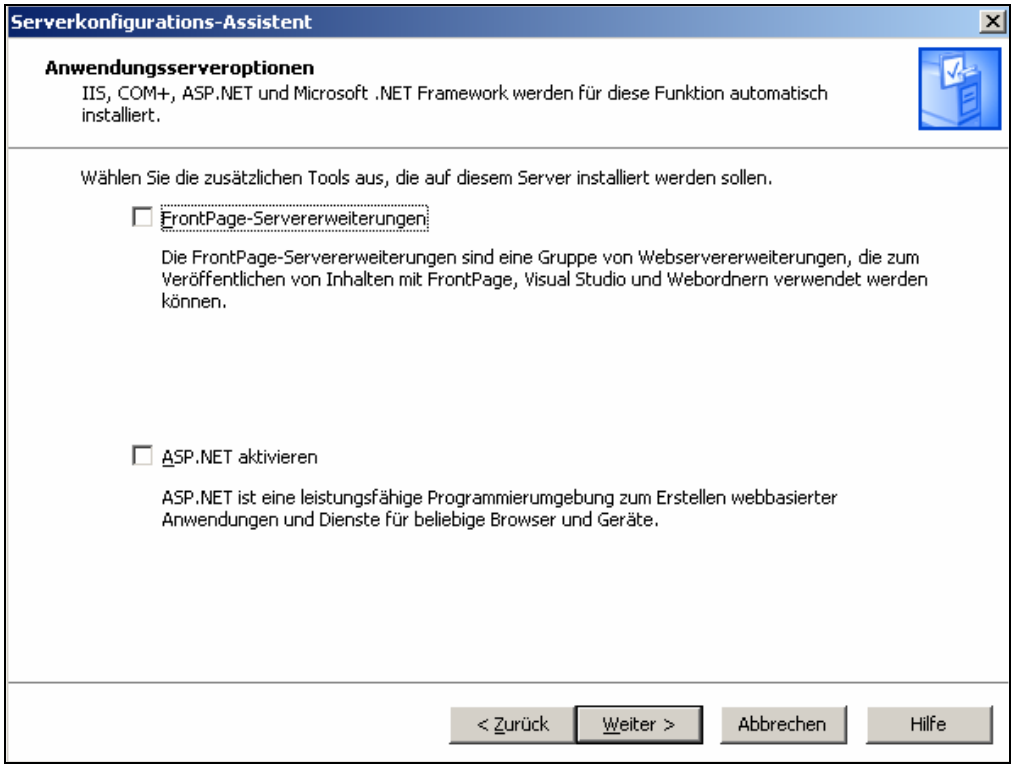


Abb. 166: Serverkonfigurations-Assistent: Anwendungsserveroptionen angeben

9. Auf der nächsten Seite überprüfen Sie nochmals Ihre Einstellungen.
10. Starten Sie die Installation des Anwendungsservers mit einem erneuten Klick auf den Button WEITER.
11. Nach Beendigung der Installation können Sie sich entweder die empfohlenen weiteren Schritte anzeigen lassen oder den Assistenten durch einen Klick auf die Schaltfläche FERTIG STELLEN beenden.

Der Serverkonfigurationsassistent von Windows Server 2003 erstellt automatisch ein Installationsprotokoll, das Sie am Ende in der letzten Ansicht durch einen Klick öffnen können.

Dieselbe Datei „Configure Your Server.log" finden Sie später auch unter WINDOWS/DEBUG.

12.4 Konfigurieren und Verwalten von IIS 6.0

12.4.1 Allgemeines

Zur Konfiguration von IIS 6.0 bietet Windows Server 2003 ebenfalls mehrere Möglichkeiten. In der Ansicht Serververwaltung unter dem Punkt DIESEN ANWENDUNGSSERVER VERWALTEN finden Sie eine spezielle Ansicht der MICROSOFT MANAGEMENT CONSOLE (MMC), die neben der Ansicht des INTERNET INFORMATIONSDIENSTE MANAGERs die Ansicht der .NET KONFIGURATION und die Ansicht der KOMPONENTENDIENSTE bietet.

Falls Sie jedoch ohne Umwege direkt zur Management-Konsole für die Internet-Informations-Dienste gelangen möchten, wählen Sie bitte den entsprechenden Punkt unter START – VERWALTUNG.

12.4.2 Internet-Informationsdienste-Manager:

Die IIS-Konsole bietet Ihnen vielfältige Einstellungs- und Administrationsmöglichkeiten und folgt in seinem Aufbau dem der Konsole der IIS-Versionen 4.0 und 5.0. Hinzugekommen sind die Punkte **Anwendungspools** und **Webdiensterweiterungen**, verschwunden die Punkte **FTP-Sites** und **SMTP**. Diese Punkte erscheinen erst nach der manuellen Installation der entsprechenden Dienste. Die Funktion von SMTP wurde, dem neuen Schema der Serverrollen folgend, in eine eigene Rolle ausgelagert und ist nunmehr ebenfalls in der Serverrolle „Mail Server" enthalten. Es bietet sich an, die Serverrolle „Mail Server" zu installieren, wenn man den SMTP-Dienst benötigt, anstatt ihn einzeln über die Software-Verwaltung zu installieren. Dabei wird neben der reinen SMTP-Funktionalität auch ein POP3-Dienst aufgesetzt und konfiguriert.

Sollte hingegen ein reiner SMTP-Support gewünscht sein, genügt die Installation mittels der erweiterten Funktionen der Softwareverwaltung vollkommen.

12.5 Installation der FTP-Funktionalität

12.5.1 Allgemeines

Da in der Vergangenheit auch die FTP-Funktionalität des IIS ein häufiger Ansatzpunkt für Attacken war, ist auch dieser Dienst standardmäßig nicht installiert.

Um den Dienst nutzen zu können, müssen Sie ihn manuell installieren und konfigurieren. Nachfolgend erfahren Sie, wie Sie die FTP-Funktionalität unter Windows Server 2003 nachinstallieren.

12.5.2 Installation der FTP-Funktionalität unter Windows Server 2003

So installieren Sie die FTP-Funktionalität in Windows Server 2003 nach:

1. Öffnen Sie die Softwareverwaltung über START – SYSTEMSTEUERUNG – SOFTWARE.
2. Wählen Sie den Punkt WINDOWS KOMPONENTEN HINZUFÜGEN/ENTFERNEN.
3. Wählen Sie den Punkt ANWENDUNGSSERVER und klicken Sie auf DETAILS.

© 2005, Microsoft Österreich GmbH

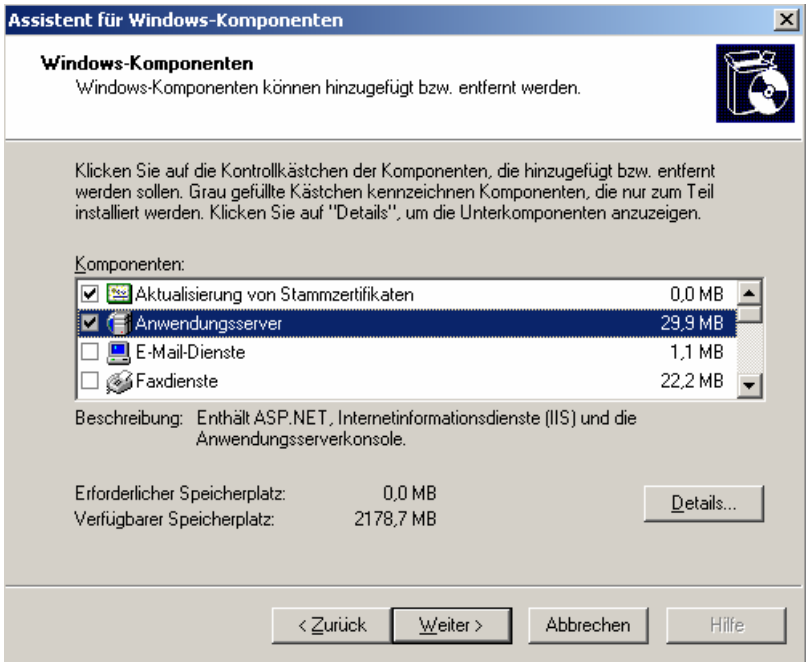


Abb. 167: Windows-Komponenten hinzufügen/entfernen

4. Wählen Sie den Punkt INTERNETINFORMATIONSDIENSTE (IIS) und klicken Sie DETAILS.

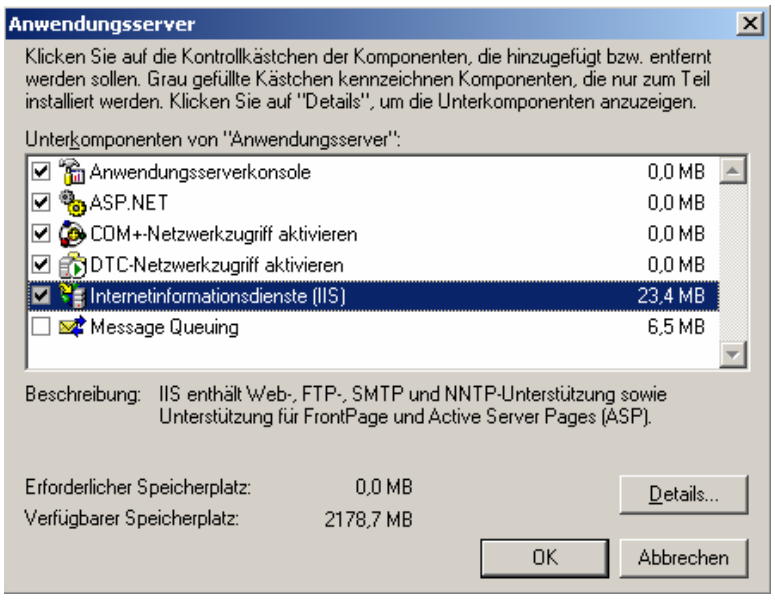


Abb. 168: Assistent für Windows-Komponenten: Anwendungsserver-Optionen

5. Markieren Sie die Checkbox vor dem Punkt FTP-DIENST (FILE TRANSFER PROTOCOL) und klicken Sie auf OK.

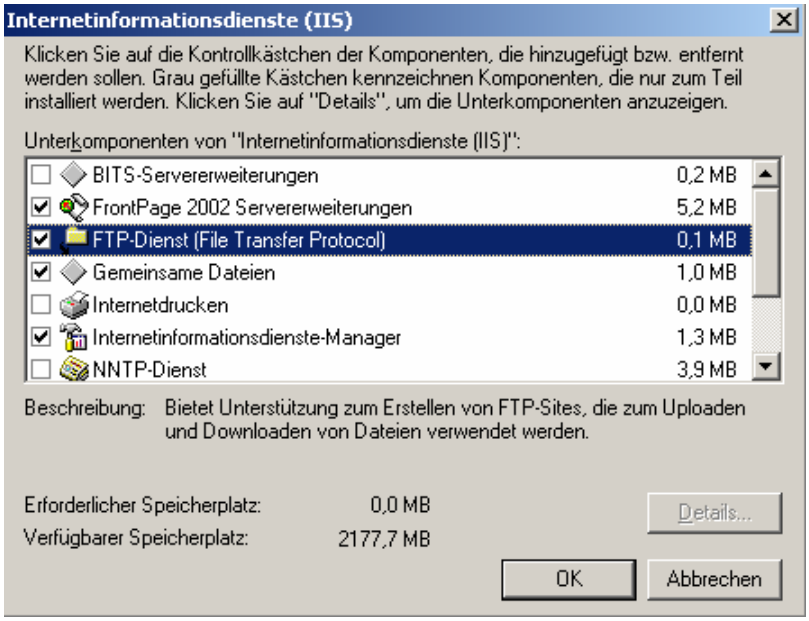


Abb. 169: Assistent für Windows-Komponenten: IIS-Optionen wählen

6. Klicken Sie wieder auf OK.
7. Klicken Sie auf WEITER, die gewählten Komponenten werden installiert.
8. Klicken Sie auf FERTIG STELLEN.

Die Installation des FTP–Diensts ist damit abgeschlossen.

12.6 Installation der SMTP-Funktionalität

12.6.1 Allgemeines

Ebenso wie der WWW- und der FTP–Dienst wird der SMTP-Dienst nicht automatisch installiert. Selbst bei einer Installation von IIS 6.0 mittels der Serververwaltung muss dieser Dienst manuell nachinstalliert werden. Nachfolgender Abschnitt beschreibt die Installation der SMTP-Funktionalität unter Windows Server 2003.

12.6.2 Installation der SMTP-Funktionalität unter Windows Server 2003

So installieren Sie die SMTP-Funktionalität in Windows Server 2003 nach:

1. Öffnen Sie die Softwareverwaltung über START – SYSTEMSTEUERUNG – SOFTWARE.
2. Wählen Sie den Punkt WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN.
3. Wählen Sie den Punkt ANWENDUNGSSERVER und klicken Sie auf DETAILS.

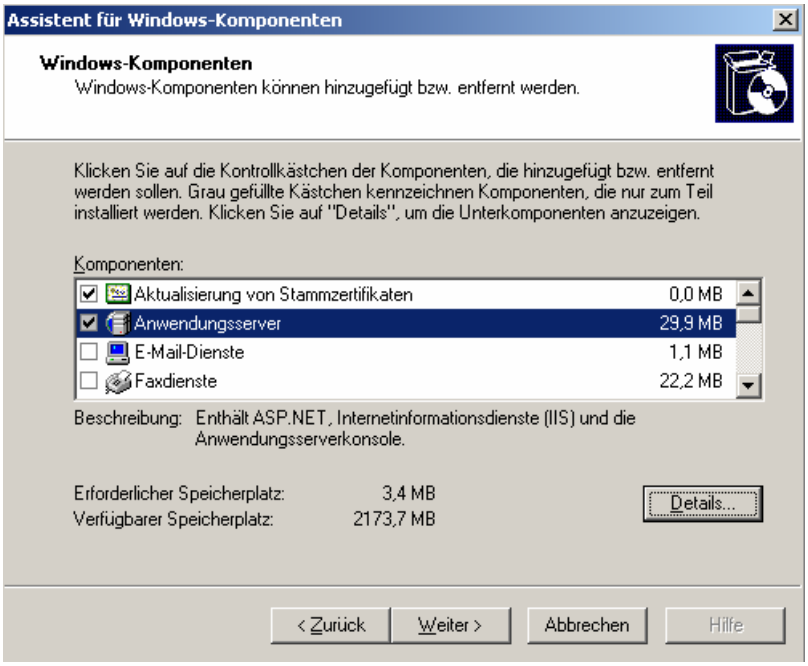


Abb. 170: Assistent für Windows-Komponenten: Anwendungsserver-Optionen

4. Wählen Sie den Punkt INTERNETINFORMATIONSDIENSTE (IIS) und klicken Sie DETAILS.
5. Markieren Sie den die Checkbox vor dem Punkt SMTP-DIENST aus und klicken Sie auf OK.

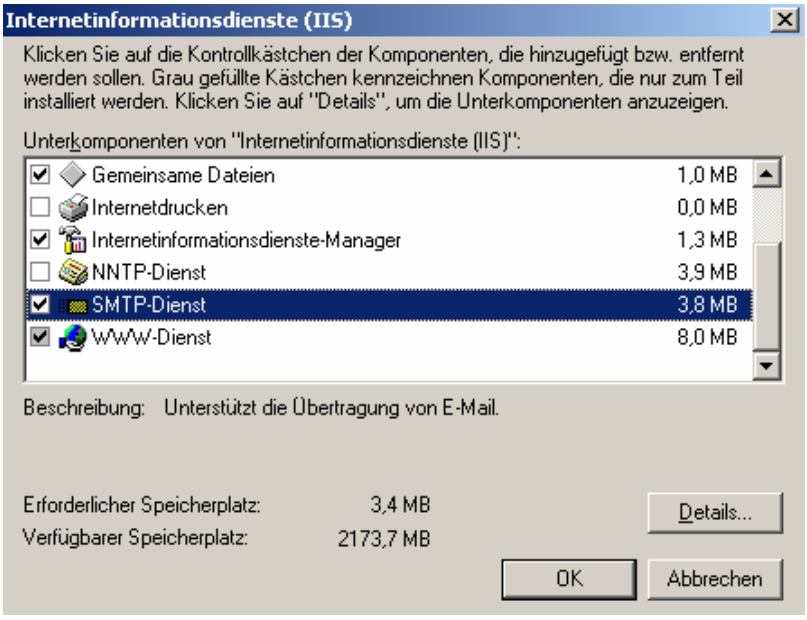


Abb. 171: Assistent für Windows-Komponenten: IIS-Optionen wählen

6. Klicken Sie wieder auf OK.
7. Klicken Sie auf WEITER.

   Die gewählten Komponenten werden installiert.

8. Klicken Sie auf FERTIG STELLEN.

Die Installation des SMTP-Diensts ist damit abgeschlossen.

12.7 Verwaltung des Webservers

12.7.1 Allgemeines

Die Verwaltung des IIS 6.0 erfolgt, wie bereits weiter oben im Kapitel erwähnt, mittels der Windows-Management-Konsole für Internetinformationsdienste, kurz **Internetinformationsdienste-Manager**. Sie erreichen die Anwendung über START – VERWALTUNG – INTERNETINFORMATIONSDIENSTE-MANAGER.

In diesem Abschnitt erfahren Sie, wie Sie Websites und virtuelle Verzeichnisse anlegen und die verschiedenen Einstellungen für Webanwendungen konfigurieren und verwalten.

12.7.2 Unterschied Website – Virtuelles Verzeichnis

Bei der Installation von IIS unter Windows Server 2003 wird automatisch eine Standard-Websitekonfiguration erstellt. Diese Konfiguration kann als Ausgangspunkt für die Bereitstellung von Internetseiten benutzt werden. Sie können Websites aber auch selbst definieren.

Der wesentliche Unterschied zwischen Website und virtuellem Verzeichnis liegt im Einsatzgebiet beziehungsweise in der Handhabung.

Prinzipiell existiert ein virtuelles Verzeichnis immer unterhalb einer Website. Ein virtuelles Verzeichnis ist ein angezeigter Name oder Alias entweder für ein physikalisches Verzeichnis auf der Festplatte Ihres Servers, das sich nicht im Basisverzeichnis befindet, oder für das Basisverzeichnis auf einem anderen Computer. Da der Alias normalerweise kürzer ist als der Pfadname des physikalischen Verzeichnisses, ist die Eingabe für die Benutzer einfacher. Die Verwendung von Aliasnamen erhöht darüber hinaus die Sicherheit, da Benutzer den physikalischen Speicherort der Dateien auf dem Server nicht kennen und die Dateien somit nicht ändern können. Darüber hinaus erleichtern Aliasnamen das Verschieben von Verzeichnissen auf der Site. Anstatt den URL für das Verzeichnis zu ändern, genügt es, die Zuordnung zwischen dem Alias und dem physikalischen Speicherort des Verzeichnisses zu ändern.

Wenn Ihre Website Dateien enthält, die sich in einem anderen Verzeichnis als dem Basisverzeichnis oder auf anderen Computern befinden, ist es erforderlich, dass Sie virtuelle Verzeichnisse erstellen, um diese Dateien in Ihre Website aufzunehmen.

So könnten Sie zum Beispiel Inhalte der Website aus verschiedenen Quellen zu einem gesamten Portal vereinen.

Physikalischer Speicherort	Alias	URL
D:\Inetpub\wwwroot	*Basisverzeichnis*	http://intranet
D:\Inetpub\wwwroot\Schüler	Schueler	http://intranet/Schueler
V:\Personal\Share	Lehrer	http://intranet/Lehrer
S:\Sport\Archiv	Sport	http://intranet/Sport

Das Basisverzeichnis der Website bezeichnet den physikalischen Ordner, in dem der Inhalt als Daten gespeichert wird. Standardmäßig wird dazu ein Verzeichnis **\Inetpub\Wwwroot** erstellt.

Im Gegensatz zum virtuellen Verzeichnis bietet die Website unter anderem die Möglichkeit, so genannte Hostheader zu verwenden und so mehrere Webseiten unter einer IP-Adresse zu betreiben.

12.7.3 Mehrere Websites unter einer IP-Adresse betreiben

Häufig verlangen die Anforderungen den Betrieb mehrere Websites auf einem Server mit nur einer verfügbaren IP-Adresse. Damit das reibungslos funktioniert, stehen folgende Möglichkeiten zur Verfügung:

Unterscheidung mittels Hostheader-Namen

Alle Websites verfügen über einen beschreibenden Namen und können einen oder mehrere Hostheadernamen unterstützen. Organisationen, die mehrere Websites auf einem einzigen Server hosten, verwenden häufig Hostheader, da sie mit dieser Methode mehrere Websiteidentitäten erstellen können, ohne eine eindeutige IP-Adresse (Internetprotokoll) für jede Site zu verwenden.

Beim Betrieb von mehreren Websites unter einer IP-Adresse ist die Verwendung von Hostheadern ratsam.

Da der WWW-Publishingdienst (WWW-Dienst) einen nicht ausgelagerten Poolspeicher zum Verwalten eines Endpunkts für jede IP-Adresse zuweisen muss, besteht ein Vorteil der Verwendung von Hostheadern darin, die mögliche Beeinträchtigung der Systemleistung zu verhindern, die mit der Identifizierung mehrerer Websites durch eindeutige IP-Adressen einhergeht.

Wenn beim Server eine Clientanforderung eingeht, verwenden die Internetinformationsdienste (Internet Information Services oder IIS) den Hostnamen, der im HTTP-Request (Hypertext Transfer Protocol) übergeben wird, um zu bestimmen, welche Siteclients die Anforderung stellen. Wenn die Site in einem privaten Netzwerk verwendet wird, kann es sich beim Hostheader um einen Intranetsitenamen handeln, z. B. **Intranet**. Wenn die Site im Internet verwendet wird, muss es sich beim Hostheader um einen öffentlich zugänglichen DNS-Namen (Domain Name System) handeln, wie z. B. **extranet.meineschule.at**. Registrieren Sie den Namen bei einer autorisierten Internetnamenstelle.

Um Hostheader verwenden zu können, benötigen Sie eine funktionierende Domänen-Namensauflösung (DNS).

Unterscheidung mittels Portnummern

Da der Port 80 der Standardport für HTTP ist, wird üblicherweise immer die Standardwebsite unter diesem Port betrieben. Bei Verwendung der Portnummer 80 bei Anwahl einer Website ist eine explizite Angabe derselbigen durch den Benutzer nicht notwendig.

Es besteht jedoch auch die Möglichkeit, mehrere Website mittels verschiedener Portnummern auf einem Server zu unterscheiden und so unter einer IP-Adresse mehrere Webseiten zu hosten. Dabei werden den einzelnen Websites unterschiedliche Portnummern zugeordnet, die beim Aufruf der Website angegeben werden müssen.

Angenommen, die Standardwebseite ist unter http://www.meineschule.at zu erreichen, so könnte man unter http://www.meineschule.at:1024 eine eigene Präsenz bereitstellen.

Portnummern unter 1023 sollten nicht verwendet werden, da viele dieser Ports bereits für spezielle Dienste reserviert sind. Durch die Wahl einer Portnummer größer als 1023 lassen sich Konflikte vermeiden.

Das Verwenden von unterschiedlichen Portnummern auf einer IP-Adresse kann zu einem erhöhten Ressourcenbedarf seitens des Webservers führen.

12.7.4 Anlegen einer neuen Website

So erstellen Sie eine neue Website:

1. Öffnen Sie den Internetinformationsdienste-Manager.
2. Erweitern Sie den Punkt Servername, wobei Servername der Name des Servers ist.
3. Erweitern Sie den Punkt Websites. Es erscheinen die derzeit installierten Websites, jeweils als eigener Unterordner.

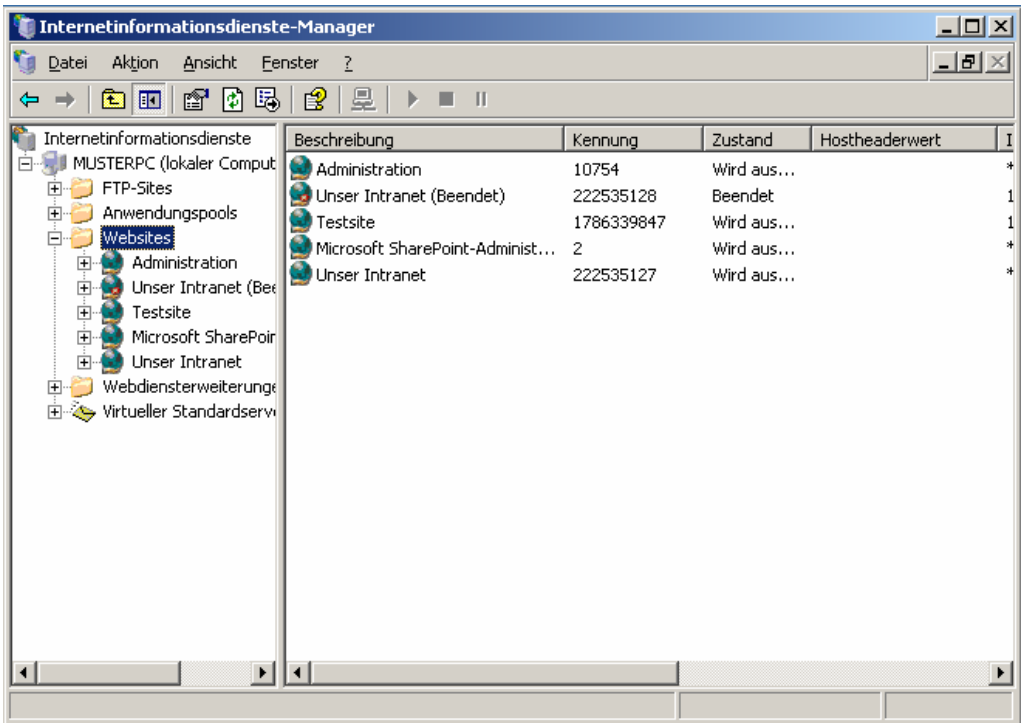


Abb. 172: IIS-Manager: Hauptansicht

4. Klicken Sie mit der rechten Maustaste auf den Punkt Websites und wählen Sie den Punkt NEU → WEBSITE...
5. Im Assistenten für neue Website klicken Sie auf WEITER.
6. Geben Sie nun eine Beschreibung für Ihre Website ein, z. B.: „Unser Intranet“. Diese Beschreibung hat keinerlei Auswirkung auf die korrekte Funktion, sondern erleichtert lediglich die Verwaltung mehrere Websites.

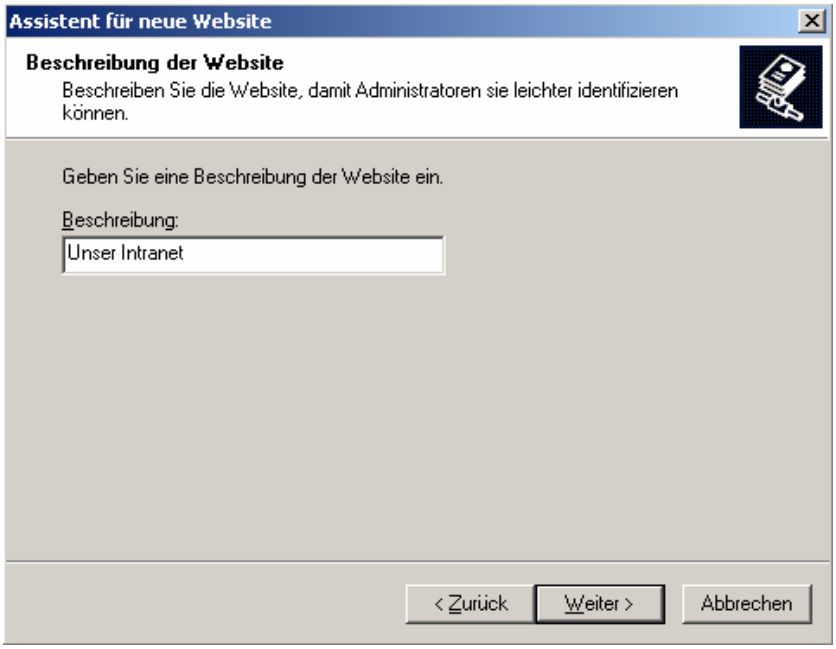


Abb. 173: Assistent für neue Website: Angabe der Beschreibung

7. In der nächsten Ansicht können Sie die Website an eine fixe IP-Adresse binden, über welche die Site im Webbrowser aufgerufen werden kann.

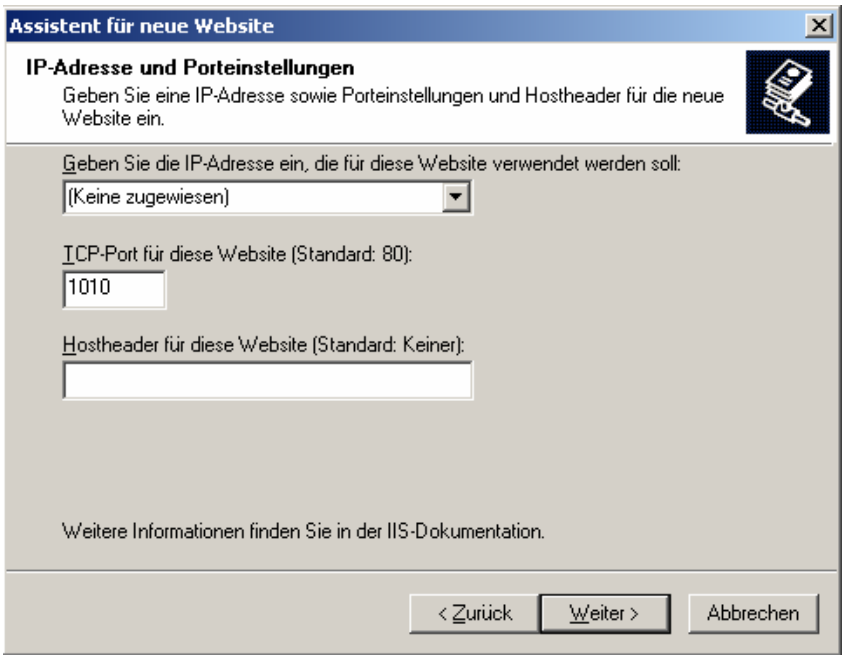


Abb. 174: Angabe der gebundenen IP-Adresse und des Ports

8. Des Weiteren können Sie einen Hostheader oder eine Portnummer angeben, unter der die Website erreichbar ist. Standardmäßig ist der Port 80 für die Standardseite reserviert. Klicken Sie auf WEITER.

9. Geben Sie nun den Pfad zum physischen Verzeichnis auf Ihrer Festplatte an. Wählen Sie gegebenenfalls mittels der Schaltfläche DURCHSUCHEN ein Verzeichnis aus. Wählen Sie hier ein geeignetes Verzeichnis aus.

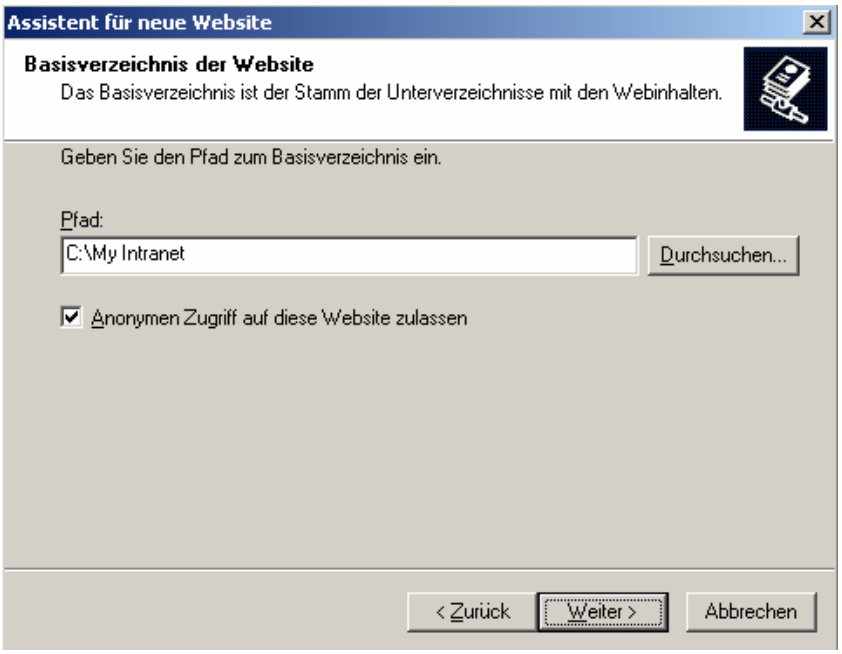


Abb. 175: Angabe des physikalischen Pfades

Standardmäßig werden Websites im Ordner C:\Inetpub\wwwroot\ gespeichert. Jedoch ist es durchaus möglich, jedes andere lokale aber auch vernetzte Laufwerk zu wählen.

Es empfiehlt sich, das Basisverzeichnis für die Websites auf einer eigenen Partition abzulegen. Aus Sicherheitsgründen sollte man auf jeden Fall vermeiden, die Systempartition für das Anlegen des Basisverzeichnisses zu verwenden.

10. Wählen Sie, ob Sie den anonymen Zugriff auf Ihre Seite zulassen wollen. Wenn Sie diese, standardmäßig aktivierte, Option wählen, erfolgt jeder Zugriff auf diese Website unter einem eigenen, speziellen Account mit sehr niedrigen Privilegien. Wenn Sie diese Option deaktivieren, können Sie in der weiteren Folge festlegen, welche Mitglieder einer Domäne Zugriff auf diese Website haben. Belassen Sie diese Option jetzt aktiviert.
11. Im nächsten Punkt wählen Sie die entsprechenden Berechtigungen, die beim Ausführen der Website zulässig sind. Für die meisten Anwendungen reichen die standardmäßigen Einstellungen vollkommen, „Lesen" und „Skripts ausführen". Belassen Sie die gewählte Option auf der Standardeinstellung und wählen Sie WEITER.

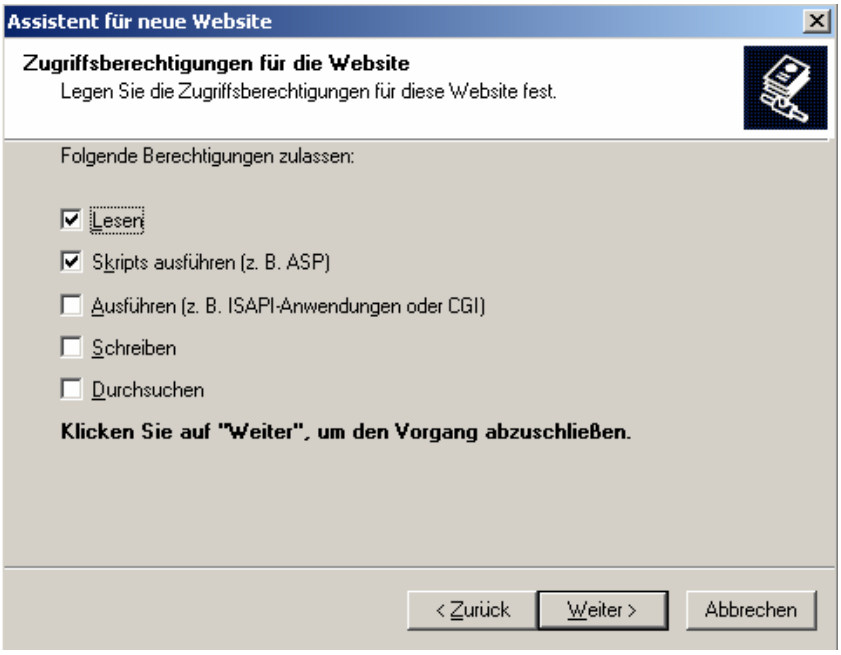


Abb. 176: Assistent für neue Website: Angabe der Zugriffsberechtigungen

12. Der Assistent erstellt das gewünschte virtuelle Verzeichnis und richtet die Website ein.
13. Klicken Sie auf FERTIG STELLEN.

Die Einrichtung des virtuellen Verzeichnisses ist abgeschlossen.

12.7.5 Entfernen einer Website

So entfernen Sie ein bestehendes virtuelles Verzeichnis:

1. Öffnen Sie den Internetinformationsdienste-Manager.
2. Erweitern Sie den Punkt Servername, wobei Servername der Name des Servers ist.
3. Erweitern Sie den Punkt Websites. Es erscheinen die derzeit installierten Websites jeweils als eigener Unterordner.
4. Wählen Sie das zu löschende Verzeichnis, in diesem Beispiel das Verzeichnis „Standardwebsite“.
5. Klicken Sie rechts und wählen Sie aus dem Kontextmenü den Punkt LÖSCHEN.

© 2005, Microsoft Österreich GmbH

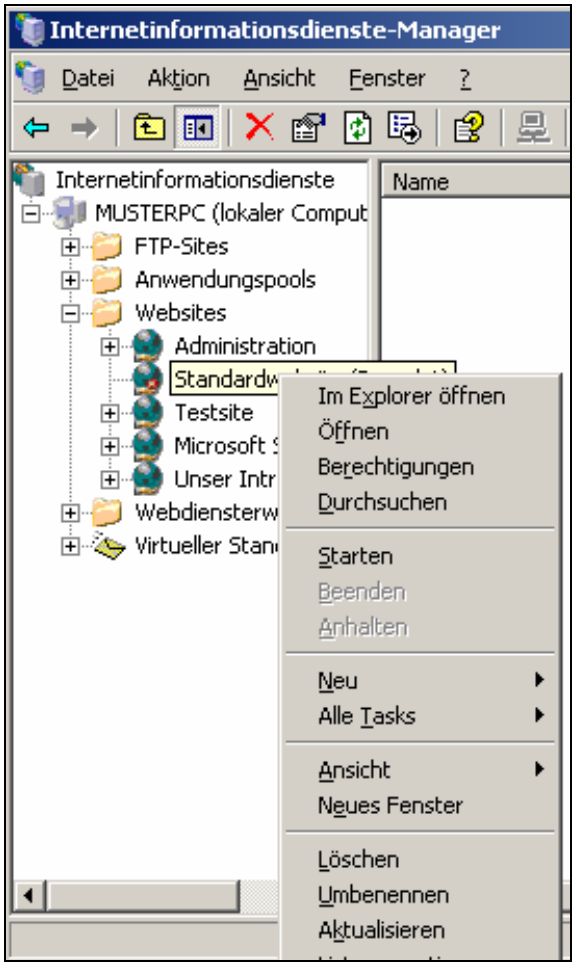


Abb. 177: IIS Manager: Ansicht Kontextmenü „Website“

6. Beantworten Sie die Frage mit JA, das Verzeichnis wird gelöscht.

Das Löschen einer Website oder eines virtuellen Verzeichnisses führt NICHT zur Löschung der physischen Dateien. Lediglich aus der XML-METABASE werden die Einstellungen des virtuellen Verzeichnisses gelöscht. Unter anderem werden die verwendeten Ports wieder freigegeben und können anderweitig verwendet werden.

Die Dateien können Sie mittels des Windows Explorers physisch löschen.

12.7.6 Ändern der Einstellungen einer Website

So ändern Sie die Einstellung eines virtuellen Verzeichnisses:

1. Öffnen Sie den Internetinformationsdienste-Manager
2. Erweitern Sie den Punkt Servername, wobei Servername der Name des Servers ist.
3. Erweitern Sie den Punkt Websites. Es erscheinen die derzeit installierten Websites, jeweils als eigener Unterordner.
4. Klicken Sie mit der rechten Maustaste auf die zu ändernde Website und wählen Sie den Punkt „Eigenschaften“ aus dem Kontextmenü.
5. Ändern Sie die entsprechenden Einstellungen und klicken Sie ÜBERNEHMEN.

Die Einstellungen werden gespeichert.

12.8 Eigenschaften einer Website

12.8.1 Allgemeines

Die Ansicht EIGENSCHAFTEN EINER WEBSITE bietet vielfältige Einstellungsmöglichkeiten, um den Anforderungen moderner Webanwendungen gerecht zu werden.

Wie Sie zu den Einstellungen einer Website gelangen, erfahren Sie weiter oben im Kapitel. Die Ansicht „Eigenschaften von ...“ bietet folgende Punkte, wovon hier die wichtigsten erläutert werden:

12.8.2 Website

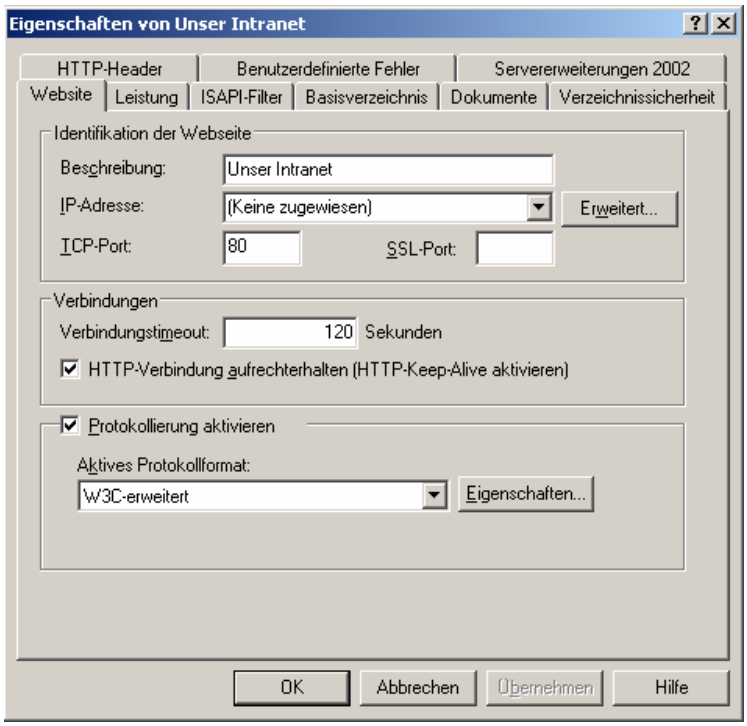


Abb. 178: Eigenschaften von Website: Ansicht „Website"

Einstellung	Bedeutung
Beschreibung	Hier können Sie eine Beschreibung der Website eingeben, die lediglich die Verwaltung vieler Websites erleichtert. Die Vergabe einer Beschreibung hat keinerlei Auswirkungen auf die Funktion der Website.
IP-Adresse	Sie können die Website an eine IP-Adresse oder auch an mehrere IP-Adressen binden. Dies ermöglicht die Anzeige der Website durch Eingabe der IP-Adresse im Adressfeld eines Internetbrowsers. Da spezielle Webserver mehrere Netzwerkverbindungen besitzen, ist die Angabe einer IP-Adresse in diesen Fällen notwendig, um zu definieren, welche Anwendung auf welcher IP-Adresse angeboten wird. Wenn keine Auswahl der IP-Adresse stattfindet, wird die Standardadresse gewählt, meistens die Adresse der ersten eingerichteten Netzwerkverbindung.
TCP-Port	Durch Angabe einer Portnummer ist es möglich, unter derselben IP-Adresse mehrere verschiedene Anwendungen zu hosten. Der Aufruf der einzelnen Anwendungen erfolgt dann mittels der Notation http://<Servername>:<Port>
Erweitert	Wenn Sie diese Option wählen, gelangen Sie in ein Untermenü. Darin können Sie unter anderem Hostheader-Einträge definieren beziehungsweise ändern.
Verbindungs-Timeout	Gibt die Zeit in Sekunden an, die der Server auf eine Antwort vom Client wartet, bevor er die Verbindung wieder für andere Clients freigibt. In diesem Zusammenhang ist darauf zu achten,

	dass ein geringeres Timeout die maximal mögliche Anzahl an gleichzeitigen Verbindungen nicht erhöht, jedoch zu einer schnellen Abarbeitung der Anfragen führt. Ein zu geringes Timeout kann jedoch zu unerwünschten Verbindungsabbrüchen führen.
Protokollierung aktivieren	Diese Option ermöglicht die Protokollierung aller Anfragen an den Server und aller Antworten desselben. Über die Auswahlliste können Sie das gewünschte Format wählen und dessen Eigenschaften bei Bedarf noch genauer einstellen. Die Protokolldateien befinden sich standardmäßig im Verzeichnis C:\Windows\System32\Logfiles

12.8.3 Leistung

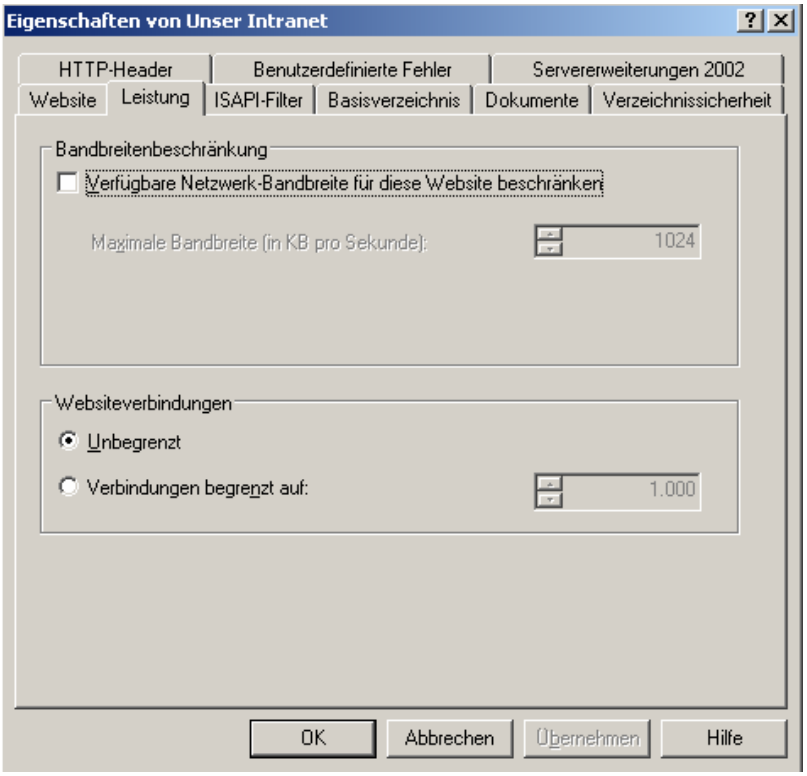


Abb. 179: Eigenschaften von Website: Ansicht „Leistung"

Einstellung	Bedeutung
Breitbandbeschränkung	Mit Hilfe dieser Option können Sie die zur Verfügung stehende Bandbreite der Netzwerkverbindung für die jeweilige Website einschränken. Damit können Sie größeren Websites auf Ihrem Server mehr Bandbreite zusprechen als kleineren. Standardmäßig findet keine Begrenzung statt.
Websiteverbindungen	Hier können Sie die maximale Anzahl an gleichzeitigen Verbindungen angeben. Standardmäßig setzt hier lediglich die Hardwareausstattung Ihres Servers die Grenzen.

12.8.4 Basisverzeichnis

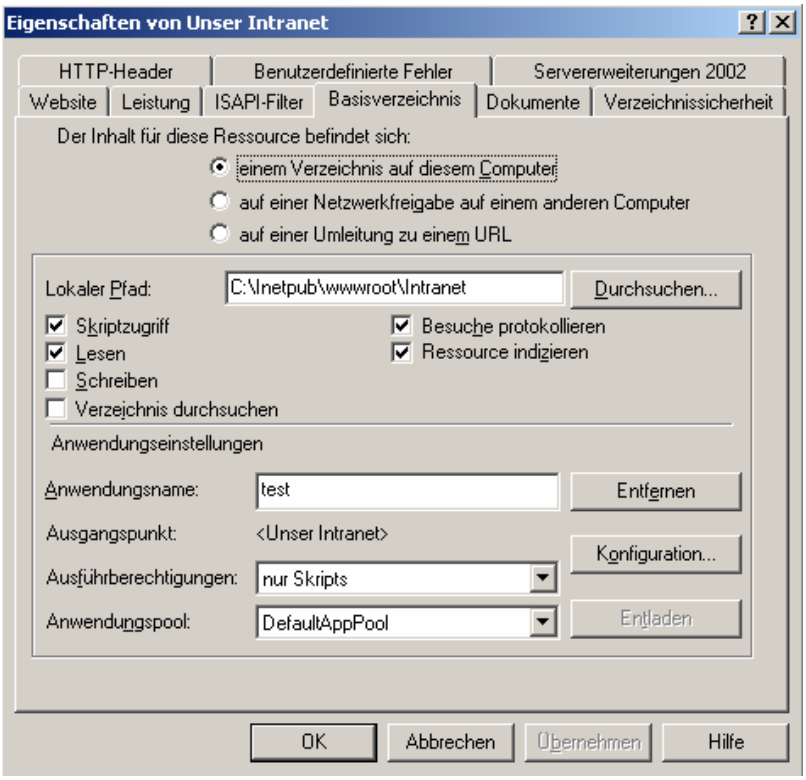


Abb. 180: Eigenschaften von Website: Ansicht „Basisverzeichnis“

Einstellung	Bedeutung
Herkunft des Inhalts	Mit Hilfe dieser Option können Sie festlegen, woher der Inhalt der Website stammt. Standardmäßig ist hier die Option „einem Verzeichnis auf diesem Computer" gewählt. Die beiden anderen Einstellungen erlauben entweder die Angabe eines Netzlaufwerks oder die Angabe einer Weiterleitung. Dabei wird der Aufruf der Site A auf die angegebene Website weitergeleitet und diese dem Client zurückgegeben.
Lokaler Pfad	Bezeichnet das physische Verzeichnis der Anwendungsdateien, die auf der Website angezeigt werden sollen.
Berechtigungen	Mit Hilfe der Checkboxen können Sie wählen, welche Rechte die Anwendung unterstützt beziehungsweise welche Rechte der Client beim Zugriff auf die jeweilige Site hat. 1 „Skriptzugriff" erlaubt die Ausführung von serverseitigem Code, wie er etwa von ASP.NET- und ASP-Anwendungen benutzt wird. 2 „Lesen" erlaubt die Anzeige statischer Inhalte. Ohne diese Option ist auch kein Skriptzugriff möglich. 3 „Schreiben" erlaubt das Schreiben von Daten auf dem Server, wie es etwa beim Upload von Bildern notwendig ist. 4 „Verzeichnis durchsuchen" ermöglicht die Anzeige des Verzeichnisinhalts. einer Site, die keine entsprechenden Startseiten (index.htm, index.aspx) hat
Anwendungsname	Hier können Sie einen Namen für die Anwendung definieren, unter dem die Anwendung im Internet sichtbar ist. So führt ein Aufruf der Adresse http://<Servername>/<Anwendungsname> durch einen Browser zur Anzeige der konfigurierten Site auf dem Server.
Ausführungs-berechtigung	Mittels diese Option legen Sie fest, ob und, wenn ja, welche nichtstatischen Dateien ausgeführt werden. Die Einstellung „Keine" führt dazu, dass keinerlei Inhalte außer statischem HTML und Bildern ausgeführt werden, selbst wenn die Anwendung serverseitige Skripte enthält. Die Einstellung „Skripts und ausführbare Dateien" hingegen kann ein Sicherheitsrisiko darstellen, da eventuell bösartiger Code zur Ausführung gelangt.
Anwendungspool	Hier können Sie einen der eingerichteten Anwendungspools wählen, zu welchem Ihre Applikation hinzugefügt wird.

13 Anhang B – Kontingentverwaltung

13.1 Allgemeines

Damit der von den Benutzern verwendete Speicherplatz eingegrenzt werden kann, stellt Windows Server 2003 in den Eigenschaften eines Datenträgers eine Kontingentverwaltung zur Verfügung.

Wenn Sie die Kontingentverwaltung aktivieren, gilt dies nicht für die bereits erstellten Benutzer, sondern erst für die nachfolgenden. Beachten Sie zudem, dass die Kontingentverwaltung sich negativ auf die Systemleistung auswirken kann.

Sie können die Kontingentverwaltung aber auch vorübergehend aktivieren, um den Speicherplatz zu überprüfen, den bestimmte Benutzer verwenden. Zudem erleichtert es die Besitzübernahme und das Verschieben von Benutzerdateien

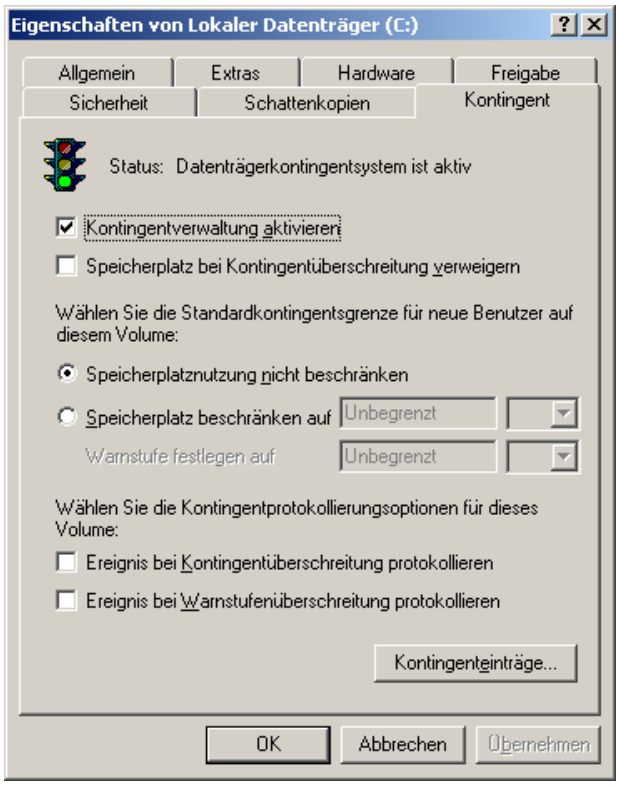


Abb. 181: Aktivieren der Kontingentverwaltung

13.2 Aktivieren der Kontingentverwaltung

So aktivieren Sie die Kontingentverwaltung:

1. Öffnen Sie den Windows Explorer und wählen Sie einen Datenträger aus.
2. Wählen Sie aus dem Kontextmenü den Befehl EIGENSCHAFTEN.
3. Klicken Sie auf das Register KONTINGENT.

Die Ampel spiegelt den aktuellen Stand der Kontingentverwaltung wider.
Rot: Die Kontingentverwaltung ist deaktiviert.
Orange: Die Statistiken zur Datenträgerverwendung werden gesammelt.
Grün: Das Datenträgerkontingentsystem ist aktiviert.

4. Markieren Sie das Kontrollkästchen bei KONTINGENTVERWALTUNG AKTIVIEREN.
5. Klicken Sie auf ÜBERNEHMEN.

   Daraufhin werden die Statistiken gesammelt. Sie können nun mit dem Befehl KONTINGENTEINTRÄGE die Begrenzungen der einzelnen Benutzer setzen.
6. Klicken Sie auf OK.

Wenn Sie einen Kontingenteintrag eines Benutzers löschen, werden sämtliche Dateien und Ordner angezeigt, die sich in dessen Besitz befinden. Sie haben die Möglichkeit, diese Dateien zu verschieben, zu löschen bzw. den Besitz dieser Elemente zu übernehmen.

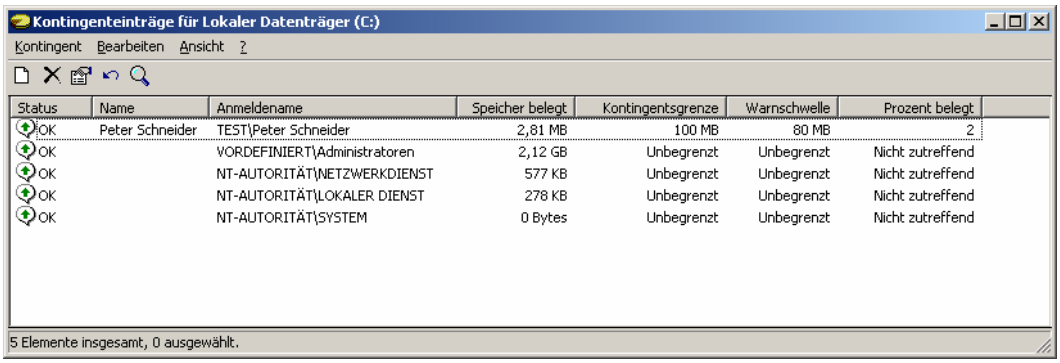


Abb. 182: Die Kontingenteinträge

Aufgrund der günstigen Plattenpreise wird die Kontingentverwaltung immer weniger eingesetzt.
Weitere Informationen zur Kontingentverwaltung finden Sie im Kapitel Dateiserver.

14 Anhang C - Remote Installation Services (RIS)

Ein solches Hilfsmittel steht Ihnen unter Windows Server 2003 in Form der **Remote Installation Services**, kurz **RIS** genannt, zur Verfügung.

RIS erlaubt Ihnen die Erstellung eines Clientrechner-Images und dessen Verteilung von einer zentralen Stelle aus, dem **RIS-Serverdienst** (auch Image-basierte Installation genannt).

Neben der Verteilung der Betriebssysteme bietet Ihnen der RIS-Serverdienst auch die Möglichkeit, andere Programme und Anwendungen zentral bereitzustellen.

Mit RIS ist - unter Verwendung von Risetup.exe - auch eine CD-basierte Installation durchführbar. Damit wird am Client nur das entsprechende Betriebssystem (W2K-WS, XP, W2K3), gemäß eines am Server vorliegendem Antwortfile und den ebenfalls dort liegenden Dateien der Workstation-CD, installiert.

14.1 Voraussetzungen

Um die Remote Installation Services unter Windows Server 2003 installieren zu können, müssen folgende Voraussetzungen erfüllt sein:

- Vorhandene Domäne mit installiertem Active Directory
- Konfigurierte DNS-Installation
- Konfigurierte DHCP-Installation
- Eigene NTFS-Partition für RIS

14.2 Installation des RIS-Serverdiensts

Um RIS nutzen zu können, benötigen Sie eine zentrale Stelle für die Verteilung der Image-Dateien an die Clientrechner.

Hierzu ist es notwendig, den RIS-Serverdienst auf Windows Server 2003 zu installieren. Die Installation des Serverdiensts erfolgt hierbei ausschließlich über die Ansicht „Software" der Systemsteuerung. Es steht hierbei kein Server-Verwaltungs-Assistent zur Verfügung.

Eine detaillierte Anleitung zur Installation des RIS-Servers finden Sie im nachfolgenden LAB.

14.3 Aufsetzen eines Clientrechners mittels RIS

Der Aufwand für das Aufsetzen des Clients reduziert sich mittels des RIS-Serverdiensts erheblich. Die Clientrechner müssen lediglich mittels einer Netzwerk-Bootdisk gestartet werden und sich zum RIS-Server verbinden können.

© 2005, Microsoft Österreich GmbH

Daraufhin startet automatisch ein unabhängiges Setup das Kopieren des hinterlegten Images. Die Aktionen des Benutzers reduzieren sich hierbei auf die Eingabe des Administrator Passworts, eventuell die Auswahl der Domäne und die Auswahl des Images, das kopiert werden soll.

Nach Abschluss des Kopiervorgangs wird noch ein Mini-Setup gestartet, das seine Einstellungen aus der hinterlegten Antwortdatei bezieht.

Je nach Umfang der installierten Produkte kann dieser Vorgang einige Zeit in Anspruch nehmen. Nachdem einem Neustart des Clientrechners ist er fertig installiert. Je nach Umfang der Vorbereitungen und hinterlegten Einstellungen ist der Client von diesem Zeitpunkt an eventuell auch bereits voll einsatzbereit.

14.4 Zusätzliche Aktionen

Um die Remote-Installation soweit wie möglich selbständig ablaufen zu lassen, ist es im Laufe der Imageerstellung notwenig, eine Antwortdatei zu erstellen beziehungsweise zur Verfügung zu stellen, die sämtliche Angaben für die im Setup abgefragten Einstellungen enthält.

Normalerweise wird diese Antwortdatei während des Mini-Setups auf dem Clientrechner erstellt. Sie können jedoch diese Datei an spezielle Bedürfnisse anpassen.

Nähere Informationen zu den Remote Installation Services und zur Antwortdatei finden Sie im Hilfe & Support-Center.