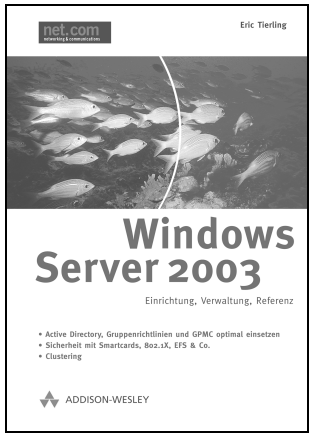
Small Business Server 2003

net.com
networking & communications

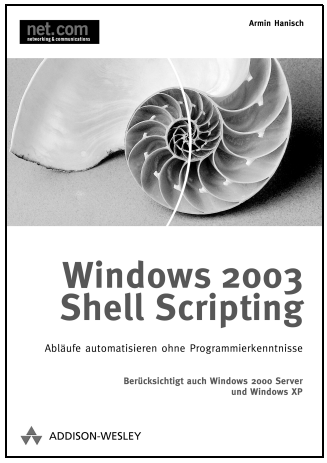
Netzwerke, Betriebssysteme, Sicherheit ... hierzu bietet Ihnen die Reihe net.com umfassende, praxisnahe Information. Neben Fragen der Systemverwaltung greift sie auch Themen wie Protokolle, Technologien und Tools auf. Profitieren Sie bei Ihrer täglichen Arbeit vom Praxiswissen unserer erfahrenen Autoren.



Windows Server 2003

Eric Tierling
1312 Seiten, € 59,95 [D]
ISBN 3-8273-2076-3

Ausführlich widmet sich dieses Buch allen wesentlichen Aspekten von Windows Server 2003 und all seiner Editionen. Active Directory, Gruppenrichtlinien, Windows NT-Domänenupgrade, TCP/IP-Dienste und Sicherheitsmerkmale sind detailliert beschrieben, um Unternehmen einen optimalen Einsatz zu ermöglichen. Clustering mit Netzwerklastenausgleich und Clusterdienst, E-Mail-Server, Group Policy Management Console, Terminaldienste, Remotedesktop und Webverwaltung, Volumen-Schattenkopie sowie die Smartcard-Integration und sichere Wireless-LAN-Unterstützung stellen weitere Highlights dieses Buches dar.



Windows 2003 Shell Scripting

Armin Hanisch
288 Seiten, € 29,95 [D]
ISBN 3-8273-2178-6

Sparen Sie durch den Einsatz von Shell-Skripten Zeit und Geld sparen. Nach einer kurzen Einführung ins Thema, erläutert der Autor anhand verschiedener Aufgabenstellungen aus der Administratorpraxis die Möglichkeiten der Windows Shell. Neben sofort einsetzbaren Batches erhält der Leser auch das notwendige Wissen, um auftretende Probleme selbstständig zu lösen. In den fortgeschrittenen Kapiteln wird Ihnen der Einsatz von komplexen Skripten gezeigt und welche Automatisierungstools für welchen Zweck am besten geeignet sind.

PEARSON Education

ADDISON-WESLEY

Stephanie Knecht-Thurmann

Small Business Server 2003

Das Integrationshandbuch für kleine und mittlere Unternehmen

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

10 9 8 7 6 5 4 3 2 1

07 06 05

ISBN 3-8273-2213-8

ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Einbandgestaltung: atelier für gestaltung, niesner & huber, Wuppertal
Lektorat: Sylvia Hasselbach, shasselbach@pearson.de
Korrektorat: Sandra Gottmann, Münster
Herstellung: Claudia Bäurle, cbaeurle@pearson.de
Satz: mediaService, Siegen, www.media-service.tv
Druck und Verarbeitung: Bercker, Kevelaer
Printed in Germany

Inhaltsverzeichnis

Vorwort

Auch für kleinere und mittlere Unternehmen mit Blick auf den expandierenden Mittelstand nimmt die Bedeutung einer funktionsfähigen und leicht zu administrierenden IT-Basis stark zu. Als Betriebssystem-Plattform bietet sich hier der Small Business Server 2003 an. Er vereinigt die essenziell wichtigen Applikationen, das Betriebssystem Windows Server 2003, den Mailserver Exchange in der aktuellen Fassung, die SharePoint Services für die Zusammenarbeit im Team sowie ggf. den Internet Security and Acceleration Server (ISA) und die leistungsfähige Datenbank MS SQL Server 2000 in einem Paket zu einem sehr attraktiven Preis-Leistungs-Verhältnis. Die Beschränkung auf einen Standort ist für kleinere Unternehmen kein Nachteil, sondern vereinfacht die Administration. Auf die Unterschiede der Lizenzierungen und die Möglichkeiten der Updates gehen wir in diesem Buch ein.

Dieses Buch soll den Leser in die Lage versetzen, einen Small Business Server mit all seinen Bestandteilen zu planen, installieren, konfigurieren und betreiben. Da dieses Buch keine Einführung in die Bedienung eines Betriebssystems sein kann, richtet es sich in erster Linie an Leser, die über praktische Vorkenntnisse in Windows NT, 2000, XP oder Windows Server 2003 verfügen. An einigen Stellen sei für spezielle Informationen auf die Bücher Windows 2003 Server (Referenz) von Eric Tierling und mein Buch zum Thema Active Directory verwiesen, die ebenfalls in diesem Verlag erschienen sind.

An dieser Stelle möchte ich mich erneut bei meiner Lektorin Frau Hasselbach für die gute Zusammenarbeit bedanken. Auch meinem Ehemann danke ich für seine Ideen, seine kompetente und konstruktive Kritik und sein Verständnis. Torsten Hoge (IBM-Hannover) für seine Tipps und Unterstützung in Hardware-Fragen sei ebenfalls an dieser Stelle erwähnt. Danke auch Ihnen, liebe Leserin, lieber Leser. Sie werden hoffentlich viel Nutzen aus diesem Buch ziehen.

Barsinghausen im November 2004

Stephanie Knecht-Thurman

1 Der Small Business Server 2003 stellt sich vor

Dieses Kapitel gibt Ihnen einen kurzen Überblick über die Einsatzgebiete, Features, Versionen, Anforderungen sowie Lizenztechnisches zum Small Business Server 2003. Der Small Business Server (SBS) 2003 ist der Nachfolger des SBS 2000 und wurde in vielen Punkten gegenüber seinem Vorgänger verbessert. Weiterhin erhalten Sie einige Grundlagen über unterstützte Basistechnologien des SBS 2003.

1.1 Einsatzgebiet des Small Business Server

Wie der Name schon sagt, ist der SBS für kleine und mittlere Unternehmen gedacht. So darf beispielsweise die maximale Anzahl der Clients 75 nicht übersteigen. Der SBS bietet für diese Unternehmen eine Reihe von speziell abgestimmten Funktionen für den gemeinsamen Zugriff auf das Internet, E-Mail- und Faxdienste sowie Dateien und Drucker. Alle diese Dienste sind in der kompletten Serverlösung des SBS 2003 vereint. Die Premium-Version des SBS bietet zudem noch Firewall- und Datenbankserver-Funktionalitäten.

Der Small Business Server bietet noch besser als sein Vorgänger eine einheitliche Gesamtlösung für das Infrastrukturmanagement kleiner und mittlerer Unternehmen. Der SBS 2003 umfasst die zentralen Anforderungen an Unternehmen wie E-Mail-Verkehr, sicherer Internetzugang, Dokumentenmanagement, gemeinsames Arbeiten an Dokumenten, Datenbankbereitstellung sowie die Vorzüge des Windows Server 2003 als Betriebssystemgrundlage. Die Zusammenfassung all dieser Komponenten in einem System bietet den Vorteil, dass nicht für jeden Bereich ein Werkzeug eines anderen Herstellers erworben werden muss. Dieses hätte einerseits höhere Lizenzierungskosten, andererseits auch einen höheren Schulungsaufwand für die Administration im Unternehmen zur Folge.

Gerade in kleinen und mittleren Unternehmen steht nicht immer unbedingt eine ausreichende Anzahl an Personen für Netzwerkbetreuung zur Verfügung, und deren Zeitaufwand für diese Aufgabe wird oftmals durch die Einbindung in die eigentliche Tätigkeit minimiert. Der SBS 2003 wird sich keinesfalls anmaßen, dass dieses System bequem von einem quasi Hobby-Administrator nach Feierabend verwaltet werden kann. Jedoch wird durch das homogene System sowie die Bereitstellung einer großen Anzahl von Verwaltungsassistenten die Administration entscheidend erleichtert.

1.1.1 Der expandierende Mittelstand

Insbesondere der Mittelstand ist vom Ende der 90er-Jahre bis heute gewaltig expandiert. Es fand eine große Investitionsbereitschaft in die IT statt. So ist in diesem Zeitraum der Desktop- und Servermarkt zwischen acht Prozent bis zehn Prozent gewachsen, Breitbandanbindungen sind um fast 20 Prozent gestiegen. Gleichzeitig ist auch das Daten-

volumen überdurchschnittlich angestiegen. Während sich im Jahre 1999 das E-Mail-Volumen noch auf 4 Billionen Terabyte belief, waren es 2003 bereits 18 Billionen Terabyte. Hinzu kommt, dass der Großteil sämtlicher Unternehmensdaten digital vorliegt.

1.1.2 Anhaltspunkte für die Einsatzplanung

Sofern Sie sich mit dem Einsatz des SBS 2003 beschäftigen, sollten Sie zusätzlich noch bedenken, inwieweit eine Durchführung auf interne Hindernisse stoßen könnte. Diese Hindernisse müssen nicht unbedingt nur betriebspolitischer Natur sein, sondern können auch in Sachzwängen begründet sein.

1.1.3 Entscheidungshilfe: SBS 2003 oder Windows Server 2003

Für kleine und mittlere Unternehmen bieten sowohl der SBS 2003 als auch der Windows Server 2003 Features, die den IT-Anforderungen des Unternehmens entsprechen können. Um eine Entscheidung zu erleichtern, werden im Folgenden einige Szenarien vorgestellt, die zum Einsatz der einen oder anderen der beiden Produkte raten.

Bei der Bereitstellung des SBS 2003 sind die folgenden zwei Punkte zu beachten:

- Sämtliche Komponenten des SBS 2003 werden auf einem einzelnen Server installiert. Dadurch wird die Integration aller Komponenten sichergestellt. Der primäre SBS kann jedoch um weitere Server ergänzt werden.
- Der SBS 2003 stellt die oberste Ebene eines neuen Active Directory dar. Es kann also problemlos eine Neuimplementierung erfolgen. Allerdings unterstützt die SBS-Active Directory-Domäne keine Vertrauensstellungen zu weiteren Domänen. Der SBS 2003 kann ein Ein-Domänen-Modell verwirklichen.

Unternehmen mit einer Zentrale bis zu 75 Mitarbeiter

Für maximal 75 Mitarbeiter bietet der SBS 2003 in der Standardversion eine All-in-One-Lösung für Internetanbindung, E-Mail- und Faxdienste sowie Intranetlösungen mit vielen Features für die Teamzusammenarbeit. Die Premium-Version erweitert diese Fähigkeiten um Internet-Proxy- und Firewall-Funktionalitäten, einen Datenbankserver sowie erweiterte Funktionen zur Webseiten-Ein- und Erstellung. Verfügt Ihr Unternehmen über mehr als 75 Mitarbeiter, so können Sie entweder über das Migration Pack auf einzelne, im SBS enthaltene Produkte wechseln oder von vornherein den Windows Server 2003 erwerben, der hinsichtlich der Benutzerzahl keinerlei Einschränkungen aufweist.

Anbindung einer Filiale an eine Zentrale

In diesem Modell können Sie auch den SBS 2003 einsetzen, sofern keine Einbindung in das Active Directory der Zentrale erfolgt. Diese Einbindung kann über den SBS 2003 nicht gewährleistet werden, da die SBS-Domäne die Stammdomäne im Active Directory bilden muss. Sofern eine Anbindung an das zentrale Active Directory erforderlich ist, müssen Sie einen Windows Server 2003 verwenden.

Jedoch können Sie eine SBS-Domäne über zwei Standorte hinweg implementieren. Voraussetzung dafür ist, dass sich an einem Standort ein Windows Server 2003 befindet, der sich mit dem SBS repliziert. Damit ist sichergestellt, dass bei langsamen WAN-Verbindungen zwischen zwei Standorten eine Anmeldung über die schnelle LAN-Verbindung des lokalen Standorts erfolgen kann.

Ausbau einer vorhandenen Active Directory-Umgebung

Der SBS 2003 kann nicht als Domänencontroller in eine bereits bestehende Active Directory-Umgebung implementiert werden, da er die Stammdomäne bilden muss. Weiterhin ist es auch nicht möglich, dass die SBS2003-Domäne Vertrauensstellungen zu weiteren Domänen aufbaut. Windows Server 2003 hingegen bietet die Möglichkeit, eine bestehende Domänen- oder Gesamtstruktur flexibel zu erweitern, zusätzliche Domänencontroller hinzuzufügen oder auch Vertrauensstellungen zu weiteren Active Directory- oder NT 4.0-Domänen herzustellen.

Erweiterung einer bestehenden Umgebung um zusätzliche Server

Der SBS 2003 muss der Domänencontroller der Stammdomäne sein. Innerhalb dieser Domäne können keine weiteren SBS 2003 hinzugefügt werden, wohl aber ist es möglich, weitere Windows Server 2003 als zusätzliche Domänencontroller oder Mitgliedserver einzurichten. Wollen Sie eine höhere Flexibilität erzielen oder planen später den Einsatz einer komplexeren Domänenstruktur als der einen SBS-Domäne, so sollten Sie von Anfang an den Windows Server 2003 verwenden.

Einrichtung eines Webservers für das Intranet/Internet

Ein Bestandteil des SBS 2003 ist auch ein Webserver. Dabei handelt es sich um den Internet Information Server (IIS) 6.0. Gegenüber dem Vorgänger IIS 5.0 wurde dieser stark verbessert und unterstützt nun ASP.NET sowie XML. Außer diesem in allen Windows Server-Versionen enthaltenen Webserver gibt es auch die spezielle Windows 2003 Server Web-Edition. Diese Version ist geeignet, wenn Sie lediglich einen Webserver hinzufügen möchten. Mit dieser Edition kann auch eine komplette Serverfarm betrieben werden.

Einsatz eines Terminalservers

Der SBS 2003 kann selbst nicht als Terminalserver eingerichtet werden. Als Terminalserver kann ein beliebiger Windows Server 2003 oder 2000 in die SBS-Domäne eingebunden werden. Der SBS 2003 unterstützt jedoch den Remote-Verwaltungsmodus der Terminaldienste des Windows Server 2003. So ist die Remote-Administration durch maximal zwei gleichzeitige Verbindungen sichergestellt.

1.2 Die Features des Small Business Server 2003

Im Folgenden werden Ihnen die Hauptfeatures des SBS 2003 nach Kategorien geordnet vorgestellt. Die größten Stärken des SBS 2003 liegen in der Netzwerksicherheit sowie dem Remote-Zugriff auf das Firmennetzwerk. Sie finden auch Informationen über Features, die gegenüber dem Vorgänger SBS 2000 verbessert worden sind.

1.2.1 Netzwerk, Internet und E-Mail

Der SBS 2003 verfügt über alle Features, die kleine und mittlere Unternehmen für ihren Internetzugriff und -auftritt benötigen. Dazu zählen Exchange- und Outlook-Technologien für E-Mail-Verkehr, wie z.B. Outlook Web Access oder Remote-Webarbeitsplatz, ein Webserver für den Internetauftritt, eine Firewall-Funktion, die Möglichkeit des gemeinsamen Internetzugriffs über Breitband- und Wahlverbindungen (PPPoE), Schutzmechanismen für das lokale Netzwerk sowie Produktivitätstools für die Teamarbeit. Bei der Konfiguration von Internet und E-Mail wird jedes Mal ein VBS-Skript erstellt (config.vbs). Mit Hilfe dieses Skriptes können dem Computer später wieder seine Einstellungen zurückgespielt werden. Es kann aber auch benutzt werden, um andere SBS 2003-Clients zu konfigurieren.

Die enthaltenen SharePoint Services bieten eine bereits vorkonfigurierte interne Webseite für eine umfassende Arbeit im Team.

Im Exchange Server ist eine Anti-Spam-Funktion enthalten. Zusätzlich verfügt Outlook 2003 über weitere Funktionen zum Filtern und Blockieren von Spam-Mails. Im Exchange Server ist z.B. der Microsoft Connector für POP3-Postfächer enthalten. Somit ist es möglich, bereits bestehende E-Mail-Konten nach Exchange zu migrieren und die E-Mails von diesen Konten herunterzuladen und dem Benutzer unter Outlook bereitzustellen. Für Dateianhänge ist eine Filterfunktion integriert.

Standardmäßig wird der SBS mit einem Fix gegen den Blaster-Wurm geliefert. Dieses Fix wird automatisch installiert. Außerdem kann beliebige Antiviren-Software eingesetzt werden, die mit Exchange und Windows Server 2003 kompatibel ist. Die Antiviren-Software sollte nach Möglichkeit eine Server-Client-Konfiguration unterstützen und nicht bloß eine einfache Client- bzw. Desktop-Lösung sein.

Der SBS 2003 kann wie ein Windows Server 2003 für Netzwerkdienste wie DNS, DHCP, WINS usw. konfiguriert werden.

Die Kombination von Outlook/Exchange 2003 sowie Windows Server 2003 erlaubt nun auch RPC über http. Dadurch ist es möglich, via Internet sichere Verbindungen zu RPC-Serveranwendungen herzustellen.

1.2.2 Sicherheit

Der SBS 2003 verfügt über eine Reihe von Assistenten zur Konfiguration der notwendigen Sicherheitseinstellungen. In Sachen Sicherheit wurde der Windows Server 2003, auf dem der SBS ja basiert, gegenüber dem Windows Server 2000 entscheidend verbes-

sert. Angriffe auf den Server konnten um 60 Prozent reduziert werden, während die Verfügbarkeit von Diensten um 275 Prozent angestiegen ist. Bereits in der Standardversion ist eine Firewall enthalten, in die Premium-Version ist der ISA Server 2000 integriert.

Der SBS unterstützt außerdem auch hardwarebasierte Firewalls. Fast sämtliche UPnP-Geräte (Universal Plug –and Play) werden durch den Internetverbindungs- und E-Mail-Konfigurationsassistenten automatisch erkannt. Ist das Firewall-Gerät nicht UPnP-fähig, ist eine manuelle Konfiguration des Geräts erforderlich. Zu Problemen kann es selbst bei UPnP-Geräten kommen, wenn diese auf ein proprietäres Protokoll zurückgreifen.

Die eingebaute Funktion des Volume Shadow Copy Service ermöglicht zeitgesteuerte Datensicherungen. Diese werden schnell und sicher ausgeführt.

1.2.3 Zusammenarbeit im Team

Der SBS 2003 bietet einen zentralen Speicherort für große Datenmengen. Diese Daten können in einfacher Weise bearbeitet, gemeinsam genutzt und archiviert werden. Selbst für unternehmenskritische Daten bietet der SBS 2003 einen sicheren Speicher.

Basierend auf den Windows SharePoint Services stellt der SBS 2003 eine vorkonfigurierte interne Webseite bereit. Über diese zentrale Webseite ist es den Mitarbeitern möglich, Dokumente, Ankündigungen, Ereignisse oder Links gemeinsam zu nutzen. Die Outlook 2003-Funktion Enhanced Outlook Web Access ermöglicht zudem die gemeinsame Nutzung von Daten oder Kalenderfunktionen über das Internet.

1.2.4 Remote-Zugriff und Mobilität

Auf die Daten des SBS 2003 kann aus der Ferne zugegriffen werden. Dabei spielen Zeit, Ort und Gerät keine Rolle. Der Zugriff kann sowohl für private, als auch für öffentliche Dateien konfiguriert werden. Ein Benutzer hat somit Zugriff auf seinen Desktop und seine E-Mails. Der Zugriff erfolgt über das neue Remote-Portal Remote-Webarbeitsplatz. Auch eine Synchronisierungsfunktion der Daten ist enthalten. Der Einbindung mobiler Geräte wie Smartphones, PDAs usw. wird unter SBS 2003 große Bedeutung zugemessen. Mobilen Benutzern wird es ermöglicht, über Outlook Mobile Access (OMA) auf E-Mails, Kalender, Zeitpläne oder Aufgaben zuzugreifen.

Für den Administrator steht selbstverständlich auch eine Remote-Verwaltung zur Verfügung.

Zudem sind Funktionen für virtuelle private Netzwerke (VPNs) enthalten.

1.2.5 Einrichtung und Administration

Die Installation und Konfiguration des SBS 2003 geschieht mit Hilfe komfortabler Assistenten und benötigt wenig Zeitaufwand. Zudem ist der SBS 2003 auf diversen OEM-Plattformen bereits vorinstalliert. Auch die Einrichtung der SBS-Clients ist gegenüber SBS 2000 vereinfacht worden, da die Aktivierung nicht mehr via Diskette, sondern bequem über das Internet via Online License Activation erfolgt. Für OEMs ist es zudem möglich, den kompletten SBS vorzuinstallieren und dabei etwa eigene Logos, Servicenummern etc. einzubinden.

Zudem erfolgt die Netzwerkeinrichtung der Clients nun bequem über eine Webseite und nicht mehr via Diskette. Zudem ist eine Vorkonfiguration von Clientanwendungen möglich. Im Gegensatz zu früheren Versionen, in denen immer nur ein Benutzer gleichzeitig angelegt werden konnte, können Sie nun mit Hilfe von Benutzervorlagen mehrere Benutzer in einem Arbeitsschritt anlegen.

Auch die Überwachungsfunktionen wurden verbessert. So können nun Leistungs- und Nutzungsberichte online oder per E-Mail empfangen und ausgewertet werden. Durch die damit gegebene schnellere Reaktionszeit werden Ausfallzeiten des SBS minimiert.

1.3 Versionen des Small Business Server

Der Small Business Server 2003 ist in zwei verschiedenen Versionen verfügbar. Es gibt eine Standard- und eine Premium-Version. Die folgende Tabelle listet die jeweils enthaltenen Bestandteile der beiden verschiedenen Versionen auf.

Bestandteil	Standardversion	Premium-Version
Windows Server 2003 (5 CAL)	x	x
Outlook 2003 (5 CAL)	x	x
Windows SharePoint Services	x	x
Exchange Server 2003	x	x
Shared Fax Services	x	x
ISA Server 2000 SP1	–	x
SQL Server 2000 SP3	–	x
Office Front Page 2003	–	x

Tabelle 1.1: Die Versionen des Small Business Server 2003 im Überblick

Die folgende Tabelle gibt Ihnen einen kurzen Überblick über die Funktion der verschiedenen Komponenten und kann bei der Auswahl der gewünschten Version helfen.

Komponente	Beschreibung
Windows Server 2003	Auf diesem Betriebssystem in der Standardversion basiert der SBS 2003. Damit ist beispielsweise die Einrichtung des Verzeichnisdienstes Active Directory möglich. Einschränkungen sind im nächsten Absatz nach dieser Tabelle beschrieben.
Exchange Server 2003 und Outlook 2003	E-Mail- und Messaging-Serverlösung, die Features wie Web Access für den Fernzugriff auf Mails oder eine vom Team gemeinsam nutzbare Kalenderfunktion bereitstellt.
SharePoint Services	Umgebung für die Zusammenarbeit und Kommunikation im Team.

Komponente	Beschreibung
Shared Fax Services	Faxfunktion, für die kein hoher Bedarf an Telefonanschlüssen besteht. Der Faxempfang kann über Drucker, E-Mail oder SharePoint erfolgen. Das Senden von Faxen ist über die Benutzer-Desktops sowie auch zeitversetzt möglich.
ISA Server 2000	Firewall-Dienst, Routing und NAT (Network Address Translation), sicherer Internetzugang für mehrere Benutzer gleichzeitig
SQL Server 2000	Leistungsstarke, relationale Datenbank, Zum Ausführen und Bereitstellen von Geschäftsanwendungen
Front Page 2003	Entwicklungsumgebung für Webseiten sowie Lösungen für die SharePoint Services

Tabelle 1.2: Beschreibung der Komponenten des SBS 2003

Der Windows Server 2003 als Bestandteil des SBS 2003 ist gegenüber der „normalen" Version eines Windows Server 2003 in folgenden Punkten eingeschränkt:

- Innerhalb einer Domäne kann nur ein Computer mit Windows Server 2003 for Small Business Server betrieben werden.
- Es ist nicht möglich, vom SBS 2003 in der Domäne die fünf Betriebsmasterrollen (FSMO, Flexible Single-Master Operation) zu entfernen. Sie können zwar weitere Domänencontroller zur Domäne hinzufügen, die fünf Betriebsmaster müssen jedoch auf dem SBS 2003 belassen werden. Lediglich der globale Katalog (siehe Kapitel Abbildung 1.9.3) kann zur Entlastung des SBS 2003 auf einem anderen Domänencontroller ausgeführt werden.
- Innerhalb des Active Directory muss der SBS 2003 die Root-Domäne, also die höchste Ebene der Active Directory-Struktur darstellen. Er kann über keine untergeordneten Domänen verfügen. So ist es nicht möglich, den SBS 2003 in ein Unternehmensnetzwerk einzubinden und innerhalb dieses beispielsweise als Zweigstellenserver zu betreiben.
- Die Domäne des Windows Server 2003 for Small Business Server kann zu keiner anderen Domäne eine Vertrauensstellung aufbauen. Deshalb ist auch kein serverübergreifender Ressourcenzugriff möglich.
- Zusätzliche Server müssen über eine Zugriffslizenz (CAL, Client Access Licence) für Windows Small Business Server verfügen.

Ansonsten entspricht der im Lieferumfang des SBS 2003 enthaltene Server einem Windows Server 2003 Standard.

Sämtliche Serverkomponenten des SBS 2003 müssen auf einem Computer ausgeführt werden. Es ist also nicht möglich, beispielsweise den SQL-Server der Premium-Version auf einem anderen Server zu installieren. Einzig Front Page 2003 der Premium-Version kann auf einem beliebigen Client innerhalb des SBS-Netzwerks installiert werden.

Neben der Version des Windows Server 2003, die im Small Business Server enthalten ist, gibt es auch einen *Windows Server 2003 for Small Business Server*. In dieser Serverversion sind keine weiteren Funktionen der Small Business Standard- bzw. Premium-Version enthalten. Es handelt sich hierbei um die reine Serverlösung als abgespeckte Version des SBS 2003. Diese Version unterliegt denselben Einschränkungen wie der Windows Server 2003 des SBS.

Der Windows Server 2003 for Small Business Server ist für einen Preis von ca. 450 € erhältlich. Darin enthalten sind fünf CALs für den Server. Zusätzlich können bis zu zehn weitere CALs für jeweils etwa 75 € erworben werden. Benötigen Sie mehr als 15 CALs, sollten Sie lieber auf den Windows Server 2003 in der Standardversion zurückgreifen, da dann dieses Modell günstiger wird.

Während die Premium-Version über den ISA-Server 2000 SP1 als integrierte Firewall-Lösung verfügt, ist in der Standardversion lediglich die Internetverbindungs-Firewall des Windows Server 2003 selbst enthalten.

Zusätzlich kann in den Small Business Server der Microsoft SUS-Server (Software Update Services) integriert werden. Diese Komponente kann kostenlos downgeloadet werden (siehe). Aktuell ist die Version SUS 1.0 mit Service Pack 1. Das Einbinden des SUS in ein Small Business Server-Netzwerk wird in Kapitel 10 näher erläutert.

Unter SBS 2003 können im Gegensatz zu SBS 2000 die Terminaldienste nicht im Anwendungsmodus ausgeführt werden. Diese Funktion wurde herausgenommen, da der Anwendungsmodus auf einem Domänencontroller Risiken für das Netzwerk birgt. Sollen dennoch die Terminaldienste im Anwendungsmodus ausgeführt werden, sollten Sie einen „richtigen“ Windows Server 2003 zur Domäne hinzufügen.

1.4 Hardwareanforderungen

Die Standard- und Premium-Version des SBS 2003 unterscheiden sich in einigen Bereichen in ihren Hardwareanforderungen.

1.4.1 Anforderungen für die Standardversion

Im Folgenden finden Sie eine Aufstellung der von Microsoft empfohlenen Hardwareanforderungen für den Betrieb des SBS 2003 in der Standardversion. Im Bezug auf die heute angebotene Hardware nehmen sich die Anforderungen eher bescheiden aus. Bedenken Sie jedoch, dass Einsparungen an der Hardware immer zu Lasten der Performanz gehen werden.

Komponente	Minimum	Empfohlen
Prozessor	300 Mhz	Ab 550Mhz
RAM	256 MB	384 MB (Maximum 4 GB)
Plattenkapazität	4 GB	4 GB
Laufwerke	CD-ROM	CD-ROM oder DVD
Grafik	VGA	SVGA (mindestens 800 x 600 Pixel)
Weitere Komponenten	Netzwerkkarte	Zwei Netzwerkkarten
Für den Internetzugang	Breitband- oder Hochgeschwindigkeitsmodem-Internetverbindung Möglicherweise entstehen zusätzliche Verbindungskosten beim Service Provider.	Breitband- oder Hochgeschwindigkeitsmodem-Internetverbindung Möglicherweise entstehen zusätzliche Verbindungskosten beim Service Provider.
Für das Netzwerk	Dediziertes Klasse-1-Faxmodem für den Faxdienst	Dediziertes Klasse-1-Faxmodem für den Faxdienst Für Outlook Mobile Access (OMA) Pocket PC Phone Edition 2003 oder Smartphone 2003 Als Client-Betriebssysteme Windows XP oder Windows 2000

Tabelle 1.3: Hardwareanforderungen für den Betrieb des SBS 2003 Standard

1.4.2 Anforderungen für die Premium-Version

Im Folgenden finden Sie eine Aufstellung der von Microsoft empfohlenen Hardwareanforderungen für den Betrieb des SBS 2003 in der Premium-Version.

Komponente	Minimum	Empfohlen
Prozessor	300 Mhz	Ab 550 Mhz
RAM	256 MB	512 MB (Maximum 4 GB)
Plattenkapazität	5 GB, bei einer Aktualisierung von SBS 2000 2 GB	5 GB, bei einer Aktualisierung von SBS 2000 2 GB
Laufwerke	CD-ROM	CD-ROM oder DVD
Grafik	VGA	SVGA (mindestens 800 x 600 Pixel)
Weitere Komponenten	Netzwerkkarte	Zwei Netzwerkkarten

Komponente	Minimum	Empfohlen
Für den Internetzugang	Breitband- oder Hochgeschwindigkeitsmodem-Internetverbindung Möglicherweise entstehen zusätzliche Verbindungskosten beim Service Provider.	Breitband- oder Hochgeschwindigkeitsmodem-Internetverbindung Möglicherweise entstehen zusätzliche Verbindungskosten beim Service Provider.
Für das Netzwerk	Dediziertes Klasse-1-Faxmodem für den Faxdienst	Dediziertes Klasse-1-Faxmodem für den Faxdienst Für Outlook Mobile Access (OMA) Pocket PC Phone Edition 2003 oder Smartphone 2003 Als Client-Betriebssysteme Windows XP oder Windows 2000

Tabelle 1.4: Hardwareanforderungen für den Betrieb des SBS 2003 Premium

Beide Versionen unterstützen maximal zwei reale physische CPUs bzw. vier virtuelle CPUs.

1.5 Lizenzinformationen und Kosten

Für den Betrieb des SBS werden sowohl eine Windows Small Business Server 2003-Lizenz als auch eine Windows Small Business Server 2003-CAL benötigt. In der erstgenannten Lizenz ist die Installations- und Nutzungserlaubnis des SBS 2003 enthalten, die zweitgenannte Lizenz gestattet den Zugriff auf die Serversoftware auf der Basis Benutzer oder Computer. Die CALs beziehen sich nicht auf gleichzeitige Verbindungen. Preislich unterscheiden sich die CALs der Standard- und Premium-Version nicht. In einer SBS 2003-Domäne dürfen maximal 75 CALs verwendet werden. Im SBS-Paket sind bereits fünf CALs enthalten.

Bei einer Benutzer-CAL darf ein bestimmter Benutzer auf den SBS 2003 zugreifen. Dabei ist es unerheblich, von welchem Computer aus er die Verbindung herstellt (z.B. Desktop oder mobiles Gerät). Eine Computer-CAL gilt nur für einen Computer. Allerdings können sich an diesem Rechner beliebige Benutzer anmelden. Für die fünf enthaltenen CALs können Sie bestimmen, ob Sie diese pro Benutzer oder Computer verwenden möchten. Ein automatisches Überwachen der Lizenzen sieht der SBS 2003 nicht vor.

Die CAL gilt nicht nur für den SBS selbst, sondern auch für weitere Windows-basierte Server innerhalb der SBS-Domäne. Dies gilt jedoch nicht für weitere Exchange-, SQL-Server usw.

Sofern Sie für die Small Business Server 2000-CAls eine Software Assurance abgeschlossen haben, können Sie sämtliche CALs kostenlos in CALs für SBS 2003 umtauschen. Ist dies nicht der Fall, müssen Sie die CALs neu erwerben.

Haben Sie eine Software Assurance für den SBS 2000 sowie die SBS 2000-CALs abgeschlossen, haben Sie Anspruch auf einen SBS 2003 Premium.

Sofern Sie eine Software Assurance für die SBS 2003-CALs abgeschlossen haben, können Sie beim Erneuern der Assurance kostenlos benutzerbasierte CALs gegen computerbasierte CALs eintauschen und umgekehrt.

Im Gegensatz zu SBS 2000 erfolgt die Aktivierung der CALs nicht mehr per Diskette, sondern ausschließlich über einen speziellen Aktivierungsschlüssel via Internet. Alternativ können Sie auch mit Hilfe des Assistenten zum Hinzufügen neuer SBS-Lizenzen arbeiten und die Lizenzen per Telefon (zum Ortstarif) aktivieren.

Ein SBS 2003 in der Standardversion kostet ca. 599 $, ein SBS 2003 in der Premium-Version ca. 1499 $. Detailliertere Preisangaben finden Sie unter *http://www.microsoft.com/windowsserver2003/sbs/howtobuy/pricing.mspx*

Soll eine bestehende SBS-Domäne erweitert werden, d.h., sind entweder mehr als 75 Benutzer in der Domäne vorhanden oder sollen die Serverkomponenten des SBS auf mehrere physikalische Systeme verteilt werden bzw. ist eine höhere Funktionalität, etwa die eines Exchange 2003 Enterprise Servers, notwendig, so empfiehlt sich der Erwerb des Small Business Server 2003 Transition Packs. Nähere Hinweise zu den Inhalten und Preisen des Transition Packs finden Sie unter dem eben genannten Link.

1.6 Active Directory als Basistechnologie des SBS 2003

Die Hinweise und Beschreibungen des Active Directory als Basistechnologie des SBS 2003 sind an dieser Stelle als Grundlage vor allem auch für die Benutzer gedacht, die bisher noch keine oder nur wenige Erfahrungen mit Active Directory-basierten Netzwerken besitzen wie z.B. Umsteiger von Windows NT 4.0 oder Novell NetWare. Eine umfassende Beschreibung dieses komplexen Themas würde an dieser Stelle den Rahmen dieses Buches sprengen.

Das Active Directory ist die seit Windows Server 2000 integrierte Verzeichnisdienstlösung für die zentrale Verwaltung von Netzwerkobjekten. Unter SBS 2003 können Sie über das Active Directory sämtliche Netzwerkobjekte des SBS 2003-Netzwerks verwalten.

1.6.1 Aufbau des Active Directory

In diesem Kapitel erfolgt eine Einführung in die Thematik Active Directory. Zunächst wird eine kurze allgemein gültige Beschreibung von Active Directory an sich gegeben sowie die Funktionsweise eines Verzeichnisdienstes detailliert erläutert. Das primäre

Zugriffsprotokoll für Active Directory ist LDAP (Lightweight Directory Access Protocol). Zusammenfassend werden am Ende die in Active Directory enthaltenen und gegenüber Windows NT neuen Kern-Features präsentiert.

Microsoft vollzog mit Active Directory in Windows 2000 den Einstieg in die Welt der Verzeichnisdienste. Bereits länger am Markt vertreten ist Novell Directory Service (NDS) der Firma Novell NetWare. Das Active Directory basiert auf Internetstandardtechnologien. Es ist vollständig in das Betriebssystem des SBS 2003 integriert. Mit Active Directory wird das Domänenmodell von Windows NT 4.0 erweitert. Das primäre Zugriffsprotokoll für Active Directory ist LDAP (Lightweight Directory Access Protocol) in der Version 3.

1.6.2 Wie arbeitet ein Verzeichnisdienst?

Ein Verzeichnisdienst arbeitet vergleichbar mit einem Telefonbuch. In einem Telefonbuch ist mit jedem Namenseintrag eine bestimmte Telefonnummer verknüpft. Außerdem können Sie dort weitere optionale Informationen wie z.B. die Adresse eines Teilnehmers finden. Im Verzeichnisdienst sind die Objekte der Netzwerkressourcen, wie z.B. Benutzer, Drucker, Datenbanken usw., mit Informationen verknüpft. Diese Informationen enthalten z.B. den Namen des Objekts, den Standort und viele objektspezifische Informationen. Je mehr optionale Informationen Sie bei den Eigenschaften eines Objekts angeben, desto schneller und präziser kann das Objekt später von den Netzwerkbenutzern gefunden werden – auch wenn dies natürlich beim einmaligen Einpflegen der Objekte in die Datenbank mehr Zeit in Anspruch nimmt.

Wenn der Name eines Objekts im Verzeichnis bekannt ist, z.B. der Benutzername, kann eine dazugehörige Information wie z.B. eine E-Mailadresse direkt bezogen werden. Dies entspricht dem Nachschlagen eines bekannten Namens in einem herkömmlichen Telefonbuch, um die zugeordnete Telefonnummer zu erhalten. Damit sind die Nachschlagefunktionen des Verzeichnisses aber noch nicht erschöpft. Angenommen, Sie kennen nicht exakt den Namen eines Objekts, dafür aber einige Informationen. Dann werden alle Objekte im Verzeichnis nach diesen Kriterien durchsucht. Dieser Vorgang entspricht dem Nachschlagen in den „Gelben Seiten“. Dieses verwenden Sie, wenn Sie nicht den genauen Namen z.B. kennen. Sie finden dann eine Liste aller. Das Verzeichnis ist den „Gelben Seiten“ aber insofern überlegen, dass die jene nur nach vordefinierten Einträgen durchsucht werden können, während Sie im Verzeichnis selbst die Kriterien bestimmen können, nach denen Sie suchen möchten.

Ein Verzeichnisdienst ermöglicht es, alle Netzwerkobjekte zentralisiert zu verwalten. Im Active Directory können Informationen über Benutzer, Server, Computer, Drucker usw. an einer Stelle gepflegt und verwaltet werden – die Informationen können aber von allen Benutzern im gesamten Netzwerk abgerufen werden. Dadurch wird sowohl das Verwalten als auch das Finden der Netzwerkressourcen stark vereinfacht.

Objekte im Verzeichnis

Im Verzeichnis werden die Objekte gespeichert. Ein Objekt ist eine gespeicherte Information, die mit einer Netzwerkressource verknüpft ist. Um die Ressourcen den Netzwerkbenutzern oder auch Applikationen zur Verfügung stellen zu können, wird der Verzeichnisdienst benötigt. Hierbei handelt es sich um einen Netzwerkdienst, der für die

Identifikation der Ressourcen zuständig ist, damit die Benutzer auf diese zugreifen können. Im Active Directory können Millionen von Objekten gespeichert werden. Deshalb muss jedes einzelne Objekt eindeutig gekennzeichnet und referenziert sein, damit es gefunden werden kann. Dafür hat jedes einzelne Objekt in Active Directory eine eindeutige Kennung, die als *GUID* (Globally Unique Identifier) bezeichnet wird. Bei dem GUID handelt es sich um einen Wert von 128 Bit Länge. Dieser Wert wird jedem Objekt beim Erstellen zugeteilt.

Es gibt zwei Arten von Active Directory-Objekten: *Container* und *Nicht-Container*. Die Nicht-Container werden auch *Endknoten* oder *Leafs* genannt. Ein Container enthält weitere Container oder Endknoten, ein Endknoten kann keine weiteren Objekte enthalten. Ein Beispiel für einen Container ist z.B. eine Organisationseinheit. In dieser befinden sich Computer, Benutzer usw. Ein Beispiel für einen Endknoten ist z.B. ein Benutzer. Auch Computer werden als Endknoten klassifiziert, obwohl sie rein theoretisch auch Objekte, wie z.B. Drucker, enthalten könnten.

Verzeichnis und Verzeichnisdatenbank

Da das Verzeichnis oftmals auch als Datenbank oder Verzeichnisdatenbank bezeichnet wird, sollen grundlegend die Unterschiede zwischen diesen beiden Begriffen klargestellt werden. Ein Verzeichnis bietet Funktionen, die weit über die der herkömmlichen relationalen Datenbanken hinausgehen. Ein großer Unterschied besteht darin, dass die Informationen aus einem Verzeichnis weitaus öfter abgerufen als geändert werden. In einer Datenbank werden vermehrt aktualisierte Daten geschrieben. Deshalb sollten in einem Verzeichnis also die Such- und Lesefunktionen gegenüber der Schreibfunktion optimiert sein. Der Lesezugriff geschieht schließlich durch alle Benutzer des Verzeichnisses, während der Schreibzugriff auf die Administratoren beschränkt ist. Es werden Daten im Verzeichnis gespeichert, die relativ statisch sind, da sie nicht oft Änderungen unterworfen sind. Die Verzeichnisbenutzer können Hunderte Male, wenn nicht sogar noch öfter die E-Mail-Adresse eines bestimmten Benutzers abfragen, während diese im selben Zeitraum vom Administrator höchstwahrscheinlich nicht geändert wird.

Ein zweiter Unterschied zwischen Verzeichnis und Datenbank besteht im Zugriff auf die jeweilige Komponente. Auf eine Datenbank wird meist mittels einer standardisierten, komplexen SQL(Structured Query Language)-Abfrage zugegriffen. Hiermit werden zwar komplexe Abfragen und Updates der Datenbank ermöglicht, aber leider geschieht dies auf Kosten von Komplexität und Größe der Applikation. Verzeichnisse wie das Active Directory benutzen das LDAP(Lightweight Directory Access Protocol)-Protokoll zum Zugriff. Hierbei handelt es sich um ein einfaches, optimiertes und schlankes Protokoll. Ausführlich wird LDAP im nächsten Kapitel beschrieben.

Client-Server-Kommunikation

Der Zugriff auf Informationen im Verzeichnis erfolgt über das Client-Server-Kommunikationsmodell. Dabei darf eine Applikation auf einem Client, die Informationen aus dem Verzeichnis benötigt, nicht direkt auf das Verzeichnis auf dem Server zugreifen. Es wird eine API (Application Programming Interface) aufgerufen, die über eine entsprechende Meldung einen neuen Prozess aufruft, den Directory Client, der die weitere Anfrage

über das TCP/IP-Protokoll durchführt. Der direkte Zugriff auf das Verzeichnis erfolgt über den Directory Server. Über diesen Mechanismus wird schließlich in umgekehrter Reihenfolge die Information an die Applikation zurückgeschickt.

Ein Verzeichnisdienst ist nur eine Beispiel für die Client-Server-Kommunikation. Weitere Dienste sind z.B. der Druckdienst, der Webservice usw. Sie können alle auf einem Computer gemeinsam vorhanden sein.

Sicherheit

Auch die Sicherheit der im Verzeichnis gespeicherten Objekte muss kurz angesprochen werden. Es muss möglich sein, dass alle Verzeichnisbenutzer öffentliche Informationen wie etwa die E-Mail-Adresse eines Kollegen finden können, weiterhin z.B. Mitglieder der Personalabteilung weitere Informationen wie etwa die komplette Privatanschrift lesen können, aber nur die Administratoren die Möglichkeit haben, diese Einträge zu verändern. Die Steuerung des Objektzugriffs erfolgt über Access Control Lists (ACL). Zu jedem Objekt wird automatisch eine Liste generiert, in der eingetragen wird, welche Benutzer welche Zugriffsrechte für das Objekt besitzen.

1.7 Das Lightweight Directory Access Protocol (LDAP)

Für die Kommunikation zwischen den Active Directory-Clients und -Servern bei der Netzwerkanmeldung oder dem Auffinden von Ressourcen wird *LDAP* (*Lightweight Directory Access Protocol*) in der Version 3.0 als das Standardzugriffsprotokoll benutzt. In diesem Kapitel wird Ihnen zunächst eine Übersicht über die Entwicklung von LDAP gegeben. Danach erfolgt eine Übersicht über die definierten LDAP-Standards.

LDAP ist ein Kommunikationsprotokoll, das den Transport sowie das Message-Format definiert, das die Clients für den Zugriff auf ein Verzeichnis benutzen, das nach dem X.500-Standard arbeitet. Die gesamte Kommunikation des LDAP läuft über den Port 389. Im LDAP-Protokoll wird festgelegt, wie der Zugriff auf die Active Directory-Server erfolgen darf, welche Verzeichnisaktionen gestattet sind, welche freigegebenen Daten benutzt werden dürfen oder wie ein sicherer Zugriff durchgeführt werden soll. Über LDAP werden Verwaltung, Abfragen und Auflistungen der Objekte durchgeführt.

Eine Applikation darf niemals direkt auf die Verzeichnisdaten zugreifen, sondern der Zugriff wird über eine API gesteuert, die über eine Message aufgerufen wird. Hierbei handelt es sich um eine LDAP-API, die von einer LDAP-Message initiiert wird. Der LDAP-Client kann direkt über TCP/IP auf das Verzeichnis des LDAP-Servers zugreifen.

LDAP hat sich zu einem offenen Industriestandard entwickelt. Über dieses Protokoll können Produkte verschiedener Hersteller in verschiedenen Betriebssystemen miteinander kommunizieren und, vergleichbar dem HTTP-Standard des Internets, damit eine globale Verzeichnisstruktur unterstützen.

1.7.1 Die LDAP-Architektur

In diesem Kapitel wird Ihnen das logische Modell von LDAP vorgestellt. Wie bereits erwähnt, ist LDAP das Zugriffsprotokoll für X.500-basierte Verzeichnisdienste. Gegenüber DAP und OSI bietet LDAP mit Active Directory die folgenden Verbesserungen: LDAP benutzt TCP/IP und nicht den ressourcenintensiven OSI-Protokoll-Stack. Das Funktionsmodell ist vereinfacht und um selten gebrauchte Funktionen erleichtert worden. Außerdem werden normale Zeichenketten zur Darstellung der Daten benutzt und nicht mehr komplizierte Syntaxen wie ASN.1 (Abstract Syntax Notation).

Über LDAP wird die Meldung definiert, die zwischen einem LDAP-Client und LDAP-Server ausgetauscht wird. Über die Meldung seitens des Clients werden die durchzuführende Handlung wie das Suchen oder Löschen eines Objekts angegeben, seitens des Servers die daraus resultierenden Antworten sowie das Format der transportierten Daten. Der Transport der Daten geschieht über das TCP/IP-Protokoll. Für das Design von Active Directory ist wichtig zu wissen, wie das Verzeichnis aufgebaut ist, welche Operationen durchgeführt werden können oder wie Daten auf dem Transport geschützt sind.

Jede Kommunikation zwischen einem LDAP-Client und -Server läuft identisch ab. Sie kann in drei Schritte unterteilt werden.

1. Der LDAP-Client stellt die Verbindung zum Server her. Dabei gibt der Client für den Server die IP-Adresse oder den Host-Namen sowie den TCP-Port (389) des LDAP-Servers an. Die Authentifizierung kann auf dreierlei Weise erfolgen: Über anonyme Authentifizierung mit Standardzugriffsrechten, der Client kann sich über einen Benutzernamen und Passwort authentifizieren, oder die Verbindung kann verschlüsselt erfolgen.
2. Der Client greift nun auf die Verzeichnisdaten zu. Der Zugriff kann als Schreib- oder Lesevorgang erfolgen. Am häufigsten werden Suchvorgänge sein. Dabei kann ein Benutzer über Boole´sche Operatoren bestimmen, welche Informationen herausgefiltert werden sollen.
3. Nach Ende der durchgeführten Aktion wird die Verbindung zum Server beendet.

Da LDAP auf dem X.500-Modell basiert, werden dementsprechend die Daten im Verzeichnis als Einträge gespeichert und organisiert. Ein Eintrag ist die Basiseinheit für die gespeicherten Informationen im Verzeichnis. Jeder Verzeichniseintrag beschreibt ein einzelnes Objekt. Jedes Objekt besitzt einen eindeutigen *definierten Namen* (= *Distinguished Name, DN*), der sich seinerseits aus einer Reihe von *relativ definierten Namen* (= *Relative Distinguished Name, RDN*) zusammensetzt. Diese Namenskette ist vergleichbar mit einem Verzeichnispfad im Windows-Explorer. Diese Objekte werden in einer hierarchischen Baumstruktur angeordnet, die auf den DNs der Objekte basieren. Diese Baumstruktur wird auch Directory Information Tree (DIT) genannt.

Jeder Eintrag besteht aus einem oder mehr Attributen zur Beschreibung des Eintrags. Jedes Attribut besteht aus einem Typ und einem Wert.

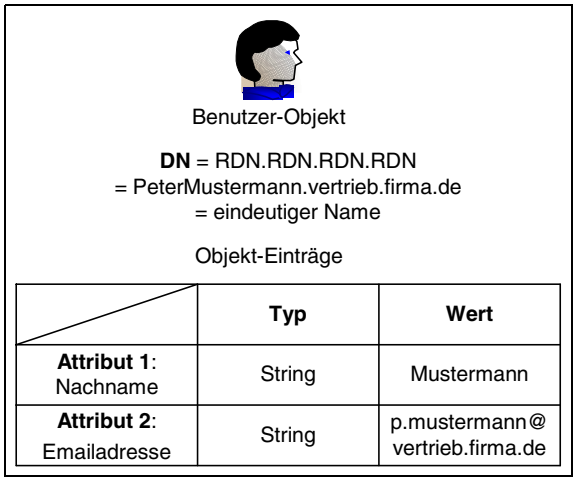


Abbildung 1.1: Der Aufbau eines Objekteintrags

In unserem Beispiel sind die Attribute *Nachname* und *E-Mailadresse* herausgegriffen. Die Syntax des Attributs bestimmt, dass es sich dabei um einen alphanumerischen String handelt. Es können in einer E-Mailadresse Buchstaben, Zahlen oder auch Sonderzeichen wie ein Bindestrich (-) vorkommen.

Durch die Verzeichniseinträge wird ein Objekt näher beschrieben. Dabei beschreibt eine Objektklasse ein Objekt. Die Objektklasse *Benutzer* wird z.B. durch die Attribute *Nachname* und *E-Mailadresse* beschrieben. Jede Objektklasse hat ihre eigenen Attribute, und jedes Attribut hat seinen eigenen Wert. So werden Sie beispielsweise in einem Druckerobjekt nicht die Attribute *Nachname* und *E-Mailadresse* finden, sondern eher ein Attribut *Farbdrucker*. Alle diese Objektklassen und in ihnen mögliche Werte werden als das Active Directory-Schema bezeichnet.

Weiterhin wird über LDAP festgelegt, welche Handlungen an einem Verzeichniseintrag vollzogen werden können. Hierzu zählen das Hinzufügen, Löschen, Ändern und Umbenennen eines Eintrags, wobei schreibend auf das Verzeichnis zugegriffen wird, sowie das Suchen und Vergleichen eines Eintrags. Hier erfolgt nur ein lesender Zugriff auf die Verzeichnisdaten.

1.8 Die Features des Active Directory

Active Directory bietet die folgenden neuen, fest integrierten, aber dennoch flexibel gestaltbaren Features, die im Windows NT-Domänenmodell nicht verfügbar waren:

- Vereinfachen der Verwaltung durch Zentralisierung. Jede Domäne kann mehrere gleichrangige Domänencontroller enthalten. Dadurch werden die Änderungen, die Sie an einem Domänencontroller vornehmen, automatisch auf die anderen repliziert. Ein Administrator kann sich von einem beliebigen Computer im Netzwerk aus anmelden und von dort aus Ressourcen auf anderen Computern der Domäne verwalten.

- Delegierung von bestimmten Verwaltungsoperationen vom zentralen Administrator an Unteradmins. Einem Benutzer wird von einer höheren Autoritätsebene gestattet, einen bestimmten Satz von Aktionen an einer festgelegten Gruppe von Objekten in einem zugewiesenen Abschnitt der Domänenstruktur durchzuführen. Hiermit erfolgt eine präzise Kontrolle darüber, wer welche Aktion ausführen darf, ohne dass dem Benutzer dafür höher privilegierte Benutzerrechte erteilt werden müssen.
- Speichern der Objekte in einer strukturierten Hierarchie, welche die Unternehmensgliederung abbildet. Domänen können z.B. nach geografischen oder funktionellen Aspekten eingerichtet werden; in Organisationseinheiten kann die physische Struktur des Unternehmens, z.B. Einteilung in Etagen, abgebildet werden.
- Hohe Verfügbarkeit der Daten sowie Lastenverteilung durch Multimaster-Replikation des Verzeichnisses auf alle Domänencontroller. Dadurch wird das Verzeichnis einer größeren Gruppe von Benutzern zugänglich gemacht. Außerdem ist beim Ausfall eines Domänencontrollers ein hohes Maß an Redundanz geboten, da die Aktualisierung von Active Directory nicht mehr an einen PDC gebunden ist, sondern auf jedem beliebigen Domänencontroller durchgeführt werden kann.
- Einfacheres und schnelleres Finden der Ressourcen im Netzwerk: Es kann z.B. nach einem Netzwerkdrucker gesucht werden, auch wenn nicht die komplette Adresse bekannt ist. Geben Sie zur Suche nur Teile der Ihnen bekannten Eigenschaften ein, z.B. Duplex – ja oder nein, Farbe – ja oder nein usw.
- Hohe Skalierbarkeit. Die Active Directory-Datenbank hat eine viel höhere Kapazität als die Windows NT-Benutzerdatenbank. Es ist möglich, zunächst eine kleine Domänenstruktur mit vielleicht 200 Objekten zu erstellen, die später dynamisch mit dem Wachstum des Unternehmens auf Millionen von Objekten erweitert werden kann.
- Erweiterbarkeit und individuelle Anpassung des Active Directory-Schemas. Jedem Objekt können eigene Attribute hinzugefügt werden, die sehr unternehmensspezifisch sein können, so z.B. ein Attribut für zeichnungsberechtigt o.Ä. hinzufügen.
- Unterstützung von Standards wie LDAP, NSPI (Name Service Provider Interface), HTTP und DNS. Active Directory unterstützt die Internetstandards und baut auf diesen auf. Durch die Unterstützung des LDAP 3.0 sowie NSPI-Standards ist die Zusammenarbeit mit anderen Verzeichnisdiensten sichergestellt, die ebenfalls diese Protokolle verwenden. Mit DNS wird das Internet-Namenskonzept in Windows 2000 integriert. Windows 2000 unterstützt sogar dynamisches DNS (DDNS). Clients mit über DHCP bezogenen IP-Adressen können sich dadurch dynamisch beim DNS-Server registrieren. In einer reinen 2000-Umgebung kann der WINS-Namensdienst durch DDNS abgelöst werden, sofern nicht noch ältere Client-Server-Anwendungen den WINS-Dienst voraussetzen.
- Verbesserung der Sicherheit: Im Active Directory kann eine präzise Zugriffssteuerung nicht nur auf Objektebene, sondern sogar auf der Objekteigenschaftsebene festgelegt werden. Weiterhin können über Gruppenrichtlinien domänenweite Sicherheitsrichtlinien für die Benutzerkonten definiert werden.

1.9 Funktionsweise und Beschreibung des Active Directory

Nachdem Sie eben einen Einblick in die Funktionsweise des Verzeichnisdienstes sowie die Vorteile von Active Directory gegenüber Windows NT erhalten haben, werden hier die wesentlichen Komponenten und Schlagwörter des Active Directory wie Domänen, Strukturen, Replikation usw. vorgestellt.

1.9.1 Domänen und Domänencontroller

In einer Domäne werden im Gegensatz zur Arbeitsgruppe alle Konten und Ressourcen zentral verwaltet. Dies bedeutet, dass ein Benutzer mit einer einzigen Anmeldung an der Domäne automatisch Zugriff auf alle Ressourcen der kompletten Domäne erhält, für die er die entsprechenden Rechte besitzt. Die Anmeldung erfolgt ausschließlich am Domänencontroller der Domäne. Dort liegt die zentrale Datenbank, welche die Einträge zu den Benutzerkonten, Rechten, Ressourcen usw. enthält. Ein Domänencontroller besitzt keine lokale Sicherheitsdatenbank. In einer einzelnen Domäne können bis zu zwei Millionen Objekte gespeichert werden. Im SBS 2003-Netzwerk bildet der SBS 2003 den Domänencontroller.

Eine Windows Server 2003-Domäne kann mehrere gleichberechtigte Domänencontroller enthalten. Der SBS 2003 besitzt jedoch die Einschränkung, dass er der einzige Domänencontroller in der SBS 2003-Domäne ist. Diese Domänencontroller in einer Nicht-SBS 2003-Domäne gleichen automatisch ihre Datenbanken untereinander ab, so dass stets die aktuellen Informationen im Netzwerk zur Verfügung stehen. Dieser Vorgang wird als Replikation bezeichnet.

Mit der Installation und der Konfiguration des SBS 2003 wird gleichzeitig auch die Domäne selbst neu eingerichtet. Im Gegensatz zu einem Windows Server 2003 müssen Sie hier nicht den Installationsassistenten für das Active Directory durchführen. Da die SBS 2003-Domäne nur aus einer Domäne mit nur einem Domänencontroller ohne Vertrauensstellungen zu anderen Domänen bestehen kann, ist die Konfiguration des Active Directory wesentlich einfacher und verläuft automatisch im Hintergrund.

Ein Domänencontroller ist in seiner Umgebung für die Anmeldung und Authentifizierung der Benutzer sowie das Durchsuchen des Verzeichnisses nach Objekten zuständig. Er speichert sämtliche Daten des Active Directory.

Eine Domäne muss nicht identisch sein mit den physischen Grenzen eines Unternehmensstandorts. Es ist möglich, dass in einer Domäne Objekte aus mehreren physisch getrennten Standorten vorhanden sind.

Wenn kein Domänencontroller für einen Client verfügbar ist, so konnte unter Windows NT der Client nicht auf Netzwerkressourcen zugreifen. Diese Problematik wurde erkannt und ab Windows 2000 verbessert. Clients ab dem Betriebssystem Windows 2000 verwenden automatisch das Login-Caching.

Dabei wird bei jeder erfolgreichen Anmeldung an der Domäne auf dem Client das Login gecacht. Standardmäßig können bis zu zehn Einträge auf dem Client vorgehalten werden. Dieser Wert kann in den Sicherheitsrichtlinien modifiziert werden. Will sich dieser Client nun zu einem späteren Zeitpunkt erneut an der Domäne anmelden und kann dabei keine Verbindung zum Domänencontroller aufbauen, so kann er sich dennoch an der Domäne anmelden. Es werden aus dem Cache des Clients die Einstellungen von Rechten, Gruppenmitgliedschaft etc. des letzten erfolgreichen Anmeldens am Domänencontroller übernommen. Auch wenn diese Einträge auf dem Domänencontroller zwischenzeitlich geändert worden sind, sind die Einstellungen aus dem lokalen Cache für den Client gültig. Der Cache wird dann bei der nächsten erfolgreichen Verbindung zum Domänencontroller automatisch aktualisiert.

Innerhalb einer SBS 2003-Domäne sind die folgenden Computertypen vertreten: ein Domänencontroller, Clientcomputer und optional Mitgliedsserver, die als Datei- oder Druckerserver dienen können.

1.9.2 Domänen- und Gesamtstruktur

Strukturen sind eine hierarchische Anordnung von mehreren Windows 2000/2003-Domänen. Wie Sie ja bereits erfahren haben, können mit dem SBS 2003 keine Strukturen gebildet werden, da dieser lediglich eine einzelne Domäne bildet. Dennoch soll dieses Thema hier kurz angerissen werden.

Es gibt übergeordnete und untergeordnete Domänen. Im Rahmen der Strukturen wird zwischen einer *Domänenstruktur* (*Tree*) und einer *Gesamtstruktur* (*Forest*) unterschieden. Die Domänenstruktur wird manchmal auch nur als Struktur bezeichnet.

In einer *Domänenstruktur* haben alle Domänen einen fortlaufenden DNS-Namensraum. Der Namensaufbau ist hierarchisch. Jede Domäne wird durch einen eindeutigen DNS-Namen bezeichnet.

In einer Domänenstruktur benutzen alle Domänen dasselbe Active Directory-Schema, dieselben Replikationsinformationen und denselben globalen Katalog.

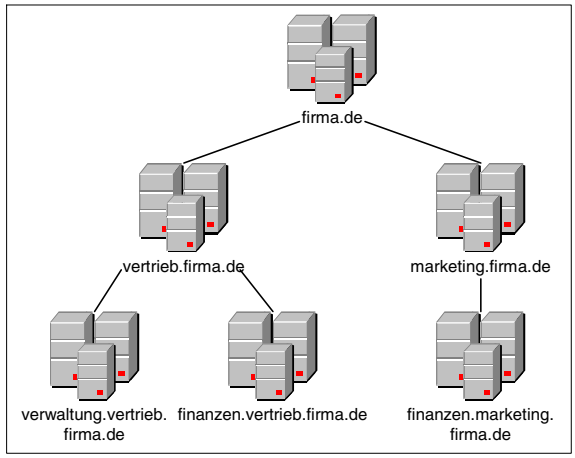


Abbildung 1.2: Übersicht über eine Domänenstruktur

In einer Struktur erbt eine untergeordnete Domäne den Namen der übergeordneten Domäne. Vor diesen wird der relative Name der untergeordneten Domäne gestellt. Beispielsweise erbt also die Domäne *vertrieb.firma.de* den Namen der übergeordneten Domäne *firma.de,* und vor diesen wird der relative Name *vertrieb* gesetzt (siehe Abbildung 1.2). Dabei spricht man vom fortlaufenden oder zusammenhängenden Namensraum.

Eine Domänenstruktur ist gleichzeitig auch immer eine komplette Gesamtstruktur.

Bei einer *Gesamtstruktur* handelt es sich um eine hierarchische Anordnung entweder nur einer Domänenstruktur oder mehrerer getrennter, unabhängiger Domänenstrukturen Selbst eine einzelne Domäne wie *firma.de* ohne weitere untergeordnete Domänen bildet eine in sich geschlossene Gesamtstruktur.

Innerhalb aller Domänen einer Gesamtstruktur werden dasselbe Active Directory-Schema, dieselben Replikationsinformationen sowie derselbe globale Katalog verwendet. Der Namensraum ist nur innerhalb der Domänenstrukturen zusammenhängend. In der Abbildung bilden die beiden Strukturen *firma.de* und *filiale.de* getrennte Domänenstrukturen innerhalb der Gesamtstruktur. Nur innerhalb der beiden Strukturen ist der Namensraum fortlaufend. Die erste Domäne in einer Gesamtstruktur heißt auch Stammdomäne der Gesamtstruktur, hier also *firma.de*.

Über den Installationsassistenten für Active Directory können Sie bestimmen, an welcher Hierarchieebene in der Gesamtstruktur die neue Domäne erstellt werden soll. Dabei haben Sie folgende Möglichkeiten:

- erste Domäne in einer Gesamtstruktur, z.B. *firma.de*
- erste Domäne einer neuen Domänenstruktur, z.B. *filiale.de*
- untergeordnete Domäne in bestehender Domänenstruktur, also alle anderen den beiden Domänen untergeordnete Domänen

Nach dem Einrichten des ersten Domänencontrollers einer der eben genannten Domänenarten können Sie für diese Domäne weitere Domänencontroller installieren.

Weiterhin werden zwischen allen Windows 2000-Domänen innerhalb der Gesamtstruktur automatisch gegenseitige Vertrauensstellungen eingerichtet. Dies gilt nur für Windows 2000-Domänen. Wenn Sie noch Windows NT-Domänen innerhalb der Gesamtstruktur verwenden, müssen die Vertrauensstellungen zu diesen manuell konfiguriert werden. Die automatische Einrichtung bezieht sich sowohl auf die Vertrauensstellung zwischen übergeordneten und untergeordneten Domänen als auch zwischen der Stammdomäne der Gesamtstruktur und den ersten Domänen neuer Domänenstrukturen.

1.9.3 Der globale Katalog

Der globale Katalog ist zuständig für die Suche nach Objekten im Verzeichnis. Er wird automatisch auf dem ersten Domänencontroller der Stammdomäne der Gesamtstruktur erstellt. Damit wird dieser spezielle Domänencontroller auch globaler Katalogserver genannt. Im SBS 2003-Umfeld stellt der SBS 2003 gleichzeitig auch den globalen Katalogserver dar.

Im globalen Katalog werden zwei verschiedene Replikate der Objektattribute gespeichert. Zum einen enthält der Katalogserver ein vollständiges Replikat aller Objektattribute im gesamten Verzeichnis und zum anderen ein Teilreplikat der Objektattribute, die sich nur im Verzeichnis in jeder Domäne der Gesamtstruktur befinden. Das Teilreplikat enthält zwar alle Objekte, aber nur eine begrenzte Anzahl der Attribute. Über dieses Teilreplikat werden die Suchanfragen zu Objekten im Verzeichnis abgewickelt. Es enthält nur die Attribute der Objekte, die am häufigsten bei Suchanfragen benötigt werden – dazu zählen beispielsweise Benutzernamen – oder die notwendig sind, um das vollständige Replikat des Objektes zu finden. Um die Sicherheit beim Zugriff auf die Objekte über den globalen Katalog zu gewährleisten, erben die Objekte die Zugriffsrechte ihrer Quelldomänen.

Bei einem Objekt sind die Informationen des definierten Namens ausreichend, um den Pfad zum vollständigen Replikat dieses Objektes zu finden. In vielen Fällen ist dem Benutzer aber nicht der vollständige definierte Name bekannt. Über den globalen Katalog wird es ihm ermöglicht, dass er das gewünschte Objekt dennoch findet, wenn er nur einige ihm bekannte Attribute für die Suche angibt. Es ist also nicht erforderlich, dass der Benutzer die genaue Lage des Objekts innerhalb der Gesamtstruktur kennen muss.

Deshalb ist es auch wichtig, bei der Erstellung von Objekten möglichst viele Eigenschaften festzulegen, um die Effektivität des globalen Katalogs optimal nutzen zu können.

Durch die Verwendung des globalen Katalogs wird der Netzwerkverkehr stark minimiert. Da im Katalog Informationen zu allen Objekten in allen Domänen der Gesamtstruktur enthalten sind, kann eine Suchanfrage innerhalb der Domäne bearbeitet werden, in welcher der Benutzer, der das Objekt sucht, angemeldet ist. Damit entfällt eine Suche und damit auch der Netzwerkverkehr über Domänengrenzen hinweg.

Auch bei der Anmeldung von Benutzern an der Domäne spielt der globale Katalogserver eine wichtige Rolle. Dieser Server stellt dem Domänencontroller Informationen über das Benutzerkonto zur Verfügung. Beim Anmelden des Clients wird eine Liste generiert, die alle Gruppen enthält, in denen der Client Mitglied ist. Dieses Feature wird jedoch nur in Multidomänenumgebungen genutzt, in denen der Client Mitglied in mehreren Gruppen in mehreren Domänen sein kann. Die globalen Katalogserver enthalten Mitgliedschaftslisten aller universellen Sicherheitsgruppen. Diese Listen werden benutzt, wenn Clients oder Server die Mitgliedschaft in den Sicherheitsgruppen prüfen müssen.

Eine weitere Funktion kommt dem globalen Katalogserver zu, wenn Sie in Ihrer Umgebung Microsoft Exchange Server 2000 oder 2003 einsetzen. Die Katalogserver sind zuständig für das Nachschlagen der Adressbucheinträge und das Auflösen von E-Mailadressen für Outlook-Clients ab der Version Outlook 98 SP2. Ältere E-Mail-Clients benutzen dafür den Exchange-Server selbst, der dann seinerseits den Zugriff auf einen Katalogserver benötigt.

1.9.4 Standorte

Standorte strukturieren wie Domänen das Netzwerk. Die Domänen spiegeln dabei die logische Struktur des Unternehmens wider, während Standorte die physische Struktur widerspiegeln. Des Weiteren dienen auch Organisationseinheiten der logischen Strukturierung des Netzwerks.

Ein Standort entspricht einer Gruppe von Computern, die zu einem bestimmten IP-Subnetz gehören. Damit gelten diese Computer untereinander als gut verbunden. Die Computer an einem Standort können auch verschiedenen IP-Subnetzen angehören. Allerdings muss dann auch zwischen diesen eine schnelle Verbindung sichergestellt sein. Diese schnelle Verbindung ist erforderlich, da innerhalb eines Standorts die Replikation sowie Ressourcenabfragen aus dem Active Directory einen nicht unerheblichen Teil der Netzwerkbandbreite in Anspruch nehmen. Deshalb ist es sinnvoller, für WANs mehrere Standorte zu konfigurieren.

Für das Verhältnis zwischen Standorten und Domänen gelten die folgenden Punkte: Eine Domäne kann mehrere Standorte enthalten (siehe Abbildung 1.3), und umgekehrt kann ein Standort auch mehrere Domänen enthalten. Daraus ergibt sich, dass keine Übereinstimmung zwischen Standortgrenzen und dem Namensraum der Domänen bestehen muss. Im SBS 2003-Umfeld können Sie also für die SBS-Domäne mehrere Standorte konfigurieren.

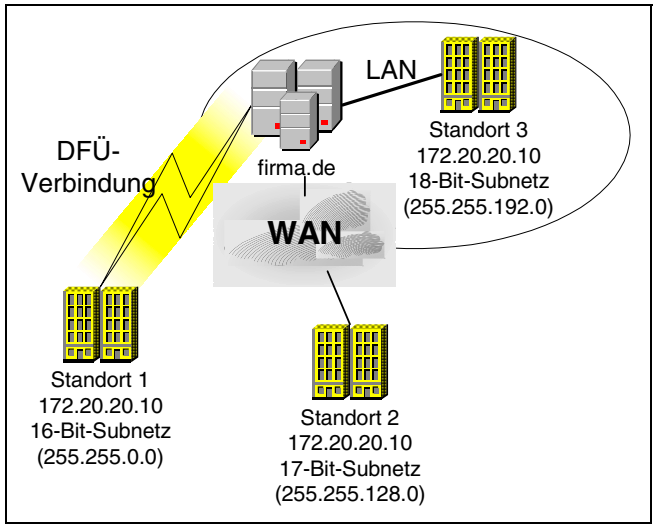


Abbildung 1.3: Eine Domäne mit mehreren Standorten

In diesem Modell verfügt eine Domäne über mehrere Standorte. Jeder der drei Standorte hat seinen eigenen Subnetzbereich. Die Computer der Standorte 1 und 2 sind nur über langsame Verbindungen (DFÜ bzw. WAN) mit der Domäne verbunden. Deshalb wurde für sie jeweils ein eigener Standort eingerichtet. Der dritte Standort umfasst die Computer eines Subnetzes, die über eine schnelle LAN-Verbindung mit der Domäne verbunden sind. Die Computer aller Standorte sind Mitglieder der Domäne *firma.de*.

In diesem Beispiel gibt es nur einen Standort mit einem zusammenhängenden 16-Bit-Subnetz. Zu diesem Standort gehören Computer, die ihrer logischen Struktur nach der Domäne *firma.de* oder der Domäne *filiale.de* angehören. Der Standort sagt also nichts über die logische Zugehörigkeit der Computer aus.

Wenn Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE öffnen, werden Sie feststellen, dass dort nicht die Computer, die zu einem bestimmten Standort gehören, aufgelistet werden. Das Durchsuchen einer Domäne gibt nur die Computer in ihrer logischen Struktur an. Die einzelnen Computer finden Sie nur unter den Domänen und Organisationseinheiten. Unter ACTIVE DIRECTORY-STANDORTE finden Sie nur die Elemente, die für die Konfiguration der Replikation zwischen den Standorten zuständig sind.

1.9.5 Organisationseinheiten

Organisationseinheiten sind neben den Domäne die zweite Einheit zur logischen Gruppierung von Netzwerkressourcen.

Die Mitglieder der Organisationseinheiten sind alle Mitglieder der Domäne, welche die Organisationseinheit(en) beinhaltet. Eine Organisationseinheit verfügt im Gegensatz zu einem Standort nicht über eigene Domänencontroller.

Die Organisationseinheiten werden statt der Ressourcendomänen in den Windows NT-Domänenmodellen verwendet. In einer Organisationseinheit werden Objekte in Gruppen gegliedert. Diese Gruppen können die Unternehmensstruktur widerspiegeln. Eine Organisationseinheit kann Objekte wie Computer, Kontakte, Gruppen, weitere Organisationseinheiten, Drucker, Benutzer und freigegebene Ordner enthalten. Durch die Übersichtlichkeit einer geringeren Anzahl von Objekten innerhalb einer Organisationseinheit werden deren Verwaltung und Anzeige erleichtert.

An eine Organisationseinheit können administrative Aufgaben delegiert werden. Die Berechtigungen, die ein Benutzer für die Durchführung seiner administrativen Aufgaben benötigt, können entweder für eine separate Organisationseinheit erteilt werden oder für eine übergeordnete Organisationseinheit, welche die Berechtigungen an die untergeordneten weitervererbt. Damit ist es möglich, die Administration der Domäne an mehrere Administratoren zu verteilen. Sie können so für die Organisationseinheit spezielle Verwaltungsaufgaben erledigen.

Standardmäßig sind keine vorkonfigurierten Organisationseinheiten in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER enthalten. Dies würde auch wenig Sinn machen, da ja gerade durch die Individualität der Organisationseinheiten Ihr Unternehmensnetzwerk strukturiert werden soll.

Abbildung 1.4 gibt einen Überblick über Organisationseinheiten innerhalb einer Domäne sowie die verschiedenen Objekte, die in jeder Organisationseinheit enthalten sein können.

Die Abbildung zeigt eine Domäne mit insgesamt vier Organisationseinheiten. Die beiden Organisationseinheiten Verwaltung und Marketing sind dabei auf einer Hierarchieebene, die Organisationseinheit Verwaltung enthält als untergeordnete Objekte die Organisationseinheiten Personal sowie Buchhaltung.

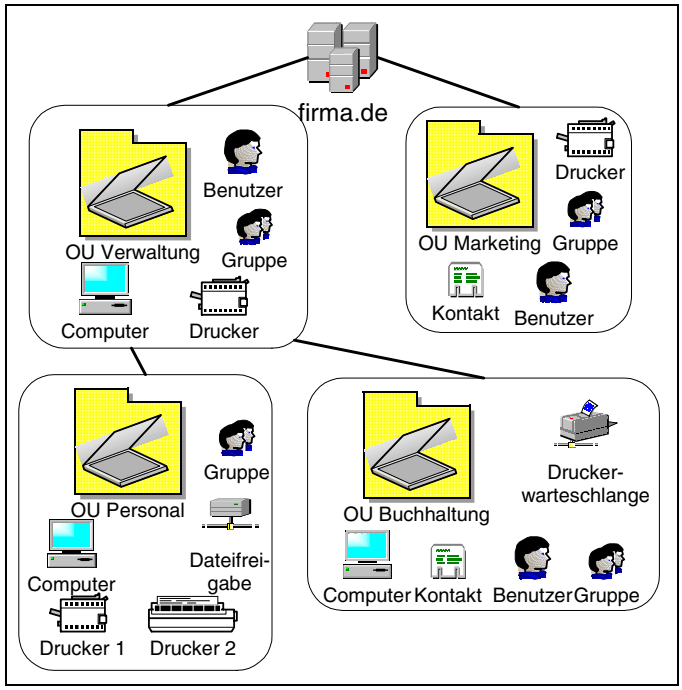


Abbildung 1.4: Die Struktur einer Organisationseinheit

Jede einzelne Organisationseinheit hat ihre eigene unabhängige Struktur und ihre eigenen Ressourcen. Objekte, die in einer Organisationseinheit vorhanden sind, müssen nicht in allen Organisationseinheiten der Domäne vorkommen, und umgekehrt müssen auch nicht alle Objekte in einer Organisationseinheit eingebunden sein.

1.9.6 Active Directory-Objekte und Schema

Im Active Directory werden sämtliche Ressourcen als Objekte gespeichert. Objekte können Computer, Konten, Drucker, Kontakte usw. sein. Jedes Objekt besteht aus einem bestimmten Satz von Eigenschaften bzw. Attributen, die für dieses Objekt spezifisch sind. So umfasst z.B. ein Domänencontroller-Objekt die folgenden Attribute unter den allgemeinen Eigenschaften: Computername, DNS-Name, Funktion und Beschreibung. Diese Eigenschaften dienen Active Directory als Vorlage für die Objekte. Diese Vorlage muss dem Verzeichnisdienst zum Speichern der Objekte bekannt sein.

Das Active Directory-Schema enthält einen vorgegebenen Satz an Definitionen für die Objekte und Informationen im Active Directory. Es gibt zwei Arten von Definitionen, nämlich Attribute und Klassen. Diese werden auch Schemaobjekte oder Metadaten genannt. Das Active Directory-Schema ist für alle Domänen innerhalb einer Gesamtstruktur verbindlich dasselbe. Die Informationen des Schemas werden automatisch repliziert.

Attribute

Ein Attribut wird nur einmalig im Schema definiert und kann von beliebigen Klassen genutzt werden. So finden Sie z.B. in diversen Objekten, wie etwa Computer, Konto usw., das Attribut „Beschreibung“. In jeder dieser Klassen erfüllt das Attribut den allgemeinen Zweck, das entsprechende Objekt näher zu erläutern, aber in jeder Klasse sieht die Beschreibung für das spezielle Objekt verschieden aus.

Klassen

Die Klassen bestimmen, welche Arten von Objekten im Active Directory erstellt werden können, so z.B. Computer, Konten usw. Jede Klasse beinhaltet einen bestimmten Satz aller möglichen Attribute. Wenn Sie ein Objekt neu erstellen, erhalten die Attribute die Werte, die das Objekt konkret beschreiben. Die Klassen werden auch als Objektklassen bezeichnet.

Unter Windows Server 2000 und 2003 haben Sie die Möglichkeit, das Schema individuell nach Ihren Bedürfnissen anzupassen.

Das Active Directory-Schema ist objektorientiert. Es wird im Verzeichnis als ein Satz von Objektinstanzen gespeichert. Dies ist der Unterschied zu anderen Verzeichnisdiensten, bei denen das Schema als Textdatei gespeichert wird, die beim Start des Verzeichnisdienstes ausgelesen wird. Aus den gespeicherten Objekten im Active Directory können Applikationen beispielsweise auslesen, welche Objekte und Eigenschaften verfügbar sind.

Das Active Directory-Schema kann dynamisch aktualisiert werden. Beispielsweise kann eine Applikation dem Schema neue Klassen und Attribute hinzufügen und diese neu hinzugefügten Metadaten sofort benutzen. Eine Änderung des Schemas wird durch das Erstellen oder Modifizieren der im Verzeichnis gespeicherten Metadaten erreicht. Auch die Metadaten werden wie jedes andere Objekt im Active Directory durch Zugriffssteuerungslisten (Access Control Lists, ACLs) geschützt So wird sichergestellt, dass nur autorisierte Benutzer das Schema ändern können.

1.9.7 Gruppenrichtlinien

Gruppenrichtlinien sind der zentrale Bestandteil des Active Directory für die effektive Verwaltung von Berechtigungen. Die Gruppenrichtlinien sind eine Weiterentwicklung der Systemrichtlinien unter Windows NT.

Gruppenrichtlinien können auf den Ebenen von Standorten, Domänen und Organisationseinheiten angewendet werden. Ein Gruppenrichtlinienobjekt gibt für einen Benutzer eine Ansammlung von Regeln des Unternehmens in Bezug auf verfügbare Ressourcen, Zugriffsrechte und Konfiguration der Ressourcen wieder. Über eine Gruppenrichtlinie werden die Desktop-Einstellungen eines Benutzers konfiguriert. Sie können ihm über diese Richtlinie beispielsweise Software zuweisen oder bestimmen, welche Objekte er im Startmenü sehen darf und welche nicht. Unter Windows NT stand Ihnen – wenn auch nicht in diesem Umfang – dafür die Systemrichtlinie zur Verfügung. Gruppenrichtlinien sind ein Bestandteil von IntelliMirror. IntelliMirror ist der Oberbegriff für die Steuerung der Client-Desktops unter Windows 2000/XP. Für jeden Client bestimmen Sie Richtlinien,

die auf seiner Funktion, seinem Standort und seinen Gruppenmitgliedschaften basieren. Der Benutzer erhält überall seine in den Gruppenrichtlinien definierten Einstellungen, egal an welchem Computer er sich anmeldet. IntelliMirror umfasst die folgenden Funktionen: Verwaltung von Benutzerdaten und -einstellungen sowie Zuweisung, Installation und Konfiguration von Software.

Die Verwaltung und Konfiguration der Gruppenrichtlinien wird ausführlich in Kapitel 8.6 besprochen.

1.9.8 Replikation

Replikation bedeutet das Austauschen von Verzeichnisinformationen zwischen mehreren Domänencontrollern. Sämtliche Domänencontroller einer Domäne müssen immer die aktuellen Verzeichnisinformationen zur Verfügung haben. Wenn Sie an einem beliebigen Domänencontroller der Domäne Änderungen vornehmen, so müssen diese schnellstmöglich auch den anderen Domänencontrollern verfügbar gemacht werden. Bei der Replikation werden die geänderten Verzeichnisinformationen von dem einen Domänencontroller an alle anderen gesendet.

1.9.9 Features von ADSI

Dieses Kapitel zeigt Ihnen kurz einige der wichtigsten Features von ADSI (Active Directory Services Interface). ADSI bietet Ihnen eine Schnittstelle für eigene Anwendungen in zahlreichen Betriebssystemen zum Zugriff auf verschiedene Verzeichnisdienste.

- ADSI ermöglicht Ihnen einen leichten Zugang zu Verzeichnisdiensten über das Component Object Model (COM). Die Applikationen sind an keine bestimmte Programmiersprache gebunden und können z.B. in Visual Basic, C/C++ oder Java geschrieben werden.
- ADSI arbeitet verzeichnisdienstunabhängig. Sie können Applikationen entwickeln, ohne die verschiedenen anbieterspezifischen Verzeichnis-APIs kennen zu müssen. Gerade administrative Applikationen sind nicht fest an einen bestimmten Verzeichnisdienst gebunden.
- Sie können jede beliebige automatisierungskompatible Skriptsprache (z.B. VB Script, REXX oder Perl) benutzen, um Applikationen für den Verzeichnisdienst zu entwickeln.
- ADSI kann von Verzeichnisdienstanbietern, Softwareentwicklern und Administratoren durch das Hinzufügen neuer Objekte und Funktionen erweitert werden. Dies ist wichtig, wenn Ihr Verzeichnis sehr spezielle Bedingungen erfüllen muss.
- ADSI bietet ein OLE-Datenbank-Interface, so dass auch Datenbankprogrammierer rasch über dieses Interface produktiv arbeiten können.

2 Die Installation des SBS 2003

Dieses Kapitel beschreibt die Vorbereitung der Installation des SBS 2003 sowie die Installation selbst und die anschließende Grundkonfiguration. An dieser Stelle wird zunächst von einer Neuinstallation ausgegangen. Eine Migration von der Version SBS 2000 oder 4.5 sowie Update-Szenarien werden in Kapitel 3 beschrieben.

2.1 Bestimmen der Netzwerkstruktur

Bevor Sie den SBS 2003 auf einem Server installieren bzw. einen OEM-seitig bereits installierten Server zum Netzwerk hinzufügen können, müssen Sie zunächst die gegebene Netzwerkstruktur analysieren, um zu bestimmen, an welcher Stelle der SBS eingefügt werden muss.

Die beiden gängigsten Netzwerkmodelle sind ein *Peer-to-Peer-Netzwerk* und ein *serverbasiertes Netzwerk*. Sofern Sie noch über kein Netzwerk verfügen, folgen Sie den Schritten in Kapitel 2.4, um den SBS 2003 zu implementieren.

In einem *Peer-to-Peer-Netzwerk* sind die Computer für den Datenaustausch und sonstige Kommunikation untereinander verbunden. Die Verbindung kann entweder über einen Switch bzw. Hub oder aber auch über eine Hardware-Firewall für die Internetverbindung realisiert sein. Eine Internetverbindung kann auch von mehreren Computern gemeinsam auf einem Computer benutzt werden.

In einem *serverbasierten Netzwerk* hingegen befindet sich (mindestens) ein Server. Über diesen Server, der meistens ein Domänencontroller ist, wird für die Clients die Internetverbindung bereitgestellt, er bildet den zentralen Datenspeicher für das Netzwerk und dient als Druckserver. Zum Schutz der Internetverbindung wird entweder eine Hardware-Firewall eingesetzt, oder auf dem Server läuft eine Software-Firewall. Im Gegensatz zum Peer-to-Peer-Netzwerk ist der Server hier als Domänencontroller die zentrale übergeordnete Instanz zur Verwaltung von Benutzerkonten, Clientcomputern und weiteren Netzwerkressourcen. Zum Zugriff auf die Ressourcen müssen sich die Clients am Server anmelden und verifizieren.

Abhängig davon, ob es sich bei Ihrem Netzwerk um ein Peer-to-Peer-Netzwerk oder ein serverbasiertes Netzwerk handelt, unterscheiden sich die Implementierungsschritte für den SBS 2003.

2.2 Den SBS zum Peer-to-Peer-Netzwerk hinzufügen

Dieses Kapitel beschreibt die Implementierung des SBS zu einem Peer-to-Peer-Netzwerk. Dabei ist zu unterscheiden, ob sich in dem Netzwerk eine Hardware-Firewall befindet oder nicht.

2.2.1 Peer-to-Peer-Netzwerk mit Hardware-Firewall

Beim Hinzufügen des SBS zu einem Netzwerk mit einer Hardware-Firewall müssen Sie sicherstellen, dass diese eingeschaltet bleibt, bis Sie den SBS hinzugefügt haben.

Der SBS wird über seine Netzwerkkarte mit dem LAN sowie dem Internet verbunden. Zur Herstellung der Internetverbindung wird z.B. ein Router als Standard-Gateway verwendet, der seine IP-Adresse vom ISP (Internet Service Provider) erhält. Dabei kann es sich um eine vom DHCP-Server des ISP zugewiesene dynamische Adresse oder um eine statische IP-Adresse handeln. Auf diesem Gerät, das die Internetverbindung zur Verfügung stellt, müssen auch der für die Verbindung gültige Benutzername sowie das Passwort (bei PPPoE(Point-to-Point Protocol over Ethernet)-Verbindungen) eingetragen werden. Dies gilt auch, wenn das Gateway-Gerät UPnP unterstützt.

Die interne Schnittstelle des Gateways muss über eine IP-Adresse aus demselben Bereich wie die Netzwerkkarte des SBS verfügen. Ist das Gateway-Gerät gleichzeitig auch als DHCP-Server konfiguriert, wird Ihnen während des SBS-Setups eine IP-Adresse aus dem Bereich der internen Gateway-Schnittstelle vorgeschlagen (siehe Abbildung 2.9). Ist das Gateway nicht als DHCP-Server konfiguriert, schlägt das Setup Ihnen auch eine IP-Adresse vor.

Auf diesem Gateway muss zwangsläufig die Firewall-Funktion ausgeführt werden, bzw. eine Hardware-Firewall muss vorhanden sein. In diesem Szenario können Sie jedoch nicht die Firewall-Funktion des SBS 2003 nutzen, da der SBS nicht das Gateway darstellt. Dies wird nur möglich, wenn Sie in den SBS eine zweite Netzwerkkarte einbauen. Ist die eingesetzte Hardware-Firewall UPnP(Universal Plug & Play)-fähig, kann diese im Rahmen der Internetkonfiguration automatisch konfiguriert werden. Für eine manuelle Konfiguration der Firewall sei auf Appendix A verwiesen.

2.2.2 Peer-to-Peer-Netzwerk ohne Hardware-Firewall

In dieser Konstellation ist zu unterscheiden, ob Sie für den Internetzugang eine Einwahlverbindung (Analogmodem, ISDN) oder eine Breitbandverbindung (z.B. DSL) benutzen.

Einwahlverbindung

Sofern Sie eine Einwahlverbindung benutzen (siehe Abbildung 2.1), müssen Sie den SBS über seine Netzwerkkarte mit dem LAN verbinden. Zur anderen Seite wird der SBS mit dem Modem oder dem ISDN-Terminaladapter verbunden. Der SBS wird in dieser Konstellation zum Standard-Gateway. Zum Schutz der Internetverbindung wird die integrierte Firewall des SBS konfiguriert.

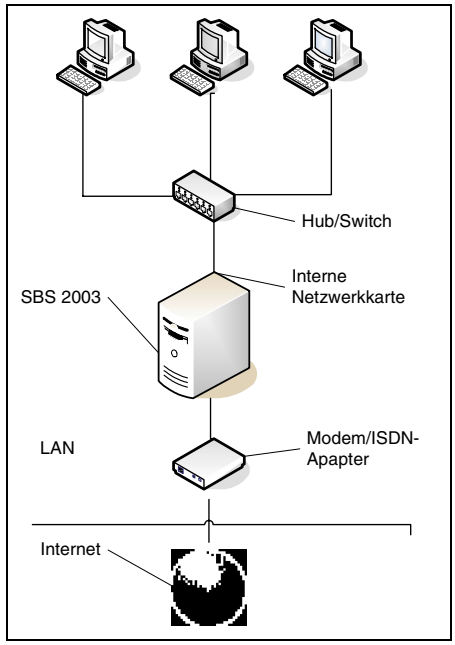


Abbildung 2.1:
SBS ohne Hardware-Firewall mit Wahlverbindung

Breitbandverbindung

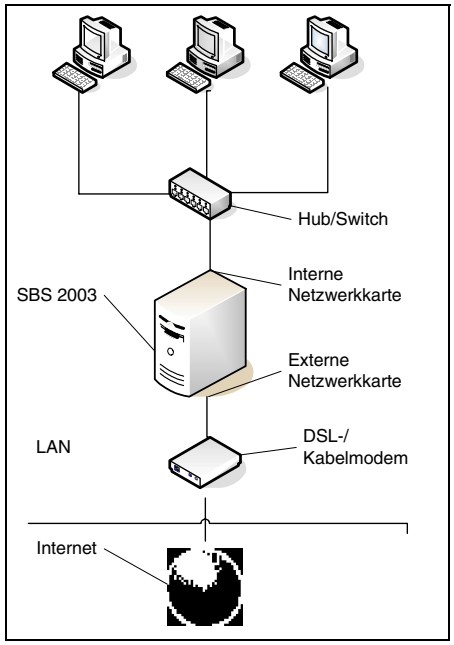


Abbildung 2.2:
SBS ohne Hardware-Firewall mit Breitband-verbindung

Bei einer Breitbandverbindung wie DSL ohne Firewall im LAN müssen Sie den SBS 2003 mit zwei Netzwerkkarten ausrüsten (siehe Abbildung 2.2). Sein interner Netzwerkadapter wird mit einem Switch oder Hub verbunden, an den die Clients des LAN angeschlossen sind. Der zweite Netzwerkadapter wird mit dem DSL-Modem verbunden. In diesem Modell aktivieren Sie zum Schutz der Internetverbindung die Firewall auf dem SBS 2003. Der SBS wird in dieser Konstellation zum Standard-Gateway. Die Benutzerinformationen für den Internetzugang werden während der Konfiguration der Internetverbindung abgefragt.

2.3 Den SBS zum serverbasierten Netzwerk hinzufügen

Bei diesem Modell gibt es verschiedene Konstellationen, die auf das bestehende Netzwerkmodell zutreffen können.

- Sofern auf dem bestehenden Server Windows Server 2000, Windows Server 2003 oder SBS 2000 ausgeführt werden, können Sie den Server updaten, so dass alle vorhandenen Daten und Einstellungen erhalten bleiben. Die Netzwerkkonfiguration des Servers ist in diesem Fall bereits vorhanden und wird vom SBS 2003 übernommen.
- Wird auf dem vorhandenen Server Windows NT 4.0 Server oder SBS 4.5 ausgeführt, müssen Sie eine Migration durchführen. In diesem Fall erfolgt eine Neuinstallation auf einem neuen System. Die bestehenden Daten und Einstellungen werden nach der Neuinstallation vom alten auf das neue System transferiert. Eine Migration ist auch von einem bestehenden Windows Server 2000/2003 und SBS 2000 möglich.
- Ist in dem Netzwerkmodell bereits ein Server vorhanden, der nicht als Domänencontroller eingerichtet ist und auch nicht zum Domänencontroller werden soll, so müssen Sie den SBS neu installieren und als Domänencontroller konfigurieren. Der bestehende Server kann dem SBS-Netzwerk anschließend als Mitgliedserver hinzugefügt werden.

2.4 Die Neuinstallation des SBS 2003

Wie bereits erwähnt, ist der SBS 2003 auf einer breiten Palette von OEM-Produkten bereits vorinstalliert. In diesem Fall können Sie dieses Kapitel überspringen und in Kapitel Abbildung 2.7 weiterlesen.

Für die Installation des SBS 2003 sind in der Standardversion drei Installations-CDs erforderlich. CD 1 enthält den Windows Server 2003 for Small Business, CD 2 den Exchange Server und CD 3 die SharePoint Services. Um die Premium-Version zu installieren, spielen Sie zunächst die drei CDs auf und danach die CD mit dem Namen Small Business Server 2003 Premium Technologies. Zum Lieferumfang beider Versionen gehört ferner die CD Office Outlook 2003 und zur Premium-Version die CD Office FrontPage 2003.

Der komplette Installations- und Konfigurationsprozess des SBS 2003 lässt sich in drei große Abschnitte gliedern. Dabei handelt es sich um:

1. Installation und Konfiguration des Windows Small Business Server
2. Installation weiterer Serverkomponenten
3. Aufgabenliste zur abschließenden Konfiguration

Anhand dieser drei Aufgabenbereiche gliedern sich auch die drei Kapitel Abbildung 2.5 bis Abbildung 2.7.

2.5 Installation und Grundkonfiguration

Vor der Installation des SBS 2003 sollten Sie sicherstellen, dass die verwendete Hardware kompatibel mit dem Windows Server 2003 ist. Um dies zu ermitteln, konsultieren Sie die Hardware Compatibility List (HCL).

Während der Installation des Windows Server 2003 wird die automatische Hardwareerkennung durchgeführt. Dabei kann es zu Problemen mit einer angeschlossenen USV kommen. Es besteht die Gefahr, dass diese in den Batteriemodus umschaltet und das Setup fehlschlägt. Um dieses Problem zu verhindern, sollten Sie vor Beginn der Installation die USV vom Server trennen und erst nach Abschluss der Installation wieder verbinden.

Sobald Sie die erste Installations-CD des SBS 2003 eingelegt haben, erscheint dasselbe Setup, das Sie von einem herkömmlichen Windows Server 2003 kennen. Dieser Installationsvorgang dauert ca. 40 Minuten. Erst bei der ersten Anmeldung am System sehen Sie im Startfenster das Logo und den Schriftzug Windows Server 2003 for Small Business Server. Nachdem Sie sich am System angemeldet haben, werden noch einige Installationskomponenten kopiert und geladen. Sie sehen die entsprechenden Fortschrittsbalken. Ist dieser Vorgang beendet, können Sie mit der Grundkonfiguration des SBS 2003 beginnen. Dieser Konfigurations- und Installationsvorgang dauert ca. 30 Minuten.

Soll der Konfigurationsvorgang erst später fortgesetzt werden, kann auch später wieder die erste Installations-CD eingelegt und nach dem Start dieser die Option SMALL BUSINESS SERVER 2003 JETZT INSTALLIEREN ausgewählt werden.

Während der Installation werden an vielen Stellen Standardwerte vorgegeben. Diese sind in der Regel für kleine und mittlere Unternehmen passend. Möchten Sie die vorgegebenen Werte ändern, klicken Sie jeweils auf die Schaltfläche WEITERE INFORMATIONEN.

Bei sämtlichen Pfaden im Startmenü des SBS 2003 wird davon ausgegangen, dass das klassische Startmenü aktiviert ist. Ist in Ihrer Umgebung das modifizierte Startmenü aktiviert, können die angegebenen Pfade gegebenenfalls leicht voneinander abweichen.

1. Als Erstes sehen Sie eine Willkommensmeldung zum Setup (siehe Abbildung 2.3). Sie erfahren hier, dass nun folgende Schritte nacheinander durchgeführt werden:

- Konfiguration des Betriebssystems
- Installation weiterer Serveranwendungen wie z.B. Exchange 2003
- Abarbeiten einer Aufgabenliste, welche die Konfiguration des SBS 2003 abschließt

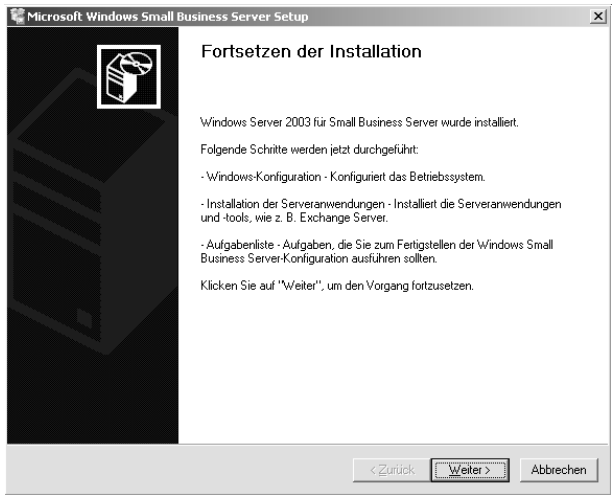


Abbildung 2.3: Fortsetzen der Installation nach Abschluss der Installation des Windows Server 2003 for Small Business

Klicken Sie hier auf WEITER.

2. Sie erhalten dann das Fenster SETUP-ANFORDERUNGEN. In dem Textfeld ANFORDERUNGEN sehen Sie Hinweise auf Probleme, die im Zuge der Installation auftreten könnten (siehe Abbildung 2.4).

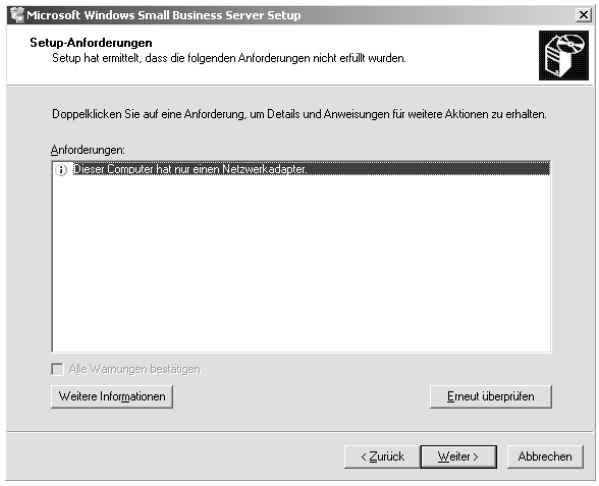


Abbildung 2.4: Übersicht über mögliche Probleme bei den Setup-Anforderungen

Die Probleme werden in drei verschiedene Kategorien unterteilt. Sobald Sie eine aufgelistete Anforderung doppelklicken, erhalten Sie weitere Hinweise zu dem Problem.

Kategorie	Beschreibung
Information	Die unter dieser Kategorie aufgelisteten Hinweise sollten Sie vor Beginn der Konfiguration zur Kenntnis genommen haben. Die hier angegebenen Hinweise müssen nicht zwangsweise zu Problemen bei der Installation führen.
Warnung	Hinweise dieser Kategorie geben an, dass es bei der Installation zu Problemen kommen kann.
Blockierung	Hinweise in dieser Kategorie geben an, dass die Installation aufgrund des genannten Problems nicht fortgesetzt werden kann. Hier gelistete Probleme müssen also zunächst beseitigt werden, bevor die Installation durchgeführt werden kann.

Tabelle 2.1: Kategorien von Problemen, die während der Installation auftreten könnten

Dieses Fenster erscheint nur, wenn es Hinweise in einer der drei eben genannten Formen gibt. Klicken Sie dann auf WEITER.

3. Geben Sie nun im Fenster FIRMENINFORMATIONEN die entsprechenden Informationen (Telefon- und Faxnummer sowie die Adresse) an (siehe Abbildung 2.5). Diese Informationen verwendet der SBS Server für die Konfiguration seiner Serverkomponenten. Klicken Sie dann auf WEITER.

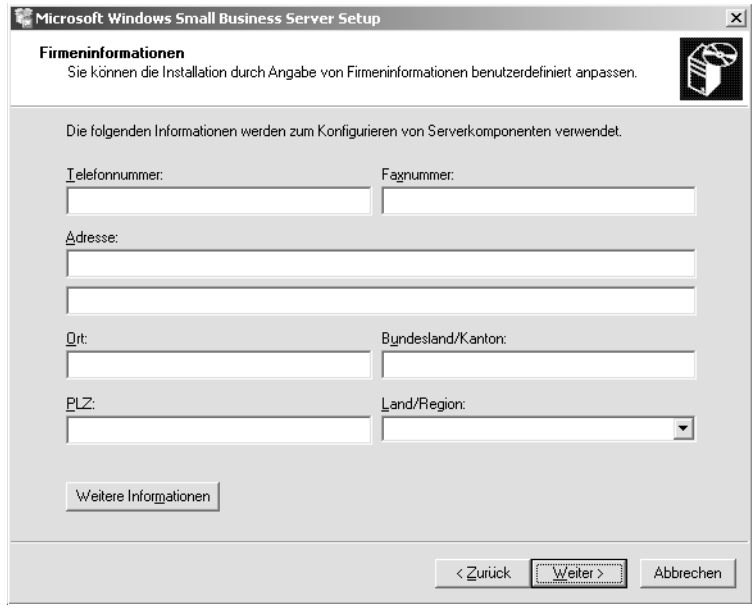


Abbildung 2.5: Die Eingabe der Firmeninformationen

4. Als Nächstes erfolgt im Fenster INTERNE DOMÄNENINFORMATIONEN die DNS-Konfiguration des Servers (siehe Abbildung 2.6). Geben Sie in den entsprechenden Feldern den DNS-Namen der Domäne, den NETBIOS-Namen der Domäne sowie den Namen des Servers an und klicken dann auf WEITER.

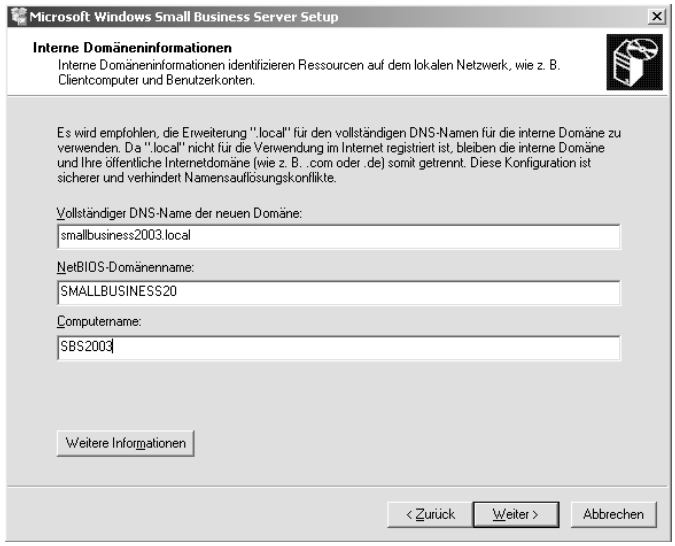


Abbildung 2.6: Festlegen des DNS- und NETBIOS-Domänennamens für die SBS 2003-Domäne

Der angegebene DNS-Domänenname darf die folgenden Zeichen besitzen:

- Die Buchstaben A–Z und a–z
- Die Zahlen 0–9
- Das Zeichen Bindestrich (-)

Der angegebene NETBIOS-Domänenname entspricht standardmäßig immer dem Namen der DNS-Domäne. Es ist jedoch möglich, einen vom DNS-Namen abweichenden NETBIOS-Domänennamen zu verwenden.

Der angegebene Computername darf die folgenden Zeichen besitzen:

- Die Buchstaben A–Z und a–z
- Die Zahlen 0–9
- Das Zeichen Bindestrich (–)

Standardmäßig wird Ihnen die Verwendung von *.local* als TLD (Top Level Domain) vorgeschlagen. Die Verwendung dieser TLD bietet Ihnen den Vorteil, dass die interne Domäne klar von externen Internetdomänen getrennt ist, die nicht *.local* als TLD verwenden können.

Dennoch können Sie auch eine beliebige andere TLD wie z.B. *.de* oder *.com* verwenden. Stellen Sie in diesem Fall jedoch sicher, dass es zu keinen Überschneidungen mit einer bereits im Internet registrierten Domäne kommt. Sobald Sie eine andere TLD als *.local* gewählt haben und Sie auf WEITER klicken, erhalten Sie ein Hinweisfenster (siehe Abbildung 2.7).

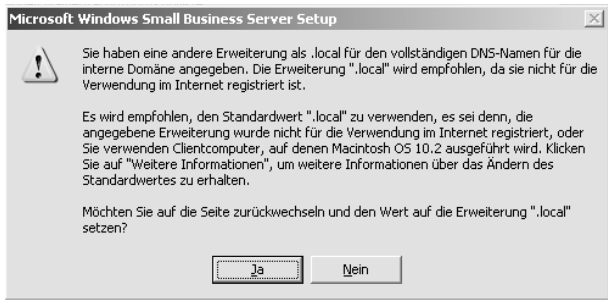


Abbildung 2.7: Hinweisfenster für die Benennung der TLD

Hier werden Sie nochmals über die Vorteile einer Verwendung von *.local* als TLD aufgeklärt. Möchten Sie nun doch diese TLD verwenden, klicken Sie auf JA, möchten Sie die gewählte TLD beibehalten, klicken Sie auf NEIN.

Nachdem die Installation des SBS 2003 abgeschlossen ist, können Sie den DNS-Domänennamen, den NETBIOS-Domänennamen sowie den Computernamen nicht mehr ändern. Überlegen Sie sich also jetzt gut, welche Namen Sie verwenden möchten. Für eine Namensänderung muss der SBS 2003 neu installiert werden.

5. Sofern sich im SBS 2003 mehr als eine Netzwerkkarte befindet, müssen Sie im Fenster Informationen zu den lokalen Netzwerkadaptern diejenige Karte auswählen, die für den Zugriff auf das lokale Netzwerk benutzt werden soll. Während des Setups werden auf dem SBS sämtliche Netzwerkkarten deaktiviert, die nicht als die Karte für die Verbindung zum lokalen Netzwerk ausgewählt wurden. Vorhandene Einstellungen der deaktivierten Netzwerkkarten werden dabei gespeichert und gehen nicht verloren.

Um sicherzustellen, dass bei den Netzwerkkabeln, die zur Netzwerkkarte mit der lokalen Verbindung führen, und der Internetverbindung keine Verwechslungen entstehen, sollten Sie die Kabel entsprechend kennzeichnen.

6. Nach der Konfiguration des DNS steht die DHCP(Dynamic Host Control Protocol)-Konfiguration an. Sofern sich noch ein weiterer DHCP-Server im gleichen Netz befindet, erhalten Sie ein Hinweisfenster (siehe Abbildung 2.8). Sie haben hier die Möglichkeit, entweder den DHCP-Server des SBS zu installieren (Schaltfläche JA) oder aber den bereits vorhandenen DHCP-Server beizubehalten (Schaltfläche NEIN).

Abbildung 2.8: Hinweis bei der DHCP-Konfiguration, wenn sich bereits ein anderer DHCP-Server im Netzwerk befindet

7. Im nächsten Schritt wird die eben gewählte bzw. einzig im Server vorhandene Netzwerkkarte des SBS konfiguriert. Sofern Sie sich im vergangenen Schritt dafür entschieden haben, den vorhandenen DHCP-Server beizubehalten, werden die Adressinformationen für IP-Adresse, Subnetzmaske und Standard-Gateway von diesem DHCP-Server bereitgestellt (siehe Abbildung 2.9).

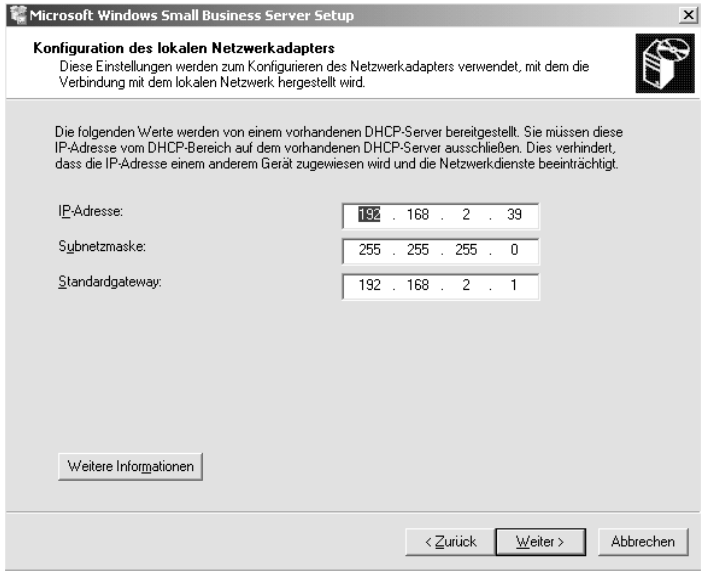


Abbildung 2.9: Von einem DHCP-Server bereitgestellte Adressinformationen für den SBS 2003

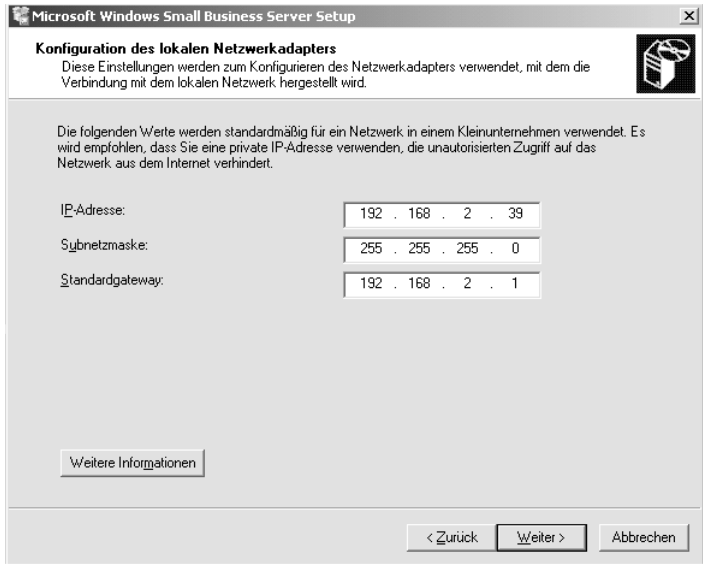


Abbildung 2.10: Die vorgeschlagene DHCP-Konfiguration, wenn der DHCP-Dienst auf dem SBS 2003 ausgeführt werden soll

Werden die Informationen nicht von einem DHCP-Server bereitgestellt, wird Ihnen eine Konfiguration vorgeschlagen (siehe Abbildung 2.10). Diese Einstellungen sollten Sie beibehalten. Wurde bisher noch keine Adresse für den Netzwerkadapter festgelegt, wird die IP-Adresse 192.168.2.2 vorgeschlagen, da Router oftmals die Adresse 192.168.2.1 verwenden und es zu keinem Adresskonflikt mit dem Gerät kommen soll. Wurde bereits eine Adresse vergeben, wird diese vorgeschlagen.

8. Im Fenster ANMELDEINFORMATIONEN können Sie festlegen, ob Sie sich während des Setups automatisch oder manuell anmelden möchten (siehe Abbildung 2.11). Da im Laufe der weiteren Konfiguration einige Neustarts erforderlich sind, sollten Sie die Option AUTOMATISCH ANMELDEN wählen. Die automatische Anmeldung funktioniert nur, wenn für das Administratorkonto ein Kennwort vergeben ist. Das Kennwort kann aus den Zeichen A–Z, a–z, 0–9 sowie Sonderzeichen wie z.B. $, * oder ! bestehen. Damit das Passwort als sicher gilt, sollten Sie zwischen acht bis 127 verwenden und die verschiedenen Zeichenarten miteinander kombinieren. Klicken Sie dann auf WEITER.

Die automatische Anmeldung des Administrators ist lediglich auf den Zeitraum des Setups beschränkt. Sobald dieses abgeschlossen wurde, muss er sich wieder manuell anmelden.

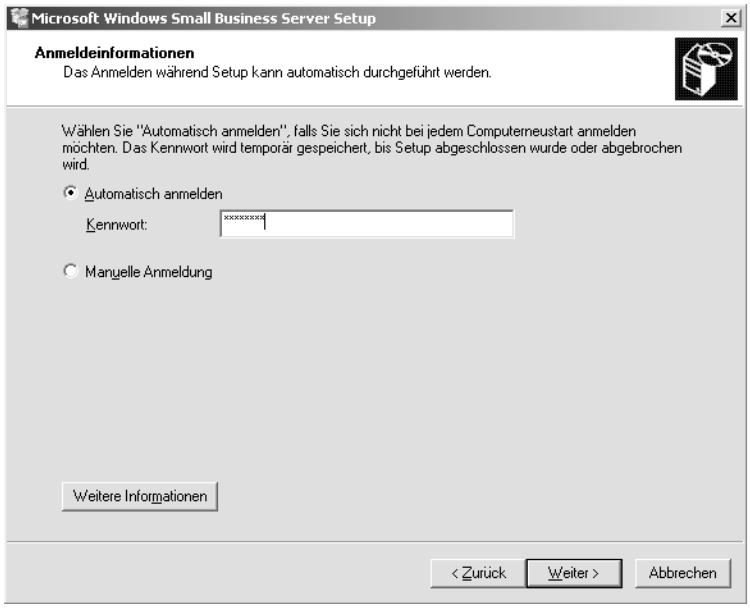


Abbildung 2.11: Die Option der automatischen Anmeldung des Administrators während des Setups

9. Im letzten Fenster WINDOWS-KONFIGURATION erhalten Sie Informationen zur weiteren Vorgehensweise (siehe Abbildung 2.12). Der folgende Konfigurationsvorgang wird ca. eine halbe Stunde dauern. Während dieser Zeit sollten sämtliche Anwendungen und Fenster (außer denen des Setups natürlich) geschlossen werden. Um mit der Konfiguration zu beginnen, klicken Sie auf WEITER.

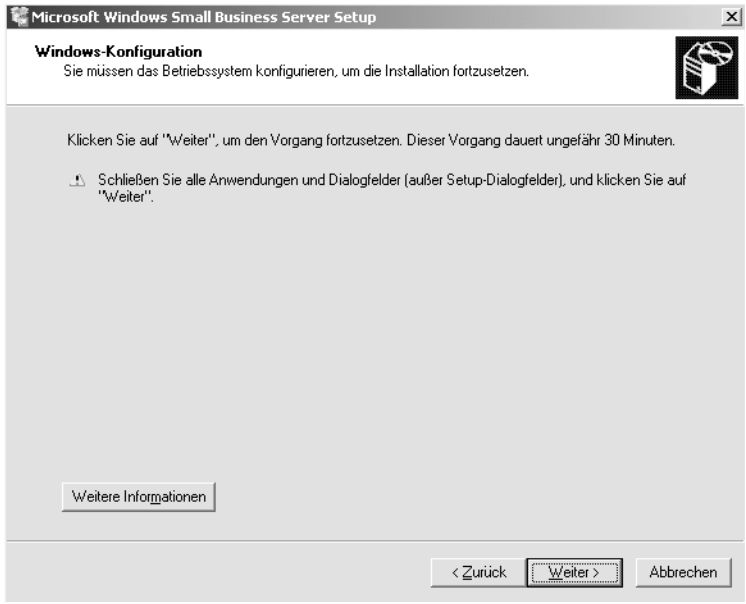


Abbildung 2.12: Hinweisfenster für die Durchführung der Konfiguration

Konnte die Durchführung der Konfiguration nicht korrekt zu Ende geführt werden, erscheint nach einem Neustart auf dem Desktop die Verknüpfung SETUP FORTSETZEN. Die erneute Konfiguration beginnt wieder bei dem eben beschriebenen Schritt 1.

10. Nachdem Sie auf WEITER geklickt haben, werden die Komponenten installiert. Dieser Installationsvorgang dauert ca. 30 Minuten. Währenddessen sehen Sie das Fenster KOMPONENTENSTATUS (siehe Abbildung 2.13). Hier erhalten Sie Informationen über den Status der Installation und Konfiguration. Zudem sehen Sie, wann ein Neustart erfolgt. Haben Sie die automatische Anmeldung gewählt, müssen Sie bis zum Ende der Konfiguration keine weiteren Einstellungen vornehmen.

Die Konfiguration des Servers sollte grundsätzlich nach der Installation des Betriebssystems erfolgen. Wenn Sie nach der Installation das Setup abbrechen, wird der SBS automatisch nach Ablauf von sieben Tagen heruntergefahren, da er so nicht den Lizenzanforderungen entspricht.

Wurde das Setup nach der Installation des Betriebssystems noch nicht ausgeführt, befindet sich auf dem Desktop die Verknüpfung SETUP FORTSETZEN. Haben Sie diese Verknüpfung gelöscht, oder möchten Sie das Setup zu einem späteren Zeitpunkt erneut ausführen, so starten Sie von der Installations-CD 1 die Datei *SETUPSBS.EXE*.

Wenn Sie das Setup auf einem Server starten, der bereits konfiguriert ist, können Sie sowohl zusätzliche Komponenten hinzufügen als auch einige entfernen und sogar fehlerhafte Komponenten reparieren oder neu installieren.

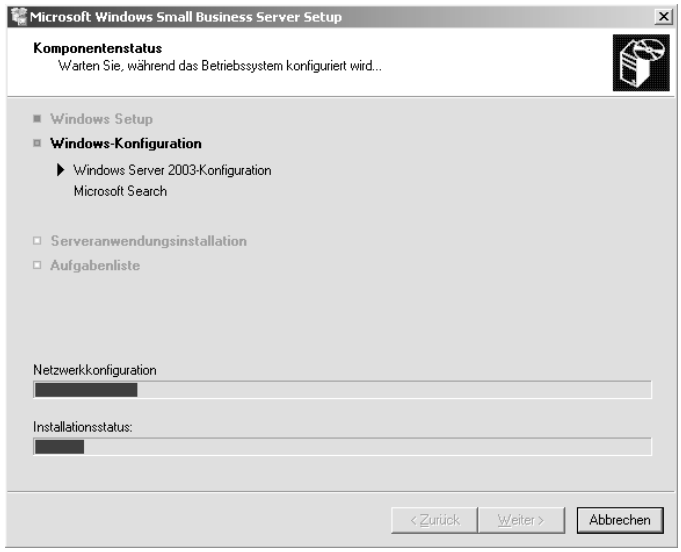


Abbildung 2.13: Der Komponentenstatus während der Windows-Konfiguration

2.5.1 Was geschieht während der Grundkonfiguration?

Während die Grundkonfiguration durchgeführt wird, werden auf dem Server zahlreiche Änderungen unterschiedlichster Anwendungen, Dienste und Komponenten vorgenommen. Dieses Kapitel gibt Ihnen einen nach Sachgebieten geordneten Überblick über die Änderungen, die an der Serverkonfiguration durchgeführt werden.

Ändern des Computernamens

Sofern im Fenster INTERNE DOMÄNENINFORMATION (siehe Abbildung 2.6) der Computername im Gegensatz zu dem während der Installation des Betriebssystems selbst angegebenen geändert wurde, werden alle Informationen auf dem Server modifiziert, die den Computernamen enthalten.

Prüfung der Netzwerkkonfiguration

In diesem Schritt wird zunächst die Konfiguration der Netzwerkkarten überprüft. Zusätzlich werden alle erforderlichen Netzwerkdienste und Protokolle installiert und konfiguriert.

Installation weiterer Komponenten

Im Zuge der Grundkonfiguration werden die Internetinformationsdienste (IIS 6.0) inklusive der IIS-Dokumentation sowie der IIS-Verwaltungsprogramme installiert. IIS ist erforderlich für die webbasierten Dienste der SharePoint Services für die Intranet-Webseite, Outlook Web Access (OWA) sowie den Remote-Webarbeitsplatz. Weiterhin werden der NNTP-Dienst (Network News Transfer Protocol), ASP.NET, RPC über http-Proxy und der SMTP-Dienst (Simple Mail Transfer Protocol) installiert.

Installation und Konfiguration des Active Directory

Weiterhin erfolgt die Einrichtung des Active Directory. Da die SBS 2003-Domäne lediglich als Root-Domäne ausgeführt werden kann, ist die Konfiguration einfacher gegenüber einem normalen Windows Server 2003. Die SBS-Domäne wird als Active Directory-Domäne im einheitlichen Betriebsmodus Windows 2000 konfiguriert. In diesem Betriebsmodus ist die Unterstützung der Servertools sichergestellt. Das Kennwort für die Verzeichnisdienst-Wiederherstellung wird mit dem während der Installation festgelegten Administratorkennwort synchronisiert.

Installation von Microsoft Search

Microsoft Search ist für die Unterstützung von Indices sowie für Abfragen im Exchange Server 2003 erforderlich.

2.6 Installation weiterer Serverkomponenten

Nachdem die Grundkonfiguration abgeschlossen wurde, erfolgt die Installation der Serveranwendungen und zugehörigen Werkzeuge. Die Auswahl und Installation der Serverkomponenten dauert ca. 90 Minuten bei der Standardversion des SBS 2003.

1. Im Fenster KOMPONENTENAUSWAHL sehen Sie die Komponenten, die typischerweise bei einer Standardinstallation ausgewählt werden (siehe Abbildung 2.14).

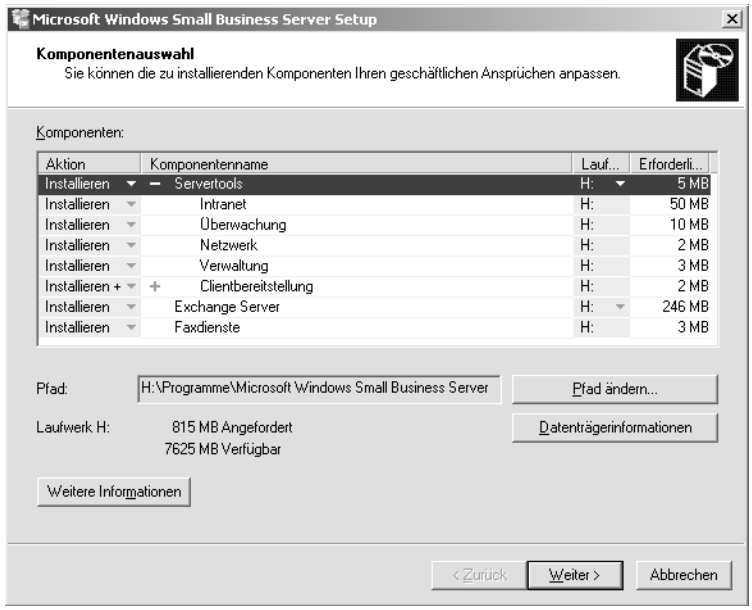


Abbildung 2.14: Die Auswahl der zu installierenden Komponenten für den SBS 2003

Möchten Sie diese vorgegebene Auswahl modifizieren, klicken Sie in der Spalte AKTION auf den kleinen Pfeil. Sie haben die Wahl zwischen INSTALLIEREN und KEINE AKTION. Im zweiten Fall wird die Komponente nicht installiert. Die Komponenten SERVERTOOLS sowie CLIENTBEREITSTELLUNG verfügen beide über eine Liste untergeordneter Features (zu erkennen an dem +-Symbol), die separat installiert werden können. Über die Schaltfläche PFAD ÄNDERN können Sie für die Komponenten SERVERTOOLS und EXCHANGE SERVER einen anderen Installationspfad bestimmen. Über die Schaltfläche DATENTRÄGERINFORMATIONEN erhalten Sie Informationen über die noch freie Festplattenkapazität Ihrer Laufwerke. Haben Sie Ihre Auswahl getroffen, klicken Sie auf WEITER.

2. Im Fenster DATENORDNER können Sie die Installationspfade für die Datenordner bestimmen (siehe Abbildung 2.15).

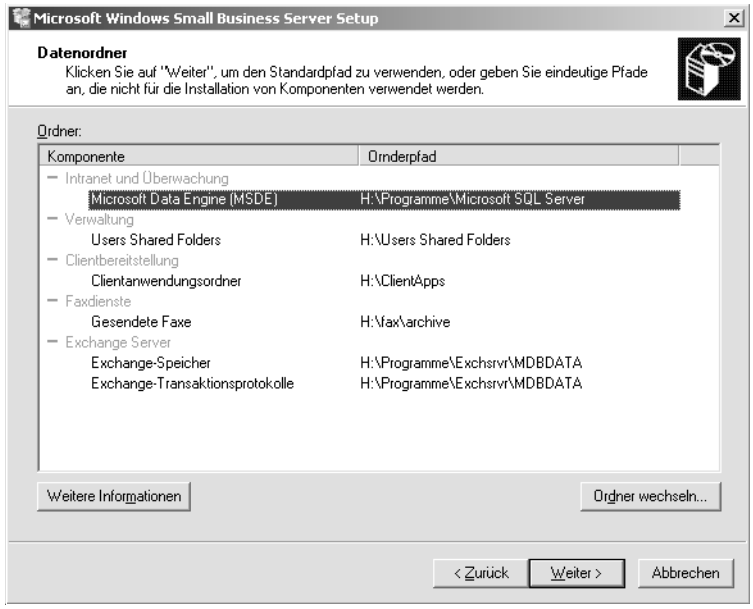


Abbildung 2.15: Anpassen der Installationspfade für die Datenordner

Sofern Ihr System über ein zweites Festplattenlaufwerk verfügt, das ebenfalls mit NTFS formatiert ist, sollten Sie dieses Laufwerk als Speicherort für die Datenordner auswählen. Klicken Sie zum Ändern des Pfades auf ORDNER WECHSELN. Haben Sie die Pfade ausgewählt oder die Standardeinstellungen übernommen, klicken Sie auf WEITER.

Was sind Datenordner?

Datenordner sind für einige Applikationen wie z.B. den Exchange Server oder die Faxdienste bei der Installation erforderlich. Ist auf dem System ein weiteres Laufwerk verfügbar, sollten Sie die Datenordner getrennt vom Systemlaufwerk installieren. Dadurch wird die Systemleistung erhöht. Zudem erleichtern Sie sich so das Sichern und Wiederherstellen der Daten.

Für den Datenordner USERS SHARED FOLDERS sind die folgenden Standardberechtigungen festgelegt:

- Domänenbenutzer: Lesen und Ändern
- Administratoren: Vollzugriff
- Folder Operators: Vollzugriff

Zudem gelten die folgenden Standardberechtigungen:

- Nicht von übergeordneten Objekten vererbbar
- Administratoren: Vollzugriff (vererbbar)
- Folder Operators: Vollzugriff (vererbbar)
- Domänenbenutzer : Lesen und Ausführen (nicht vererbbar)

Die folgenden Standardberechtigungen für die Ordner aller Benutzer haben auch für den Ordner USERS SHARED FOLDERS Gültigkeit:

- Name des Benutzers: Vollzugriff
- Administratoren: Vollzugriff
- Folder Operators: Vollzugriff

Diese Standardberechtigungen können Sie ändern. Sobald Sie aber den SBS 2003 neu installieren, werden die Berechtigungen für USERS SHARED FOLDERS auf die eben genannten Standardberechtigungen zurückgesetzt. Die Standardberechtigungen werden auch wieder hergestellt, wenn Sie einen SBS 2000 auf SBS 2003 aktualisieren und unter SBS 2000 die Berechtigungen für USERS SHARED FOLDERS modifiziert hatten.

3. Als Nächstes erscheint das Fenster KOMPONENTENZUSAMMENFASSUNG (siehe Abbildung 2.16). Hier sehen Sie die Zusammenfassung Ihrer in Schritt 1 gewählten Installationsoptionen. Möchten Sie noch Änderungen vornehmen, gehen Sie über die Schaltfläche ZURÜCK bis an die gewünschte Stelle. Anderenfalls klicken Sie auf WEITER.
4. Wie bei der Grundkonfiguration erhalten Sie auch jetzt wieder das Fenster KOMPONENTENSTATUS, das Sie über den Installations- und Konfigurationsfortschritt unterrichtet (siehe Abbildung 2.17). Die Installation dauert ca. 60 Minuten.

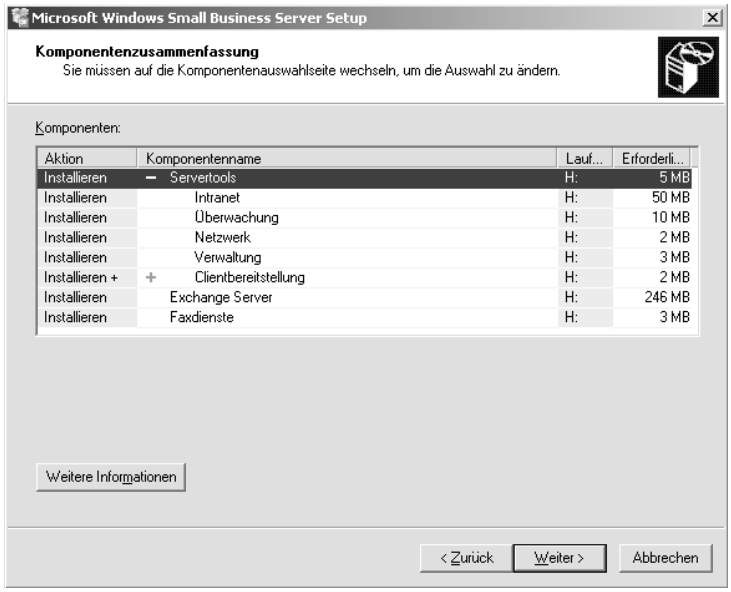


Abbildung 2.16: Die Komponentenzusammenfassung vor der Installation

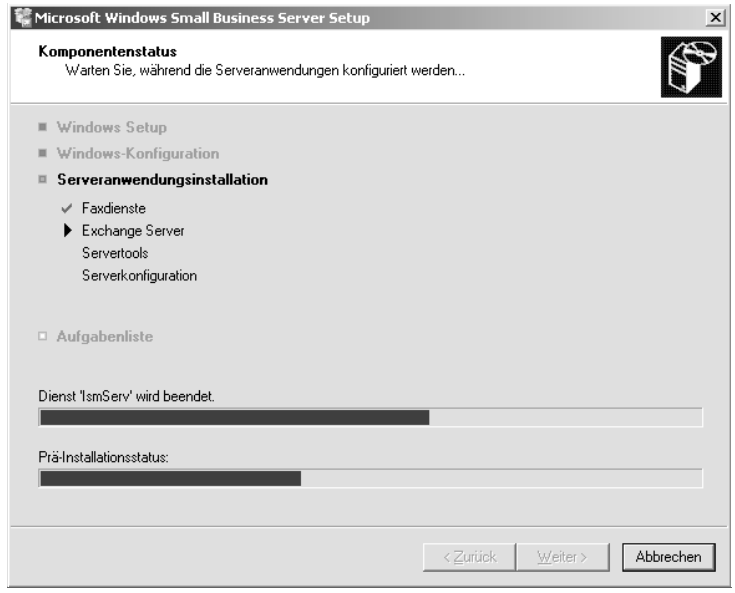


Abbildung 2.17: Die Übersicht über den Installationsfortschritt

5. Nachdem alle Serveranwendungen und Werkzeuge erfolgreich installiert wurden, erhalten Sie das Fenster FERTIGSTELLEN DER INSTALLATION. Klicken Sie hier auf FERTIG STELLEN und dann auf OK. Damit wird der abschließende Neustart des Systems eingeleitet.

2.7 Aufgabenliste zur abschließenden Konfiguration

Nach Abschluss der Installation der Serverkomponenten wird der SBS neu gestartet, und Sie sehen eine Aufgabenliste mit Aufgaben zur abschließenden Konfiguration von Serveranwendungen und Werkzeugen. Nachdem Sie diese abschließende Aufgabenliste abgearbeitet haben, ist der SBS 2003 einsatzbereit. Um später Änderungen oder weitere Einstellungen vorzunehmen, rufen Sie die Serververwaltung des SBS 2003 auf. Um zu beginnen, klicken Sie auf die Schaltfläche START. Sie erhalten dann das Fenster AUFGABENLISTE (siehe Abbildung 2.18).

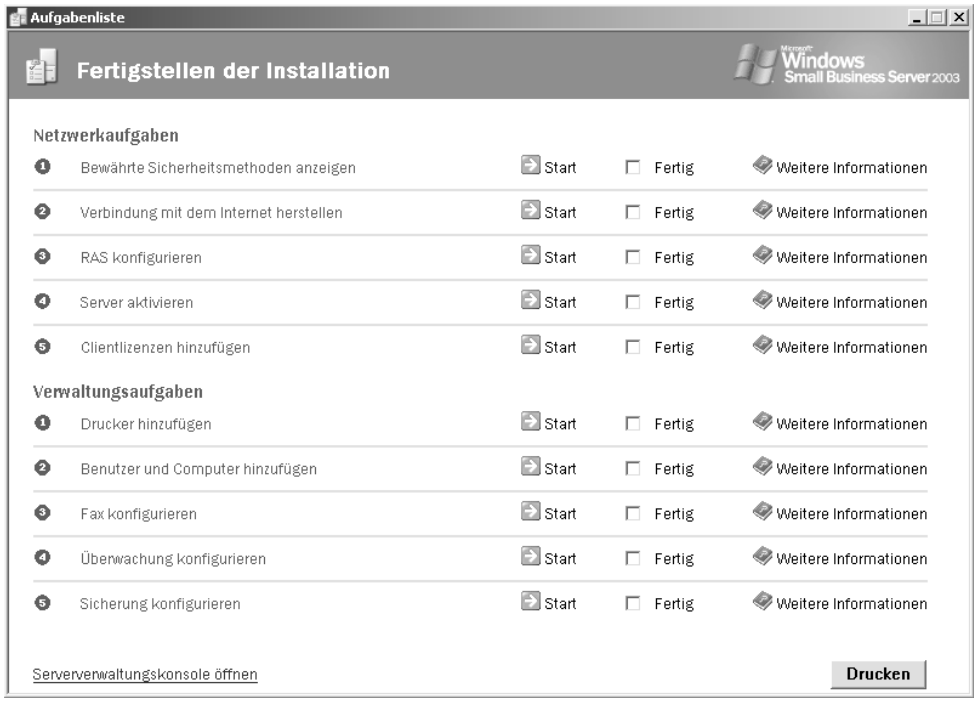


Abbildung 2.18: Die Aufgabenliste zum Fertigstellen der Installation

Bei der Abarbeitung der Liste sollten Sie die vorgegebene Reihenfolge der einzelnen Schritte einhalten. Die Konfigurationszeit wird ca. 30 Minuten in Anspruch nehmen (ohne die Zeit, die für die Durchführung der Client-Setups auf den einzelnen Clients erforderlich ist).

Die Aufgabenliste ist unterteilt in die beiden übergeordneten Abschnitte Netzwerkaufgaben und Verwaltungsaufgaben. Die einzelnen Aufgaben dieser beiden Bereiche werden in den folgenden Kapiteln detailliert vorgestellt.

2.7.1 Netzwerkaufgabe: Bewährte Sicherheitsmethoden anzeigen

Unter diesem Punkt werden Sie auf die Hilfe des SBS 2003 weitergeleitet. Sie erhalten hier Hinweise zu Sicherheitsempfehlungen in diversen Netzwerkbereichen wie z.B. die Konfiguration von Kennwortrichtlinien, des Remote-Zugriffs, das Implementieren einer Antivirenlösung, Ausführen von Sicherheitstools oder Gewähren von Zugriffsberechtigungen. Entscheiden Sie anhand dieser Liste selbst, welche vorgeschlagenen Punkte sich am sinnvollsten in Ihrem Netzwerk etablieren lassen.

2.7.2 Netzwerkaufgabe: Verbindung mit dem Internet herstellen

Mit Hilfe dieses Assistenten konfigurieren Sie das Netzwerk, die Firewall, sichere Webseitenveröffentlichungen und E-Mail-Einstellungen für den SBS 2003.

1. Nach einer Willkommensmeldung wählen Sie zunächst den gewünschten Verbindungstyp aus (siehe Abbildung 2.19).

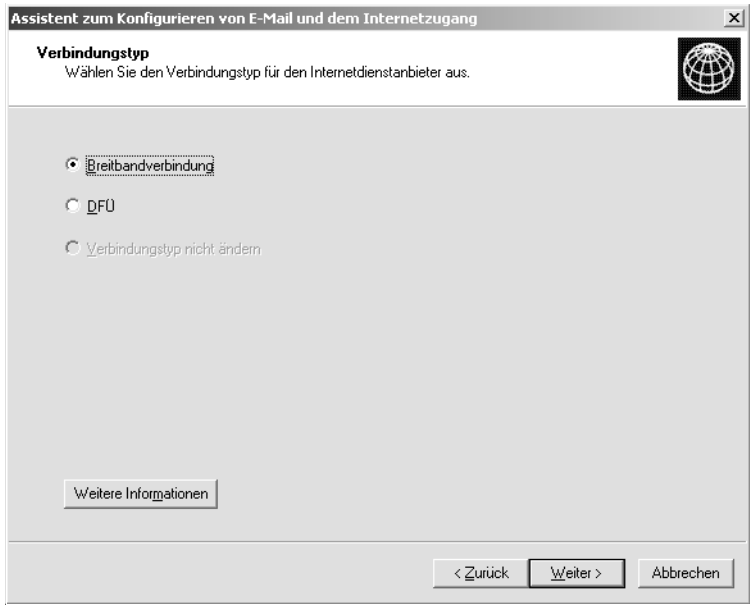


Abbildung 2.19: Der Verbindungstyp der Internetverbindung

Sie können hier zwischen BREITBANDVERBINDUNG und DFÜ wählen. Wählen Sie BREITBANDVERBINDUNG, wenn Sie über eine Hochgeschwindigkeitsverbindung wie DSL oder schneller verfügen.

Die Option VERBINDUNGSTYP NICHT ÄNDERN ist erst verfügbar, wenn Sie den Assistenten bereits einmal ausgeführt haben und nun nur Änderungen auf einigen Seiten vornehmen möchten. Die so übersprungenen Einstellungen werden nicht geändert. Die Option NICHT ÄNDERN finden Sie auf zahlreichen Seiten sämtlicher Assistenten der Aufgabenliste. Sie dient jedes Mal demselben Zweck.

Verwenden Sie eine Wahlverbindung, so benutzen Sie die Option DFÜ. In diesem Fall müssen Sie sicherstellen, dass das Modem korrekt erkannt und installiert wurde. Anderenfalls kann das Modem nicht konfiguriert werden. Klicken Sie dann auf WEITER.

2. Haben Sie eben den Verbindungstyp Breitbandverbindung gewählt, müssen Sie nun angeben, wie diese Verbindung hergestellt wird (siehe Abbildung 2.20). Wählen Sie dazu aus der Listbox DER SERVER VERWENDET einen der folgenden Einträge: EIN LOKALES ROUTERGERÄT MIT EINER IP-ADRESSE, EINE VERBINDUNG, DIE EINEN BENUTZERNAMEN UND EIN KENNWORT ERFORDERT (PPPOE) oder EINE DIREKTE BREITBANDVERBINDUNG.

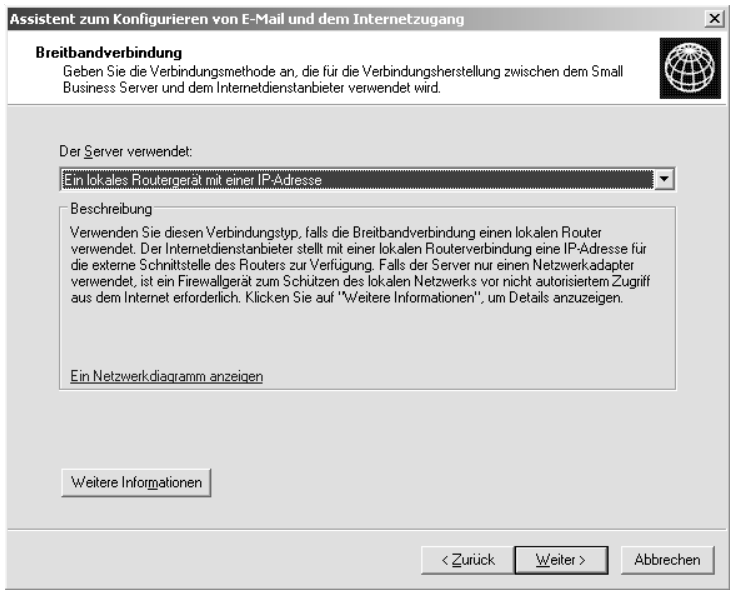


Abbildung 2.20: Bestimmen der Internetverbindungsmethode

Eine Hilfestellung, welche Methode auf Ihr Netzwerk zutrifft, erhalten Sie über WEITERE INFORMATIONEN sowie den Link EIN NETZWERKDIAGRAMM ANZEIGEN. Klicken Sie dann auf WEITER.

3. Im Fenster ROUTERVERBINDUNG (siehe Abbildung 2.21) geben Sie die für den Router erforderlichen Daten für die Verbindungsherstellung an. In unserem Beispiel gehen wir davon aus, dass Sie in Schritt 2 die Option EIN LOKALES ROUTERGERÄT MIT EINER IP-ADRESSE ausgewählt haben.

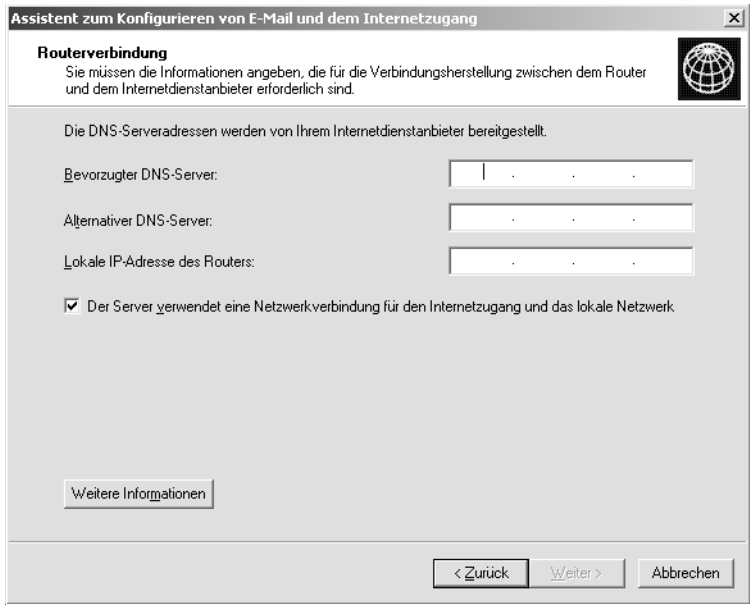


Abbildung 2.21: Die erforderlichen Daten für eine router-basierte Internetverbindung

In das Feld BEVORZUGTER DNS-SERVER tragen Sie die IP-Adresse des DNS-Servers ein. Sofern Sie einen zweiten DNS-Server verwenden, können Sie dessen IP-Adresse unter ALTERNATIVER DNS-SERVER eintragen. Im Feld LOKALE IP-ADRESSE DES ROUTERS tragen Sie die IP-Adresse dessen interner Schnittstelle ein. Sofern Sie nur über eine Netzwerkkarte verfügen, ist automatisch die Checkbox DER SERVER VERWENDET EINE NETZWERKVERBINDUNG FÜR DEN INTERNETZUGANG UND DAS LOKALE NETZWERK markiert. Klicken Sie dann auf WEITER.

4. Ist im Server nur eine Netzwerkkarte installiert, erhalten Sie ein entsprechendes Hinweisfenster (siehe Abbildung 2.22), das Sie darüber informiert, dass die im SBS 2003 enthaltene nicht installiert werden kann. Um dennoch das Netzwerk über eine Firewall abzusichern, sollten Sie entweder eine externe Firewall konfigurieren oder eine zweite Netzwerkkarte hinzufügen. Um den Vorgang dennoch fortzusetzen, klicken Sie auf NEIN.

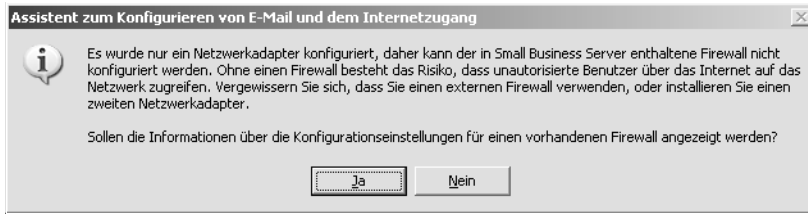


Abbildung 2.22: Hinweise bei nur einer installierten Netzwerkkarte bezüglich der Firewall

5. Auf der Seite WEBDIENSTEKONFIGURATION legen Sie fest, auf welche der Webdienste des Servers über die Firewall aus dem Internet zugegriffen werden soll (siehe Abbildung 2.23). Standardmäßig sind nur die Dienste OUTLOOK WEB ACCESS sowie REMOTE-WEBARBEITSPLATZ aktiviert.

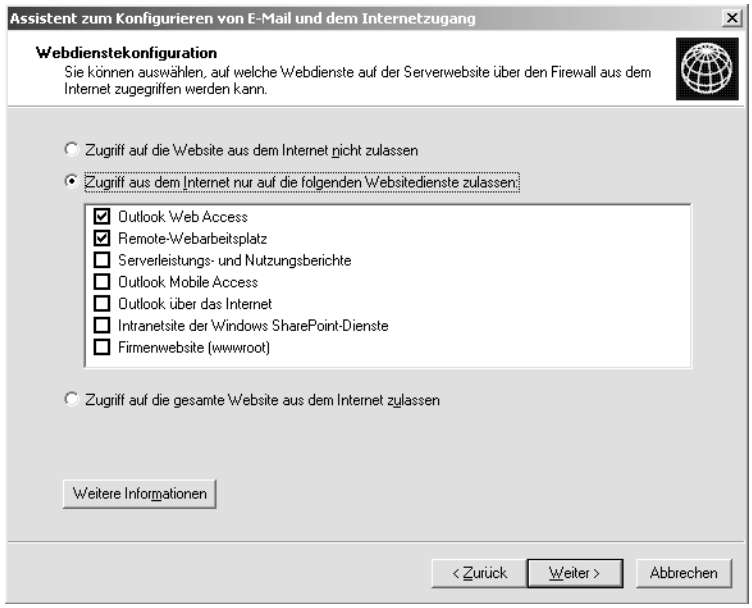


Abbildung 2.23: Auswählen der Webdienste des SBS 2003, auf die über das Internet zugegriffen werden darf

Sie können die folgenden Dienste auswählen:

OUTLOOK WEB ACCESS: Zugriff auf E-Mails über das Internet über einen Webbrowser. Bei einer sicheren Verbindung zwischen den Webservern müssen die Benutzer https:// verwenden.

REMOTE-WEBARBEITSPLATZ: Herstellen einer Verbindung zum lokalen Netzwerk über einen Webbrowser. Damit kann auf Outlook Web Access, die Remote-Desktop-Verbindung zu Clients im Netzwerk, die Serverleistungs- und Nutzungsberichte und die SharePoint Services-Intranetsite zugegriffen sowie der Verbindungsmanager downgeloadet werden. Für eine sichere Verbindung müssen die Benutzer https:// eingeben. Der Remote-Webarbeitsplatz bietet den Vorteil, dass die Benutzer keine VPN-Verbindung für den Zugriff auf das lokale Netzwerk herstellen müssen.

SERVERLEISTUNGS- UND NUTZUNGSBERICHTE: Diese Berichte ermöglichen dem Administrator Berichte über den Zustand und die Auslastung des Servers sowie etwaige Probleme und Engpässe auf dem Server. Zudem erhalten Sie in den Nutzungsberichten statistische Angaben über die Auslastung des Servers.

OUTLOOK MOBILE ACCESS: Mit mobilen Geräten wie z.B. PDAs können die Benutzer auf ihre E-Mails über das Internet zugreifen.

OUTLOOK ÜBER DAS INTERNET: Zugriff auf die E-Mails über Outlook 2003, ohne dass dazu eine VPN-Verbindung hergestellt werden muss. Der Zugriff auf den Exchange Server erfolgt über Remote Procedure Calls (RPCs) über http.

INTRANETSITE VON WINDOWS SHAREPOINT SERVICES: Zugriff auf die bei der Installation angelegte Intranetsite der SharePoint Services.

FIRMENWEBSITE (WWWROOT): Zugriff auf die Intranetsite der Firma.

Wählen Sie die Option ZUGRIFF AUF DIE GESAMTE WEBSITE AUS DEM INTERNET ZULASSEN, so können sämtliche authentifizierten Benutzer auf alle Website-Verzeichnisse der Standardwebsite über das Internet zugreifen. Ein anonymer Zugriff ist nicht möglich. Aus Sicherheitsaspekten sollten Sie dennoch abwägen, ob Sie diese Option wirklich auswählen möchten. Wählen Sie die Option ZUGRIFF AUF DIE WEBSITE AUS DEM INTERNET NICHT ZULASSEN, wird keiner der eben beschriebenen Dienste für die Benutzer über das Internet verfügbar. Klicken Sie dann auf WEITER.

6. Im Fenster WEBSERVERZERTIFIKAT treffen Sie die Einstellungen für Zertifikate (siehe Abbildung 2.24). Ein Zertifikat ist erforderlich für die SSL-gesicherte (Secure Sockets Layer) Kommunikation zwischen Webserver und Browser bei einigen Webdiensten. Sie können entweder über den Assistenten ein Zertifikat erstellen lassen oder eine Zertifikatsdatei von einer Zertifizierungsstelle auswählen.

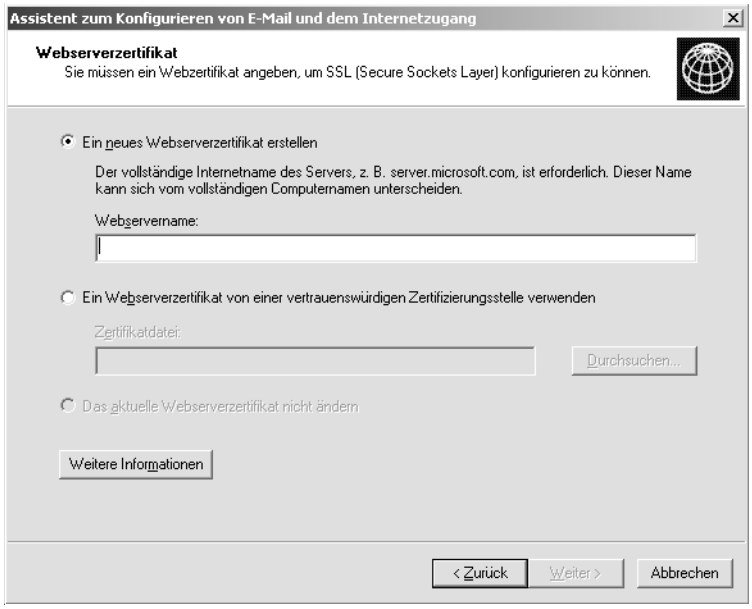


Abbildung 2.24: Das Erstellen eines Webserverzertifikats für SSL-gesicherte Verbindungen

Um ein neues Zertifikat zu erstellen, wählen Sie die Option EIN NEUES WEBSERVERZERTIFIKAT ERSTELLEN. Damit wird ein selbst signiertes Zertifikat erstellt. Dieses wird im Ordner \CLIENTAPPS\SBSCERT gespeichert und besitzt eine Gültigkeitsdauer von fünf Jahren. Dieses Zertifikat wird den Clients über den Client-Setup-Assistenten bereitgestellt.

Geben Sie in das Feld WEBSERVERNAME den Namen des SBS an, mit dem Sie vom Internet aus auf Ihren Server zugreifen.

Die Option EIN WEBSERVERZERTIFIKAT VON EINER VERTRAUENSWÜRDIGEN ZERTIFIZIERUNGSSTELLE VERWENDEN wird gewählt, wenn Sie bereits eine Zertifikatsdatei erhalten haben. Diese können Sie über DURCHSUCHEN angeben. Besitzen Sie noch keine Zertifikatsdatei, so können Sie diese auch anfordern. Verwenden Sie hierzu den Assistenten für Webserverzertifikate in den Internetinformationsdiensten (IIS). Dieses Zertifikat wird nicht den Clients zur Verfügung gestellt wie das eigene selbst signierte Zertifikat, da es sich hier um ein vertrauenswürdiges Zertifikat handelt. Haben Sie ein Zertifikat erhalten, führen Sie diesen Assistenten für die E-Mail- und Internetverbindung erneut aus. Klicken Sie dann auf WEITER.

7. Als Nächstes erfolgt die Konfiguration von Internet-E-Mail (siehe Abbildung 2.25). Hiermit wird der Exchange Server für das Senden und Empfangen von Internet-E-Mail konfiguriert. Zum Senden wird der Small Business-SMTP-Connector erstellt. Für den Empfang von E-Mails wird der Microsoft POP3-Connector benutzt.

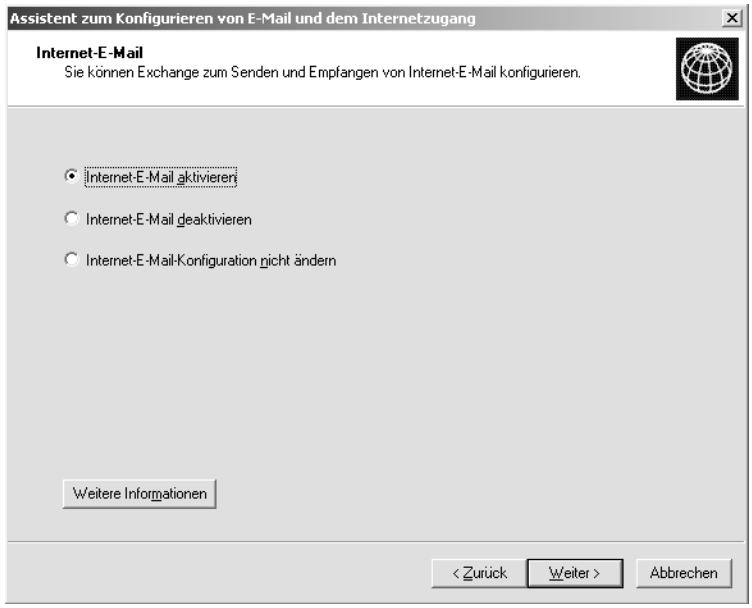


Abbildung 2.25: Die Konfiguration von Internet-E-Mail

Um den Exchange Server zu konfigurieren, wählen Sie die Option INTERNET-E-MAIL AKTIVIEREN. Mit der Option INTERNET E-MAIL DEAKTIVIEREN wird der Small Business-SMTP-Connector gelöscht und der Microsoft POP3-Connector deaktiviert. Sie haben dann keine Möglichkeit mehr, Internet-E-Mails über den Exchange Server zu senden und empfangen. Lediglich E-Mails im internen Netzwerk können noch gesendet und empfangen werden. Klicken Sie dann auf WEITER.

8. Sofern Sie im letzten Schritt Internet-E-Mail aktiviert haben, bestimmen Sie zunächst die E-Mail-Übermittlungsmethode (siehe Abbildung 2.26).

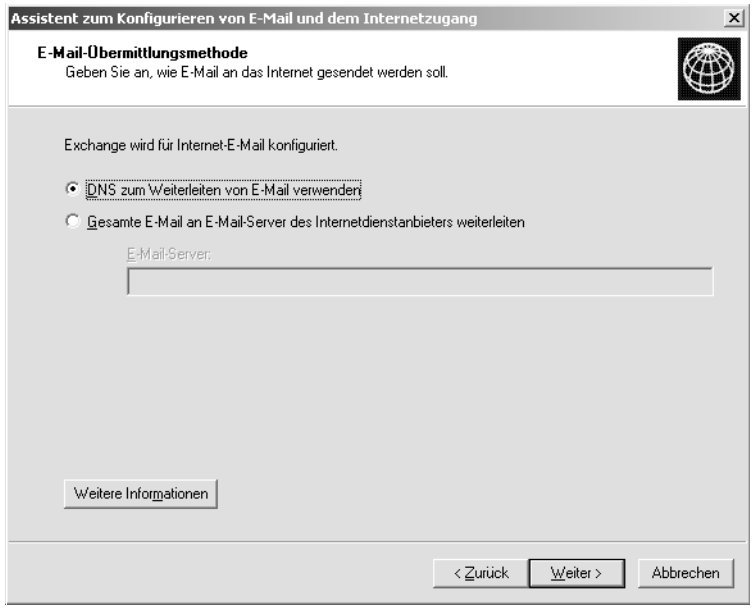


Abbildung 2.26: Konfiguration der E-Mail-Übermittlungsmethode

Verwenden Sie hier die Option DNS ZUM WEITERLEITEN VON E-MAIL VERWENDEN, wenn DNS für das Senden von E-Mails verwendet werden soll. In diesem Fall sendet der Exchange Server über den entsprechenden DNS-Ressourceneintrag für Mail-Exchanger (MX).

Ist es hingegen von Ihrem Internetdienstanbieter (ISP) aus erforderlich, dass Sie Ihre E-Mails an einen dedizierten Mailserver senden, wählen Sie die Option GESAMTE E-MAIL AN E-MAIL-SERVER DES INTERNETDIENSTANBIETERS WEITERLEITEN. Das Senden der E-Mails über den Mailserver des Internetdienstanbieters wird auch als Relaying bezeichnet. Der Exchange Server leitet sämtliche Mails an den SMTP-Smarthost des Internetdienstanbieters weiter. Geben Sie in das Feld E-MAIL-SERVER den Mailservernamen des Internetdienstanbieters ein. Besitzt dieser mehrere Namen, so geben Sie alle Namen an und trennen die einzelnen Einträge durch ein Semikolon. Klicken Sie dann auf WEITER.

Ein Smarthost bzw. Relayhost ist ein Computer, der ausgehende Nachrichten von Remote-Domänen verarbeitet. Er kann auch als Mail-Gateway konfiguriert werden, da er sowohl über eine Verbindung zum Internet als auch zum Intranet verfügt.

9. Im Fenster E-MAIL-ABRUFMETHODE (siehe Abbildung 2.27) geben Sie an, auf welche Weise die E-Mails aus dem Internet empfangen werden sollen.

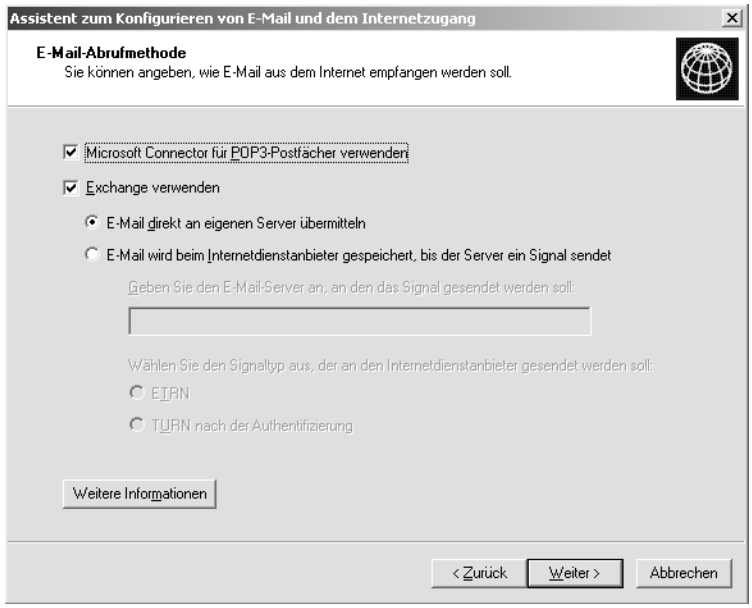


Abbildung 2.27: Die Auswahl der E-Mail-Abrufmethode für Internet-E-Mails

Markieren Sie die Checkbox MICROSOFT CONNECTOR FÜR POP3-POSTFÄCHER VERWENDEN, wenn Sie die E-Mails von einem POP3-Konto des Internetdienstanbieters an ein Exchange-Konto weiterleiten möchten. Dies bietet für den Benutzer den Vorteil, dass er nur sein Exchange-Postfach prüfen muss und nicht sein Exchange-Postfach und gleichzeitig noch sein POP3-Postfach. Zudem können die ans Exchange-Postfach gesendeten Mails auch über Outlook-Web Access abgerufen werden.

Wählen Sie die Option EXCHANGE VERWENDEN, werden die Mails über SMTP aus dem Internet empfangen. Hierzu müssen Sie bei Ihrem Internetdienstanbieter die erforderlichen Mail-Exchanger-Ressourceneinträge (MX) beantragen.

Die Abrufmethode E-MAIL DIREKT AN EIGENEN SERVER ÜBERMITTELN wird verwendet, wenn eingehende E-Mails direkt an den Exchange Server weitergeleitet und nicht beim Internetdienstanbieter gesammelt werden.

Über die Option E-MAIL WIRD BEIM INTERNETDIENSTANBIETER GESPEICHERT, BIS DER SERVER EIN SIGNAL SENDET veranlassen Sie den Exchange Server, ein Signal an den Mailserver des Internetdienstanbieters zu senden, wenn eine Internetverbindung des Exchange Servers besteht. Bis der Exchange Server das Signal sendet, werden die E-Mails bei dem Internetdienstanbieter gespeichert. Geben Sie in das entsprechende Feld den DNS-Namen oder die IP-Adresse des Mailservers bei Ihrem Internetdienstanbieter an. An diesen sendet der Exchange Server sein Signal. Hierzu müssen Sie noch den Signaltyp bestimmen.

ETRN: Dieses ist die Standardmethode für das Signal. Oftmals ist es erforderlich, dass der SBS 2003 über eine statische IP-Adresse verfügt, die vom Internetdienstanbieter für ein DFÜ-Modem oder einen Router für das Wählen bei Bedarf zugewiesen ist.

TURN NACH DER AUTHENTIFIZIERUNG: Bei dieser Signalart kann auch eine dynamische IP-Adresse des SBS 2003 verwendet werden. Wenn Sie diese Option wählen, erhalten Sie ein zusätzliches Fenster, in dem Sie den Benutzernamen und das Kennwort für die Exchange-Authentifizierung beim Internetdienstanbieter angeben.

In jedem Fall sollten Sie sich bei Ihrem Internetdienstanbieter erkundigen, welcher Signaltyp verwendet werden kann. Konfigurieren Sie den falschen Typ, schlägt möglicherweise die Weiterleitung der E-Mails an den Exchange Server fehl.

Klicken Sie dann auf WEITER.

Im Fenster NAME DER E-MAIL-DOMÄNE (siehe Abbildung 2.28) geben Sie den registrierten Internetdomänennamen an. Dieser Name wird für die E-Mail-Antwortadressen benutzt. Bei der Verwendung von Exchange sollten Sie darauf achten, dass der angegebene Name mit dem MX-Ressourceneintrag übereinstimmt.

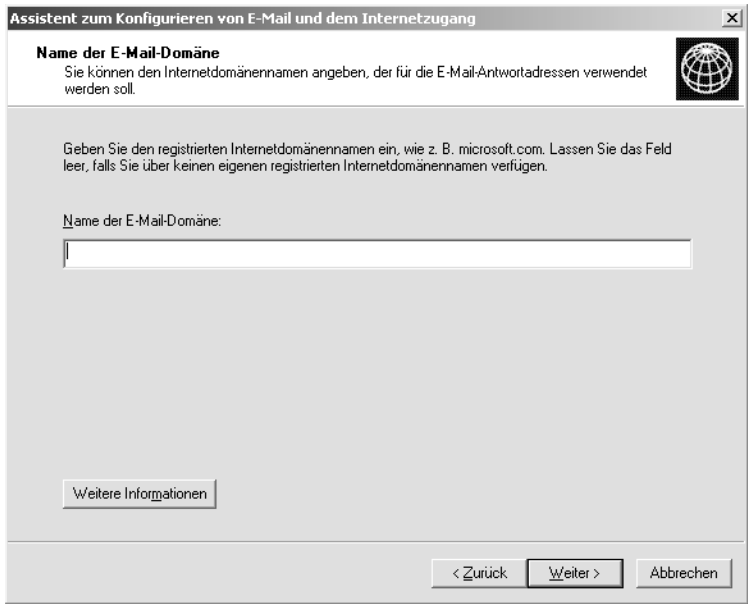


Abbildung 2.28: Den Namen der E-Mail-Domäne bestimmen

Verfügen Sie über keinen registrierten Internetdomänennamen, lassen Sie das Namensfeld leer. Dies gilt auch, wenn Sie den Exchange Server nur für den internen Mailverkehr nutzen möchten. Klicken Sie dann auf WEITER.

10. Im Fenster POP3-POSTFACHKONTEN (siehe Abbildung 2.29) legen Sie die POP3-Konten fest, von denen der POP3-Connector E-Mails abrufen und an den Exchange Server weiterleiten soll.

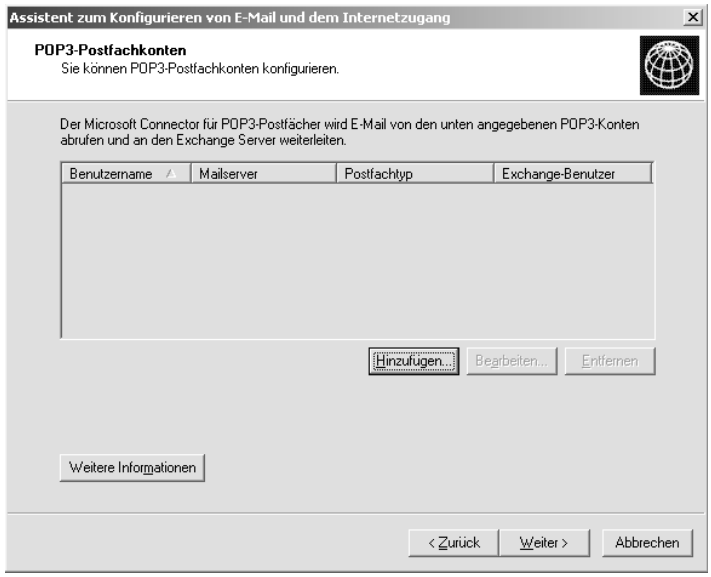


Abbildung 2.29: Auswahl der POP3-Konten, von denen der POP3-Connector E-Mails abrufen soll

Um ein neues Konto zu erstellen, klicken Sie auf HINZUFÜGEN. Sie erhalten das Fenster POP3-POSTFACH (siehe Abbildung 2.30).

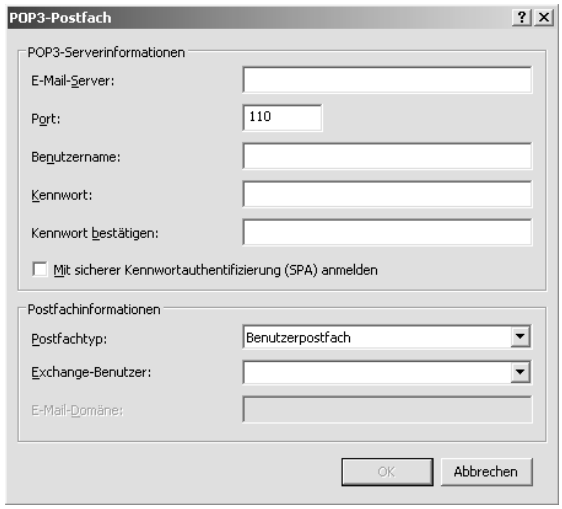


Abbildung 2.30: Die Informationen für das POP3-Postfach

In diesem Fenster geben Sie die Informationen für das POP3-Postfach an. Unter E-MAIL-SERVER geben Sie den vollständigen Namen des Mailservers Ihres Internetdienstanbieters an, unter BENUTZERNAME und KENNWORT die Authentifizierungsdaten. Unter POSTFACHTYP wählen Sie aus, um welche Art von Postfach es sich handelt. Es gibt die folgenden Optionen:

BENUTZERPOSTFACH: Ein Benutzerpostfach enthält die E-Mails, die an einen bestimmten Benutzer gesendet worden sind. Sobald die E-Mails dieses Postfaches über den POP3-Connector abgerufen werden, ändert sich im Header der E-Mail die An-Zeile auf den angegebenen Exchange-Empfänger ab. Geben Sie in das Feld EXCHANGE-BENUTZER den Benutzernamen oder eine Verteilergruppe ein.

GLOBALES POSTFACH: In einem globalen Postfach werden beim Internetdienstanbieter sämtliche an Sie adressierte E-Mails gesammelt. Sobald Exchange diese Mails abholt, wird der jeweilige Empfänger anhand der Zeile An oder Cc ermittelt und diesem die E-Mail in sein Postfach zugestellt. Geben Sie in das Feld E-MAIL-DOMÄNE den Namen der Mail-Domäne an, an die alle für Ihr Unternehmen bestimmten E-Mails gesendet werden.

Klicken Sie dann auf OK. Sie gelangen wieder in das Fenster POP3-POSTFACHKONTEN (siehe Abbildung 2.29). Hier können Sie nun weitere POP3-Konten hinzufügen, bestehende bearbeiten oder löschen. Klicken Sie dann auf WEITER.

11. Im nächsten Schritt wird unter E-MAIL-ZEITPLAN festgelegt, in welchen Intervallen der Exchange Server und der POP3-Connector Mails vom Mailserver des Internetdienstanbieters abrufen sollen (siehe Abbildung 2.31).

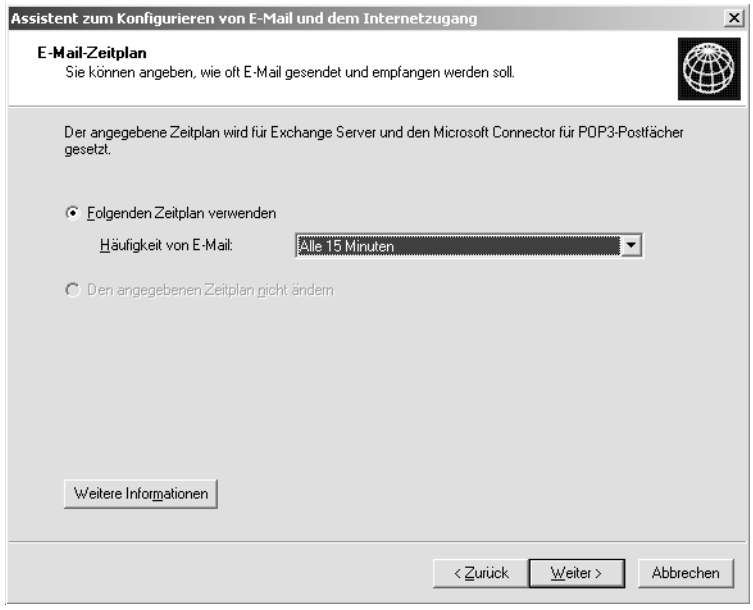


Abbildung 2.31: Festlegen eines Zeitplans für das Abrufen von E-Mails durch Exchange und POP3-Connector

Aus der Listbox FOLGENDEN ZEITPLAN VERWENDEN wählen Sie das gewünschte Abrufintervall aus. Die verfügbaren Intervalle liegen zwischen alle 15 Minuten bis alle 24 Stunden. Dieser Zeitplan besitzt jedoch nur Gültigkeit, wenn Sie unter der E-MAIL-ÜBERMITTLUNGSMETHODE (siehe Abbildung 2.26) die Option GESAMTE E-MAIL AN E-MAIL-SERVER DES INTERNETDIENSTANBIETERS WEITERLEITEN gewählt haben. Bei einer Breitbandverbindung werden E-Mails grundsätzlich sofort gesendet.

Haben Sie unter E-MAIL-ABRUFMETHODE (siehe Abbildung 2.27) den POP3-Connector gewählt, gilt der festgelegte Zeitplan für den E-Mail-Empfang. Bei einer Breitbandverbindung und der Wahl von Exchange hat der Zeitplan keinen Einfluss auf das Empfangen von E-Mails.

Werden die E-Mails erst nach einem Signal des Exchange Servers vom Internetdienstanbieter gesendet, greift für die Übermittlung der festgelegte Zeitplan.

Soll der Zeitplan unter Exchange definiert werden, öffnen Sie die SERVERVERWALTUNG und wählen aus dem Kontextmenü von SMALL BUSINESS-SMTP-CONNECTOR den Eintrag EIGENSCHAFTEN. Hier wählen Sie die Option DEN ANGEGEBENEN ZEITPLAN NICHT ÄNDERN.

Klicken Sie dann auf WEITER.

12. Im Fenster E-MAIL-ANLAGEN ENTFERNEN können Sie festlegen, ob bestimmte E-Mail-Anhänge vom Exchange Server entfernt werden sollen (siehe Abbildung 2.32).

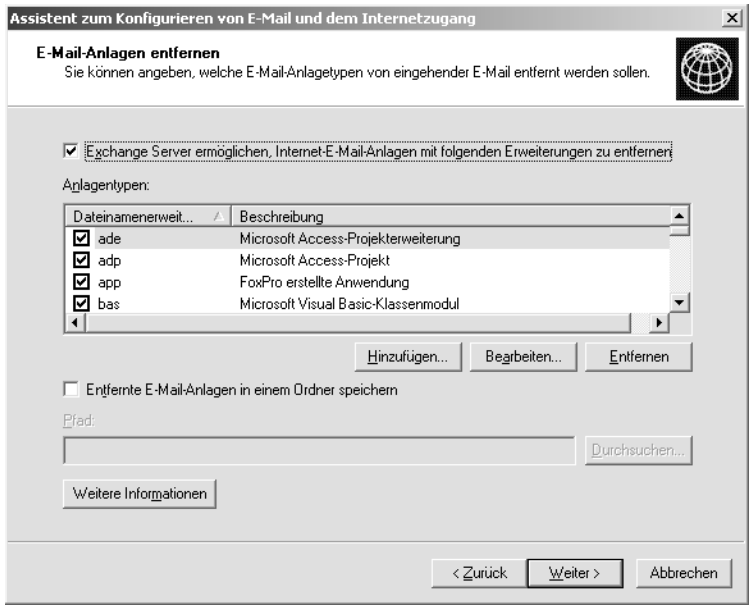


Abbildung 2.32: Festlegen, welche Typen von E-Mail-Anhängen automatisch vom Exchange Server entfernt werden sollen

Markieren Sie die Checkbox EXCHANGE SERVER ERMÖGLICHEN, INTERNET E-MAIL-ANLAGEN MIT FOLGENDEN ERWEITERUNGEN ZU ENTFERNEN und wählen aus der Liste sämtliche Dateitypen aus, die der Exchange Server automatisch löschen soll. Über die entsprechenden Schaltflächen können Sie auch Einträge hinzufügen, löschen oder bearbeiten. Das Löschen dieser Dateitypen bezieht sich nur auf SMTP-basierte Mails sowie die Mails der POP3-Postfächer, jedoch nicht auf interne E-Mails, die innerhalb des Firmennetzwerks versendet werden.

Sobald ein Anhang entfernt wurde, wird der E-Mail eine Notiz hinzugefügt, die den Benutzer darüber informiert, dass der Anhang gelöscht worden ist. Der Standardtext für diesen Benutzerhinweis befindet sich in der Datei \PROGRAMME\MICROSOFT WINDOWS SMALL BUSINESS SERVER\ICW\ATTACHMENT.TXT.

Sollen die entfernten Anlagen nicht sofort gelöscht, sondern in einem Ordner gespeichert werden, markieren Sie die Checkbox ENTFERNTE E-MAIL-ANLAGEN IN EINEM ORDNER SPEICHERN und geben den Pfad des Speicherordners an. Klicken Sie dann auf WEITER.

13. Danach erscheint das Fenster FERTIGSTELLEN DES ASSISTENTEN. Sie sehen hier Ihre Konfigurationen und können diese bei Bedarf noch ändern. Um die Einstellungen zu übernehmen, klicken Sie auf FERTIG STELLEN. Nach Abschluss der Konfiguration erhalten Sie das Statusfenster (siehe Abbildung 2.33). Schließen Sie dieses Fenster.

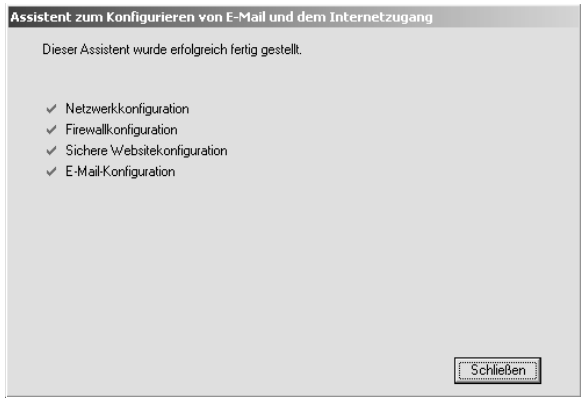


Abbildung 2.33: Abschluss der Aufgabe zur Konfiguration von E-Mail und Internetzugang

14. Nachdem Sie das Fenster geschlossen haben, erhalten Sie ein Fenster, das Sie zur Konfiguration der Kennwortrichtlinien auffordert. Bestätigen Sie mit JA. Es erscheint das Fenster KENNWORTRICHTLINIEN KONFIGURIEREN (siehe Abbildung 2.34).

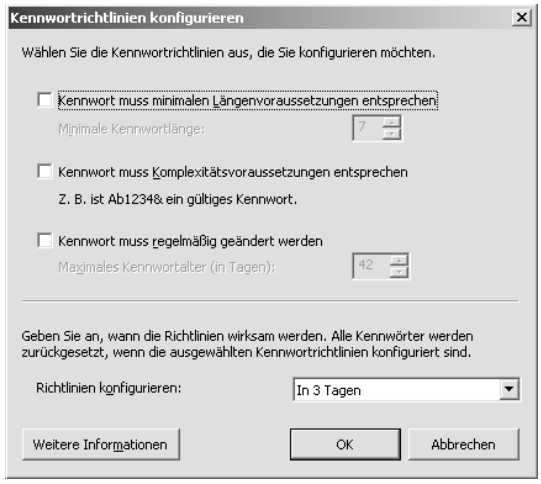


Abbildung 2.34: Die Konfiguration der Kennwortrichtlinien

Aus Sicherheitsgründen sollten Sie über die Kennwortrichtlinien Anforderungen für die Vergabe von Kennwörtern festlegen. Markieren Sie die Checkbox KENNWORT MUSS MINIMALEN LÄNGENVORAUSSETZUNGEN ENTSPRECHEN und wählen eine Zeichenlänge aus. Kennwörter, die kürzer sind, werden nicht mehr akzeptiert. Die Mindestlänge beträgt sieben Zeichen.

Ist die Checkbox KENNWORT MUSS KOMPLEXITÄTSVORAUSSETZUNGEN ERFÜLLEN aktiviert, müssen die Kennwörter Zeichen aus drei der vier folgenden Kategorien enthalten:

- Großbuchstaben A–Z
- Kleinbuchstaben a–z
- Ziffern 0–9
- Sonderzeichen wie z.B. %, # oder $.

Zudem darf das Kennwort nicht dem Kontonamen des Benutzers (auch nicht in Teilen) entsprechen.

Ist die Checkbox KENNWORT MUSS REGELMÄSSIG GEÄNDERT WERDEN aktiviert, können Sie bestimmen, nach wie vielen Tagen das Kennwort geändert werden muss. Die längste Gültigkeitsdauer für ein Kennwort beträgt 42 Tage.

Schließlich geben Sie unter RICHTLINIEN KONFIGURIEREN an, ab wann die neuen Richtlinien wirksam werden sollen. Standardmäßig geschieht dies nach drei Tagen. Sie sollten zunächst dieses Intervall beibehalten, damit Sie im Zuge der Clientkonfiguration bei der Anmeldung an den Clients noch keine komplexen Kennwörter verwenden müssen. Nach Abschluss der Clientkonfiguration sollten Sie den Wert auf SOFORT setzen.

Klicken Sie dann zum Übernehmen der Einstellungen auf OK.

15. Ist die Konfiguration der Kennwörter abgeschlossen, erscheint das folgende Fenster (siehe Abbildung 2.35), das Sie nach Herstellung der Internetverbindung zum Download der verfügbaren Updates und Patches für das Betriebssystem des SBS 2003 auffordert.

Abbildung 2.35: Aufforderung zum Download der verfügbaren Patches und Updates für den SBS 2003

16. Sobald Sie auf OK geklickt haben, werden Sie mit der Microsoft Update-Seite im Internet verbunden. Es werden alle für den SBS 2003 verfügbaren Updates und Patches aufgelistet und können danach installiert werden. Möglicherweise ist im Zuge der Installation ein Neustart des Servers erforderlich.

2.7.3 Netzwerkaufgabe: RAS konfigurieren

Mi Hilfe dieses Assistenten wird der SBS 2003 für den Remote-Zugriff per DFÜ und VPN konfiguriert.

1. Im Willkommensfenster klicken Sie auf WEITER. Sie erhalten dann das Fenster RAS-METHODE (siehe Abbildung 2.36).

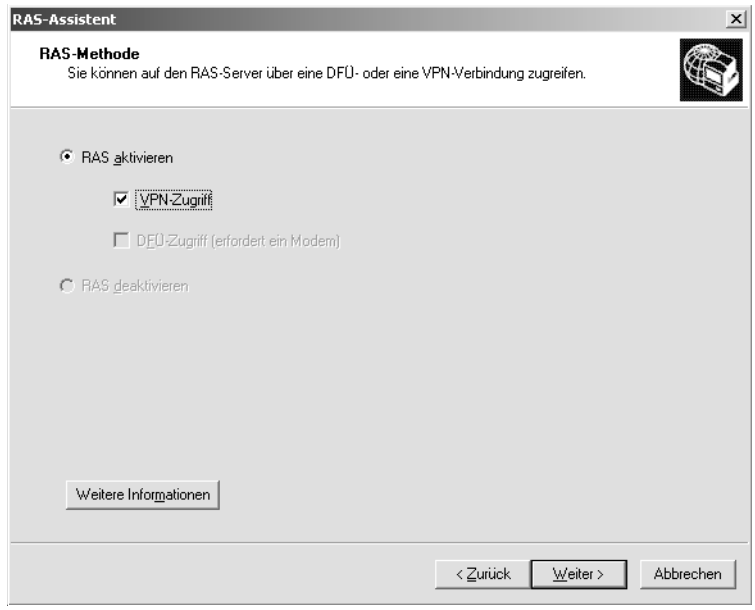


Abbildung 2.36: Die Auswahl der RAS-Methode (VPN oder DFÜ)

Sofern Sie den RAS-Zugriff gestatten möchten wählen Sie die Option RAS AKTIVIEREN. Die Checkbox RAS DEAKTIVIEREN ist erst verfügbar, wenn die RAS-Dienste aktiviert wurden, da diese standardmäßig deaktiviert sind. Als Verbindungstyp können Sie VPN-ZUGRIFF und DFÜ-ZUGRIFF wählen. Im zweiten Fall muss ein Modem auf dem Server installiert sein. Ansonsten ist diese Option nicht anwählbar.

VPN-ZUGRIFF: Bei der Benutzung einer VPN-Verbindung stellt der Remote-Benutzer zunächst eine Verbindung zu seinem Internetdienstanbieter her. Sobald diese Verbindung besteht, wird über Tunneling-Protokolle eine Verbindung zum Server hergestellt. Diese Verbindung wird als sichere Verbindung bezeichnet.

Verwenden Sie für die Internetverbindung einen lokalen Router, müssen Sie möglicherweise auf diesem die Einstellung vornehmen, dass die PPTP-Ports nicht von der Firewall blockiert werden. Die entsprechenden Konfigurationseinstellungen finden Sie in der Dokumentation Ihres Routers. Verwenden Sie hingegen die Firewall des SBS 2003, wird der VPN-Filter aktiviert. Dadurch wird der VPN-Verkehr nicht durch die Firewall blockiert.

DFÜ-ZUGRIFF: Bei dieser Zugriffsart wird die Verbindung über eine Telefonleitung und ein Modem auf dem Server hergestellt. Für die Verwendung des DFÜ-Zugriffs sollten Sie nach Möglichkeit ein anderes Modem auf dem Server verwenden als das Gerät, das Sie für die Faxdienste (siehe Kapitel Abbildung 2.7.8) einsetzen möchten. Wird ein Modem von mehreren Diensten benutzt, kann dies möglicherweise zu Komplikationen führen.

Wenn Sie den RAS-Zugriff für mindestens eine Zugriffsart zugelassen haben, werden die RAS-Richtlinien automatisch so konfiguriert, dass sämtlichen Mitgliedern der Sicherheitsgruppe Mobile Users der RAS-Zugriff gestattet wird.

Klicken Sie dann auf WEITER.

2. Das Fenster CLIENTADRESSIERUNG erhalten Sie, wenn auf dem SBS 2003 nicht der DHCP-Dienst ausgeführt wird (siehe Abbildung 2.37). Sie müssen hier eine Option auswählen, wie den RAS-Clients die IP-Adressen zugewiesen werden sollen.

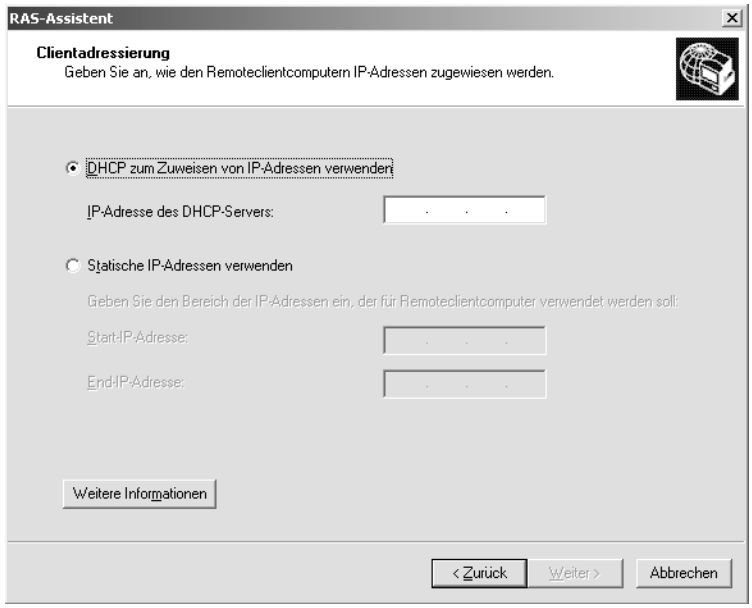


Abbildung 2.37: Auswahl der Zuweisungsmethode von IP-Adressen an die RAS-Clients

Wenn sich in Ihrem Netzwerk ein Gerät befindet, das den DHCP-Serverdienst ausführt, so markieren Sie den Eintrag DHCP ZUM ZUWEISEN VON IP-ADRESSEN VERWENDEN. Dabei ist es gleichgültig, ob es sich um einen weiteren Server oder einen Router handelt. Geben Sie in das entsprechende Feld die IP-Adresse des Geräts ein.

Sobald der Routing- und RAS-Dienst aktiv ist, vergibt der DHCP-Server automatisch zehn Adressen seines aktuellen Adressbereichs an die RAS-Clients. Werden alle zehn IP-Adressen von RAS-Clients verwendet, werden zehn weitere Adressen bereitgestellt.

Ist im Netzwerk kein DHCP konfiguriert, wählen Sie die Option STATISCHE IP-ADRESSEN VERWENDEN. Legen Sie dann den Startwert und Endwert für die Zuteilung von IP-Adressen durch den SBS 2003 fest.

Beachten Sie dabei, dass es zu keinen Überschneidungen mit bereits im Netzwerk vergebenen IP-Adressen kommt und genügend Adressen für alle RAS-Clients bereitgestellt werden. Zudem sollte sich der für die RAS-Clients gewählte Adressbereich mit dem der Netzwerkclients decken.

Klicken Sie dann auf WEITER.

3. Als Letztes bestimmen Sie im Fenster VPN-SERVERNAME (siehe Abbildung 2.38) den Namen oder die IP-Adresse, die für den Zugriff auf den Server über das Internet verwendet werden soll. Der Server wird durch die Konfiguration der RAS-Dienste auch als VPN-Server bezeichnet.

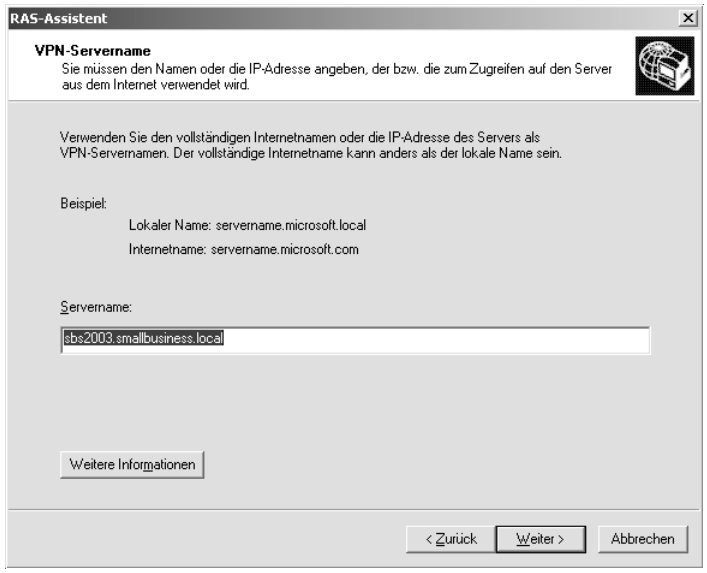


Abbildung 2.38: Festlegen des Namens oder der IP-Adresse für den Zugriff auf den Server über das Internet

Geben Sie in das Feld SERVERNAME den Namen des Servers an. Dabei muss es sich um den vollständigen Hostnamen des Servers im Format *servername.firma.de* handeln. Dieser Name muss also auf dem DNS-Server des Internetdienstanbieters registriert sein. Der hier angegebene Name dient als Standardname des Zielservers in der Konfigurationsdatei des Client-Verbindungsmanagers. Standardmäßig ist in dem Feld SERVERNAME der lokale Name des Servers eingetragen. Alternativ zum vollständigen Namen können Sie auch die IP-Adresse des Servers angeben.

Klicken Sie dann auf WEITER. Sie erhalten eine Zusammenfassung Ihrer Angaben und können den Assistenten über FERTIG STELLEN die Konfigurationen vornehmen lassen.

4. Haben Sie nach dem Abschluss des Assistenten zur Konfiguration der Internetverbindung noch nicht die Kennwortrichtlinien konfiguriert, so werden Sie nun abermals zu diesem Schritt aufgefordert. Führen Sie zur Konfiguration die in Kapitel Abbildung 2.7.2, Schritt 14 beschriebenen Vorgänge aus.

2.7.4 Netzwerkaufgabe: Server aktivieren

Wie bereits seit dem Betriebssystem Windows XP ist auch für den Small Business Server 2003 eine Aktivierung erforderlich. Die Aktivierung erfolgt am bequemsten über das Internet. Hierbei haben Sie die Wahl, ob Sie den Server lediglich aktivieren oder gleichzeitig aktivieren und registrieren möchten.

Bevor der Server nicht aktiviert wurde, können Sie nicht mit dem nächsten Schritt (Clientlizenzen hinzufügen) beginnen.

2.7.5 Netzwerkaufgabe: Clientlizenzen hinzufügen

Die letzte Aufgabe der Netzwerkaufgaben besteht darin, zusätzliche Clientlizenzen hinzuzufügen. Im Lieferumfang des SBS 2003 befinden sich fünf Client-Zugriffslizenzen (CALs). Sind in Ihrem Netzwerk lediglich fünf Clients vorhanden, können Sie diese Aufgabe überspringen.

1. Nach der Willkommensmeldung erhalten Sie das Fenster LIZENZVERTRAG (siehe Abbildung 2.39). Lesen Sie sich die Bestimmungen des Microsoft Client-Zugriffs-Lizenzvertrages durch und wählen dann die Option ICH STIMME ZU. Sofern Sie nicht zustimmen, kann diese Aufgabe nicht weiter durchgeführt werden. Klicken Sie dann auf WEITER.

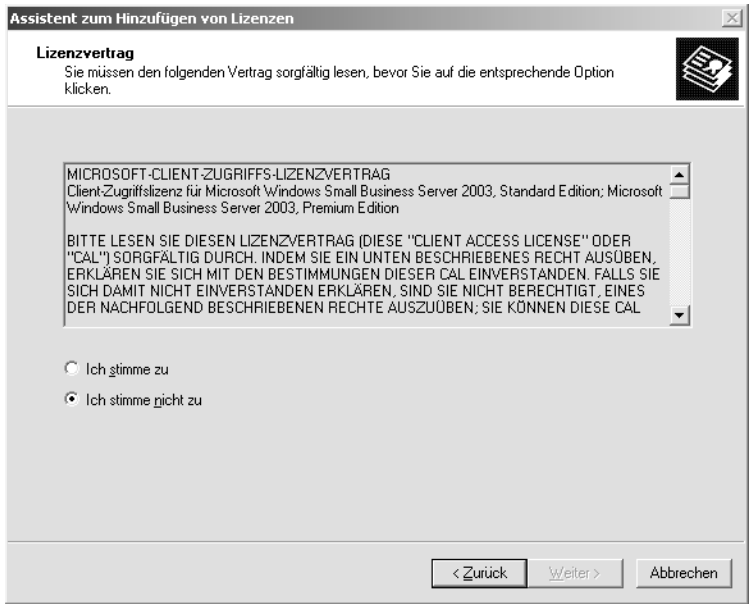


Abbildung 2.39: Der Microsoft Client-Zugriffs-Lizenzvertrag

2. Im Fenster KONTAKTMETHODE (siehe Abbildung 2.40) bestimmen Sie, ob Sie das Hinzufügen von Clientlizenzen per INTERNET oder per TELEFON durchführen möchten. Klicken Sie danach auf WEITER.

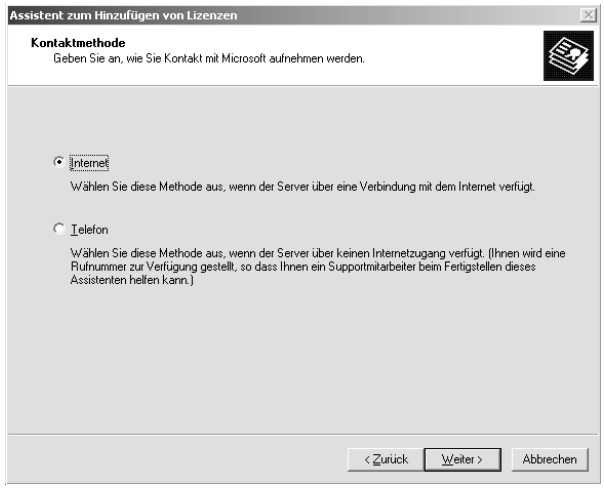


Abbildung 2.40: Auswahl der Kontaktmethode für die Clientlizenzierung

3. Jetzt müssen Sie im Fenster LIZENZNUMMERNINFORMATIONEN (siehe Abbildung 2.41) in das Feld LIZENZNUMMER den 25-stelligen Lizenzcode eingeben und auf HINZUFÜGEN klicken. Hier können Sie nacheinander beliebig viele Lizenznummern eingeben. Im Abschnitt HINZUZUFÜGENDE LIZENZNUMMERN sehen Sie, welche Nummern wie viele Lizenzen umfassen. Überprüfen Sie, ob die Lizenznummern korrekt eingegeben worden sind. Finden Sie hier einen Fehler, löschen Sie diese Nummer und geben sie erneut ein. Falsch eingegebene Lizenznummern verzögern die Aktivierung der Lizenzen. Klicken Sie dann auf WEITER.

Abbildung 2.41: Die Eingabe der Lizenznummern

4. Die Lizenzaktivierung wird nun abgeschlossen. Folgen Sie dazu den Hinweisen des Assistenten. Wollen Sie später weitere CALs hinzufügen, rufen Sie erneut diesen Punkt in der Aufgabenliste auf.

2.7.6 Verwaltungsaufgabe: Drucker hinzufügen

Nach Abschluss der Netzwerkaufgaben müssen Sie einige Verwaltungsaufgaben durchführen. Als Erstes werden die Drucker zum Netzwerk hinzugefügt.

Sie müssen den Assistenten zum Hinzufügen der Drucker nicht ausführen, wenn Sie über einen Plug & Play-fähigen Drucker verfügen, der via USB, Infrarot oder einen anderen IEEE 1394-basierten Anschluss am Server betrieben wird. In diesem Fall kabeln Sie den Drucker an, und er wird automatisch installiert.

1. Nach dem Willkommensfenster erhalten Sie die Seite LOKALER DRUCKER ODER NETZWERK. Bestimmen Sie hier, ob der Drucker lokal am SBS angeschlossen ist oder an einem anderen Computer (siehe Abbildung 2.42). Bei der Verwendung eines Printservers lesen Sie die Dokumentation des Geräts. Klicken Sie dann auf WEITER.

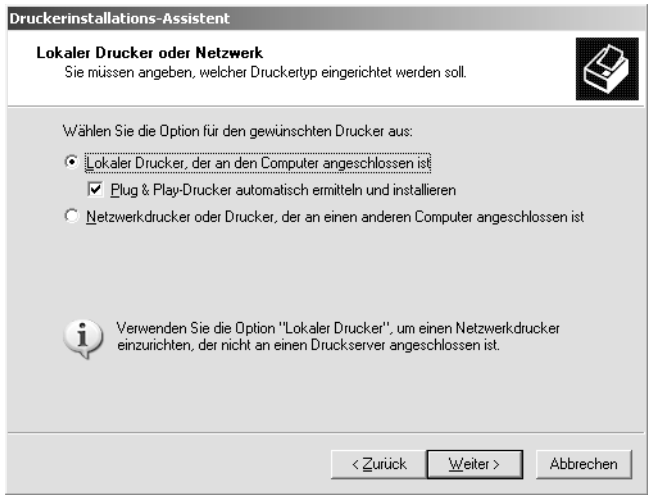


Abbildung 2.42: Konfigurationsauswahl für einen lokalen oder Netzwerkdrucker

2. Im Fenster DRUCKERANSCHLUSS AUSWÄHLEN (siehe Abbildung 2.43) legen Sie fest, an welchem Anschluss der Drucker an den Server angeschlossen ist. In der Regel handelt es sich dabei um den Anschluss LPT1. Klicken Sie danach auf WEITER.
3. Dann wird im Fenster DRUCKERSOFTWARE INSTALLIEREN (siehe Abbildung 2.44) der Drucker aus der Hersteller- und Druckerliste ausgewählt. Befindet sich der Drucker nicht in der List oder haben Sie einen separaten Datenträger für den Druckertreiber, klicken Sie auf DATENTRÄGER und folgen den weiteren Anweisungen. Klicken Sie auf WEITER.

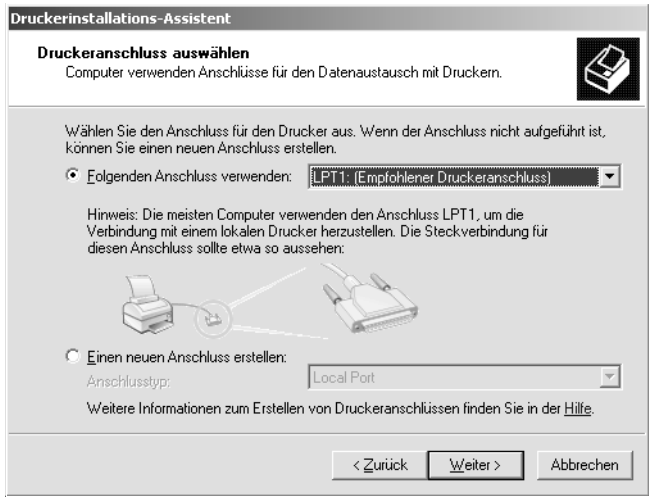


Abbildung 2.43: Auswahl des Anschlusses für den Drucker

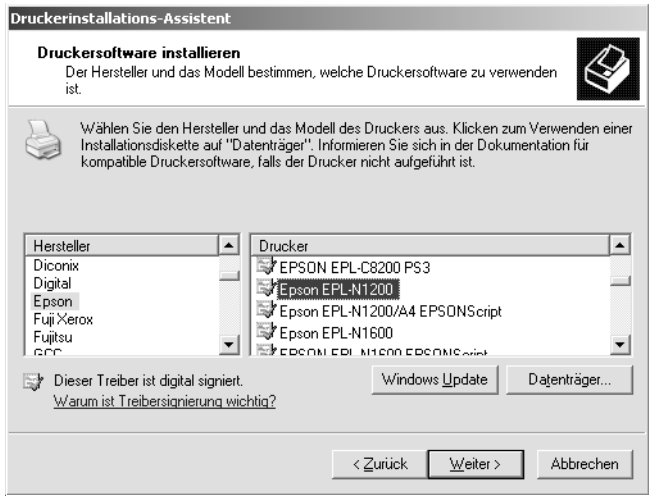


Abbildung 2.44: Auswahl des Druckerherstellers und des Druckermodells

4. Als Nächstes geben Sie dem Drucker im Fenster DRUCKER BENENNEN einen Namen. Dieser Name darf maximal 31 Zeichen umfassen. Zusätzlich bestimmen Sie, ob dieser Drucker als Standarddrucker verwendet werden soll oder nicht. Klicken Sie dann auf WEITER.
5. Im Fenster DRUCKERFREIGABE (siehe Abbildung 2.45) legen Sie fest, ob Sie diesen Drucker für die Benutzung von anderen Benutzern freigeben möchten. Soll der Drucker freigegeben werden, geben Sie in das Feld FREIGABENAME einen Namen für den Drucker an. Klicken Sie dann auf WEITER.

Abbildung 2.45: Festlegen, ob der Drucker im Netzwerk freigegeben werden soll oder nicht

6. Danach können Sie optional im Fenster STANDORT UND KOMMENTAR in die entsprechenden Textfelder Angaben zum Standort des Drucker sowie einen Kommentar zum Drucker eintragen. Klicken Sie danach auf WEITER.
7. Abschließend werden Sie im Fenster TESTSEITE DRUCKEN gefragt, ob nach der Installation des Druckertreibers eine Testseite gedruckt werden soll. Sie sollten dies tun, um sich zu überzeugen, dass der Drucker korrekt installiert ist. Klicken Sie hier auf WEITER.
8. Sie erhalten zum Schluss eine Zusammenfassung des Assistenten. Dort klicken Sie auf FERTIG STELLEN, um den Drucker hinzuzufügen.

2.7.7 Verwaltungsaufgabe: Benutzer und Computer hinzufügen

Dieser Konfigurationsschritt beinhaltet eine Reihe von Aufgaben. Es wird für jeden Benutzer ein Benutzerkonto, Postfach und Basisordner eingerichtet. Weiterhin werden die Mitgliedschaften des Benutzers in den Sicherheits- und Verteilergruppen festgelegt. Auch die SharePoint-Zugriffe sowie die Datenträgerkontingente werden konfiguriert. Schließlich wird dem Benutzer noch ein Clientcomputer zugewiesen.

1. Bevor Sie den Benutzer erstellen, müssen Sie für ihn im Fenster VORLAGENAUSWAHL (siehe Abbildung 2.46) eine Benutzervorlage auswählen. Standardmäßig sind bereits die folgenden vier Benutzervorlagen vorhanden:

- USER TEMPLATE: In dieser Vorlage ist der Zugriff auf das Internet, E-Mail, Netzwerkdrucker, Faxgeräte und freigegebene Ordner gestattet. Diese Vorlage sollte für normale Benutzerkonten angewendet werden.

- MOBILE USER TEMPLATE: In dieser Vorlage sind alle Berechtigungen des User Templates enthalten. Zusätzlich kann eine Verbindung auf den SBS 2003 per VPN-Zugriff oder DFÜ-Zugriff hergestellt werden.
- POWER USER TEMPLATE: Diese Vorlage beinhaltet alle Berechtigungen des Mobile User Templates. Weiterhin können Benutzer, die auf dieser Vorlage basierend arbeiten, Benutzer, Gruppen, Drucker, Faxe und freigegebene Ordner verwalten. Sie können auch eine Remote-Verbindung mit dem Server herstellen. Eine lokale Anmeldung am Server ist jedoch nicht möglich.
- ADMINISTRATOR TEMPLATE: Diese Vorlage verfügt über einen uneingeschränkten Zugriff für die Server- und Domänenverwaltung.

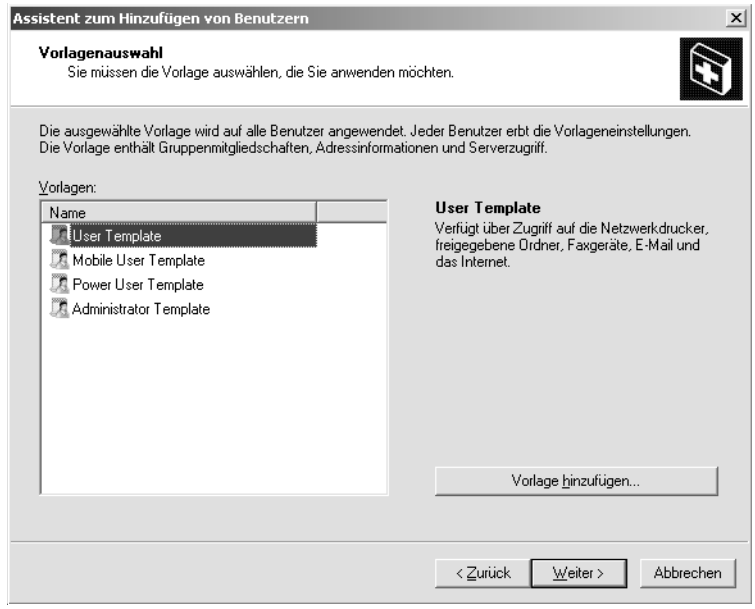


Abbildung 2.46: Auswahl der Benutzervorlage, die auf den Benutzer angewendet werden soll

Neben diesen vordefinierten Benutzervorlagen können Sie auch noch eigene Benutzervorlagen erstellen. Weiterhin können Sie zu einem späteren Zeitpunkt für jeden Benutzer die Benutzervorlage ändern.

Nachdem Sie die passende Vorlage gewählt haben, klicken Sie auf WEITER.

2. Im Fenster BENUTZERINFORMATIONEN (siehe Abbildung 2.47) können Sie über HINZUFÜGEN einen neuen Benutzer für die gewählte Vorlage erstellen. Haben Sie bereits einige neue Benutzer für die Vorlage erstellt, so finden Sie diese unter BENUTZER aufgelistet.

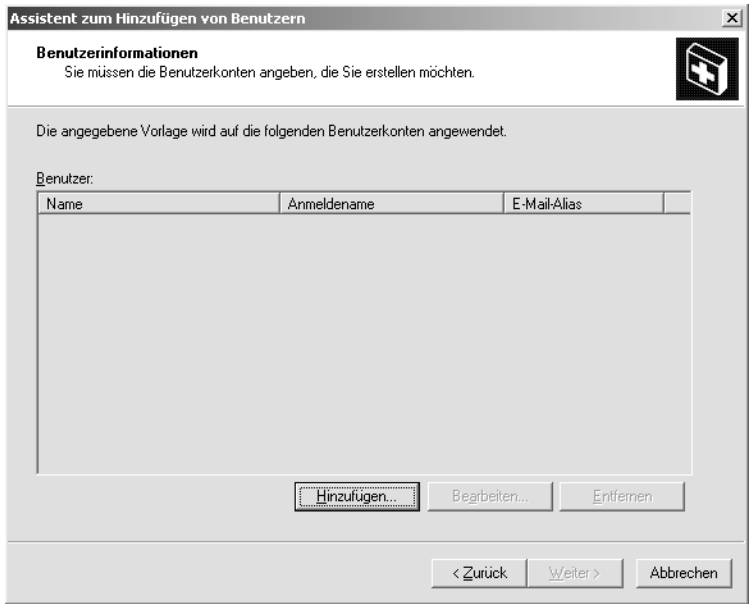


Abbildung 2.47: Die Benutzerinformationen

3. Nachdem Sie eben auf HINZUFÜGEN geklickt haben, füllen Sie im Fenster BENUTZERINFORMATIONEN ANGEBEN (siehe Abbildung 2.48) die entsprechenden Felder aus. Für das Feld ANMELDENAME können Sie aus der Liste eines von vier verfügbaren Formaten auswählen, wie der Anmeldename lauten soll. In unserem Beispiel können Sie zwischen *Pmustermann*, *MustermannPeter*, *PMustermann* und *PeterM* wählen. Der hier gewählte Wert wird standardmäßig auch für das Feld E-Mail-Alias übernommen, jedoch können Sie dieses auch ändern. Haben Sie die Eingaben abgeschlossen, klicken Sie auf OK.

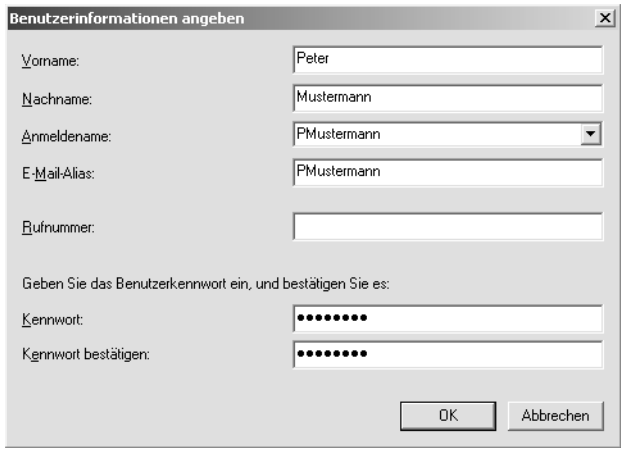


Abbildung 2.48: Die Eingabe der Benutzerinformationen

4. Im Fenster CLIENTCOMPUTER (siehe Abbildung 2.49) können Sie für den Benutzer auch einen Computer einrichten. Wenn Sie die Option COMPUTER JETZT EINRICHTEN wählen, wird dieser in den folgenden Schritten konfiguriert. Klicken Sie dann auf WEITER.

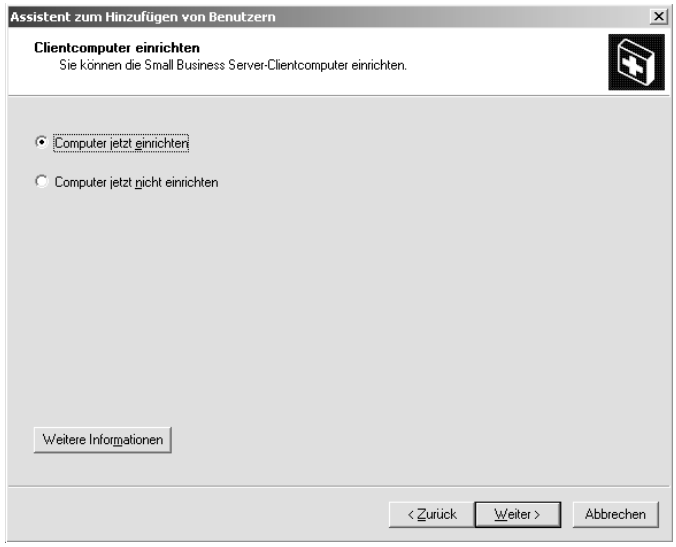


Abbildung 2.49: Dem Benutzerkonto einen Clientcomputer zuweisen

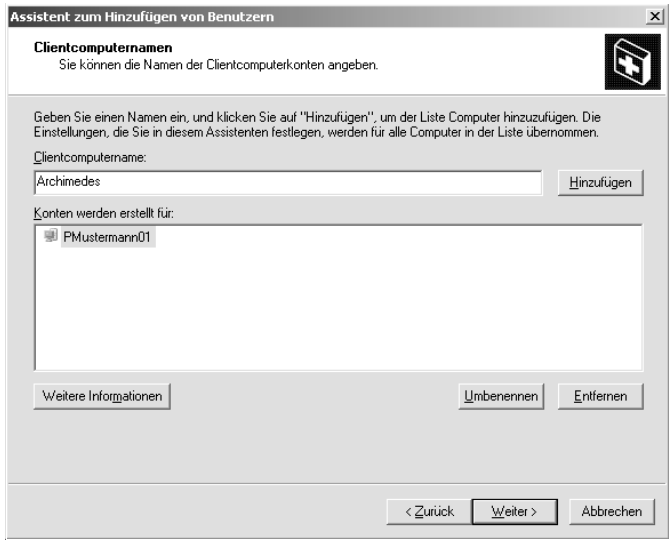


Abbildung 2.50: Bestimmen des Computers für den Benutzer

5. Im Fenster CLIENTCOMPUTERNAMEN (siehe Abbildung 2.50) geben Sie den Namen des Computers an und klicken dann auf HINZUFÜGEN. Gültige Zeichen für den Computernamen sind A–Z, a–z, 0–9 sowie - (Bindestrich). Alle Informationen, die Sie über den

Assistenten festlegen, werden für sämtliche Computer übernommen, die sich in der Liste KONTEN WERDEN ERSTELLT FÜR befinden. Aus dieser Liste können Sie auch wieder Computer entfernen. Der standardmäßige Name des Computerkontos lautet immer *Benutzername01*, in unserem Beispiel *PMustermann01*. Dieser Name kann jedoch gelöscht und durch einen anderen ersetzt werden. Klicken Sie dann auf WEITER.

6. Als Nächstes werden im Fenster CLIENTANWENDUNGEN (siehe Abbildung 2.51) die Applikationen ausgewählt, die auf dem Computer installiert werden sollen. Standardmäßig werden dort die Applikationen *Clientbetriebssystem-Service Packs*, *Internet Explorer 6.0*, *Outlook 2003* sowie der *Faxclient* installiert. Diese Auswahl können Sie jedoch ändern und ergänzen.

Deaktivieren Sie die Checkbox vor einer bereits installierten Applikation, so wird diese dadurch *nicht* vom Clientcomputer deinstalliert.

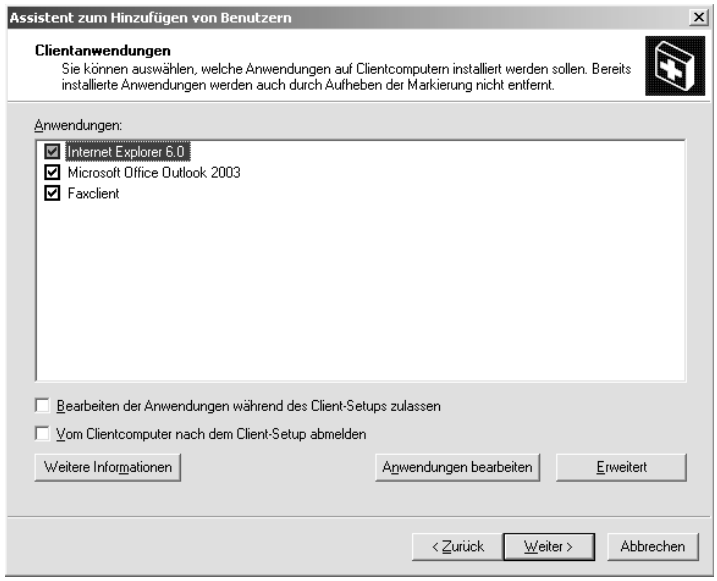


Abbildung 2.51: Festlegen der Clientapplikationen, die auf dem Computer installiert werden sollen

Haben Sie Outlook 2003 für die Installation ausgewählt und ist auf den Clients bereits eine frühere Outlook-Version installiert, müssen Sie auf den Clients die COM-Add-Ins deaktivieren. Führen Sie dazu auf dem Client unter Outlook die folgenden Schritte aus:

- Wählen Sie aus dem Menü EXTRAS den Eintrag OPTIONEN und wechseln dann auf die Registerkarte WEITERE.
- Klicken Sie auf ERWEITERTE OPTIONEN und danach auf COM-ADD-INS.
- Deaktivieren Sie die Checkbox bei dem Add-In.

7. Markieren Sie im Fenster CLIENTANWENDUNGEN die Checkbox BEARBEITEN DER ANWENDUNGEN WÄHREND DES CLIENT-SETUPS ZULASSEN, wenn Sie dem Benutzer während der Installation gestatten möchten, einen anderen Installationspfad oder eine Applikation nicht zu installieren. Die Checkbox VOM CLIENTCOMPUTER NACH DEM CLIENT-SETUP ABMELDEN sollten Sie dann aktivieren, wenn das Beenden des Setups vom Benutzer nicht abgewartet werden kann und niemand nach Ende der Installation unbefugt auf den Computer zugreifen soll.
8. Klicken Sie auf ANWENDUNGEN BEARBEITEN, erhalten Sie das Fenster VERFÜGBARE ANWENDUNGEN (siehe Abbildung 2.52). Hier sind alle Applikationen aufgelistet, die für die Installation bereitstehen. Über HINZUFÜGEN können Sie noch weitere Applikationen für die Installation auf den Clients bereitstellen.

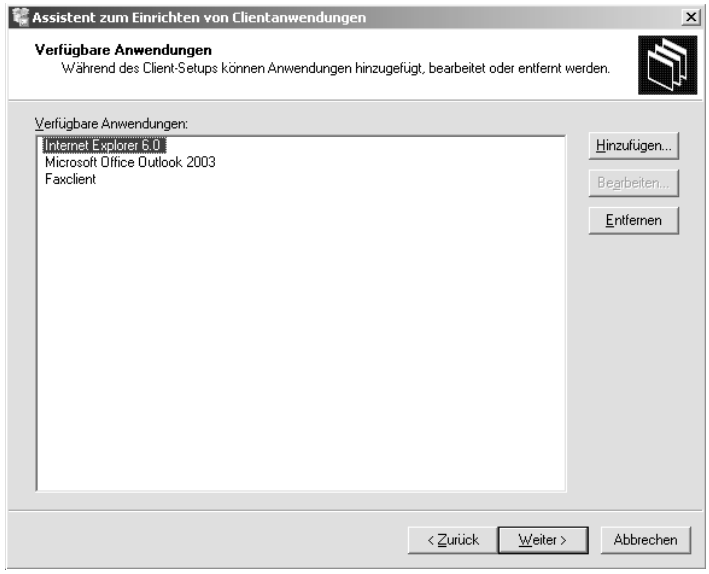


Abbildung 2.52: Für die Clientinstallation verfügbare Applikationen

Haben Sie sich entschieden, eine weitere Applikation hinzuzufügen, erhalten Sie das Fenster ANWENDUNGSINFORMATIONEN (siehe Abbildung 2.53).

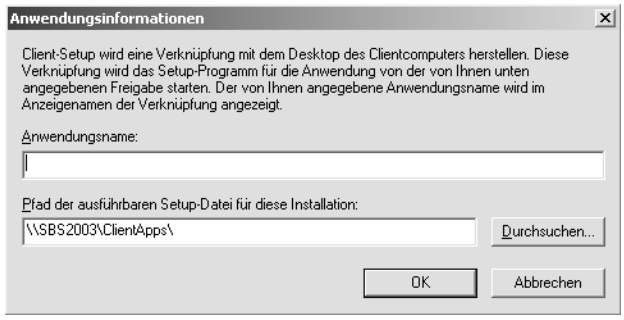


Abbildung 2.53: Angabe der weiteren zu installierenden Clientapplikationen

Bevor Sie hier eine Applikation hinzufügen können, müssen Sie das Installationsprogramm in eine Freigabe kopieren. Am sinnvollsten ist es, diese Applikationen in das Standardverzeichnis \CLIENTAPPS auf dem SBS2003 aufzunehmen. Für den freigegebenen Ordner müssen die Domänenbenutzer über die Berechtigung *Lesen* und *Ausführen* verfügen. Ansonsten können sie die Installation nicht ausführen.

9. Geben Sie im Textfeld ANWENDUNGSNAME einen Namen für die Applikation an und wählen über DURCHSUCHEN den Pfad zu der Applikation. Für diese Applikation wird auf dem Desktop des Clients eine Verknüpfung angelegt. Klicken Sie dann auf OK. Sie gelangen wieder auf das Fenster VERFÜGBARE ANWENDUNGEN (siehe Abbildung 2.52) zurück. Dort können Sie die hinzugefügten Applikationen jederzeit bearbeiten. Für die standardmäßig vorhandenen ist die Funktion BEARBEITEN nicht verfügbar. Auch das Löschen von Applikationen aus der Liste ist möglich. Klicken Sie hier auf WEITER, und der Assistent zum Hinzufügen neuer Anwendungen wird beendet.
10. Sie gelangen dann wieder auf die Seite CLIENTANWENDUNGEN (siehe Abbildung 2.51). Wenn Sie dort auf ERWEITERT klicken, erhalten Sie das Fenster ERWEITERTE CLIENTCOMPUTEREINSTELLUNGEN (siehe Abbildung 2.54).

Abbildung 2.54: Erweiterte Einstellungen für den Clientcomputer

Für jeden der aufgeführten Punkte können Sie die Standardeinstellung für den Clientcomputer übernehmen, indem Sie die jeweilige Checkbox markieren.

Für die einzelnen Punkte sind die folgenden Standardeinstellungen festgelegt:

- INTERNET EXPLORER-EINSTELLUNGEN: Als Startseite ist die interne Firmenwebsite (*http://Companyweb*) eingestellt. In den Favoriten befinden sich Links zu verschiedenen internen Webseiten. Wurde der ISA Server installiert, ist der Internet Explorer auch für die Verwendung des Proxy-Servers eingerichtet.
- OUTLOOK-PROFILEINSTELLUNGEN: Outlook ist für die Benutzung des Exchange Servers konfiguriert. So werden in den Profilen für neue Benutzer die Kontoinformationen sowie die Exchange Server-Einstellungen verwendet. Sind auf dem Computer bereits Profile vorhanden, wird das Exchange-Profil des SBS hinzugefügt und als Standard festgelegt. Zusätzlich ist der Faxmailtransport konfiguriert. Dieser ermög-

licht das Senden von Faxen aus Outlook und anderen E-Mail-Applikationen heraus. Ist für den Clientcomputer die Remote-Verwendung eingestellt, wird unter Outlook die manuelle Synchronisation von Outlook-Ordnern eingerichtet.

- DESKTOP-EINSTELLUNGEN: Im Ordner Netzwerkumgebung werden Verknüpfungen und Links erstellt.
- FAXDRUCKER: Auf dem Computer wird ein Faxdrucker eingerichtet, der die Verbindung zum Faxserver verwendet.
- DRUCKER: Es wird der im Active Directory veröffentlichte Drucker vom SBS den Clients als Standarddrucker hinzugefügt. Sind im Active Directory jedoch mehrere Drucker veröffentlicht oder ist an den Client ein lokaler Drucker angeschlossen, so wird kein Standarddrucker festgelegt.
- FAXKONFIGURATIONSINFORMATIONEN: Es werden die vom SBS gespeicherten Faxinformationen an die Clients weitergegeben. Dazu zählt beispielsweise das Faxdeckblatt mit den Absenderinformationen, so dass die Benutzer diese Angaben nicht für jedes Fax erneut angeben müssen.
- REMOTE-DESKTOP: Für die Clients werden der Remote-Desktop sowie die Remote-Desktop-Unterstützung aktiviert. Über den Remote-Desktop können die Benutzer beispielsweise von zu Hause oder von unterwegs eine Sitzung mit ihrem Clientcomputer herstellen. Über die Remote-Desktop-Unterstützung wird es anderen Benutzern ermöglicht, eine Verbindung zum Client herzustellen und beim Beheben von Problemen einzugreifen.

Wird die Checkbox deaktiviert, können Sie die Einstellung auf dem Client manuell konfigurieren. Klicken Sie dann auf OK.

11. Als Nächstes erhalten Sie die Seite MOBILCLIENT UND OFFLINEVERWENDUNG (siehe Abbildung 2.55).

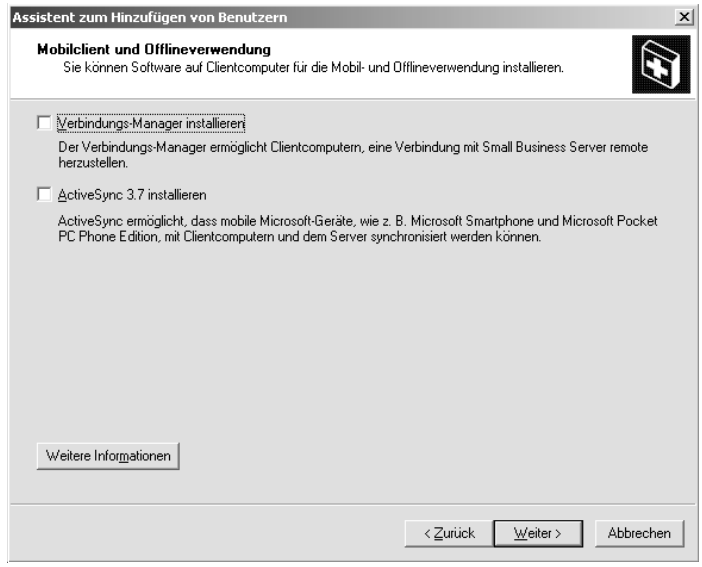


Abbildung 2.55: Konfiguration des Computers für die Mobil- und Offline-Benutzung

Sie haben hier die Möglichkeit, den Verbindungs-Manager und ActiveSync 3.7 zu installieren.

- VERBINDUNGS-MANAGER: Mit Hilfe des Verbindungs-Managers können die Benutzer eine Remote-Verbindung mit dem SBS 2003 herstellen.
- ACTIVESYNC 3.7: Über ActiveSync können die Benutzer mobile Geräte wie z.B. Microsoft Smartphone oder Microsoft Pocket PC Phone Edition mit dem Clientcomputer und Server synchronisieren.

Damit die Benutzer die Remote-Verbindung nutzen können, müssen Sie den Assistenten für die RAS-Verbindung abgeschlossen haben. Zusätzlich muss der Benutzer zu der Benutzervorlage Mobile Users (siehe Schritt 1 in diesem Kapitel) hinzugefügt worden sein.

Klicken Sie anschließend auf WEITER.

12. Sie erhalten nun das Fenster FERTIGSTELLEN DES ASSISTENTEN (siehe Abbildung 2.56). Sofern Sie mit den Einstellungen einverstanden sind, klicken Sie auf FERTIG STELLEN. Über ZURÜCK können Sie noch Änderungen an der Konfiguration vornehmen.

Abbildung 2.56: Fertigstellen des Assistenten für das Hinzufügen von Benutzern

13. Während die Einstellungen für den Benutzer konfiguriert werden, erhalten Sie ein Hinweisfenster (siehe Abbildung 2.57). Um die Konfiguration des Clientcomputers inklusive seiner Netzwerkkonfiguration und der Anwendungsbereitstellung abzuschließen, müssen Sie sich auf dem Client anmelden und im Browser die Adresse *http://SBSServername/ConnectComputer* eingeben. Klicken Sie zum Bestätigen auf OK.

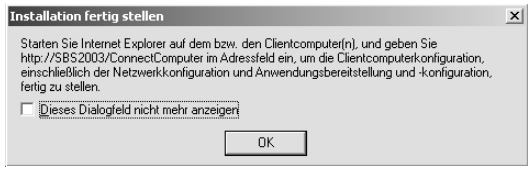


Abbildung 2.57: Hinweis für den Abschluss der Clientcomputerkonfiguration

14. Nachdem das Benutzerkonto erstellt worden ist, werden Sie gefragt, ob Sie den Assistenten erneut starten möchten, um einen neuen Benutzer anzulegen. Haben Sie hier NEIN gewählt, erfolgt noch ein Hinweisfenster (siehe Abbildung 2.58), das Sie darüber informiert, dass Sie nun für die Benutzerkonten die Übermittlung von POP3-E-Mail konfigurieren können. Bestätigen Sie dieses Fenster mit OK.

Abbildung 2.58: Hinweisfenster für die Konfiguration von POP3-E-Mail

2.7.8 Verwaltungsaufgabe: Fax konfigurieren

Mit Hilfe dieses Assistenten wird der SBS 2003 für den Empfang, das Senden und Weiterleiten von Faxen eingerichtet. Diese Verwaltungsaufgabe können Sie nur ausführen, wenn auf dem Server mindestens ein Faxmodem installiert ist.

1. Als Erstes erstellen Sie im Fenster FIRMENINFORMATIONEN ANGEBEN (siehe Abbildung 2.59) die Informationen, die auf dem Deckblatt der Faxe gesendet werden sollen.

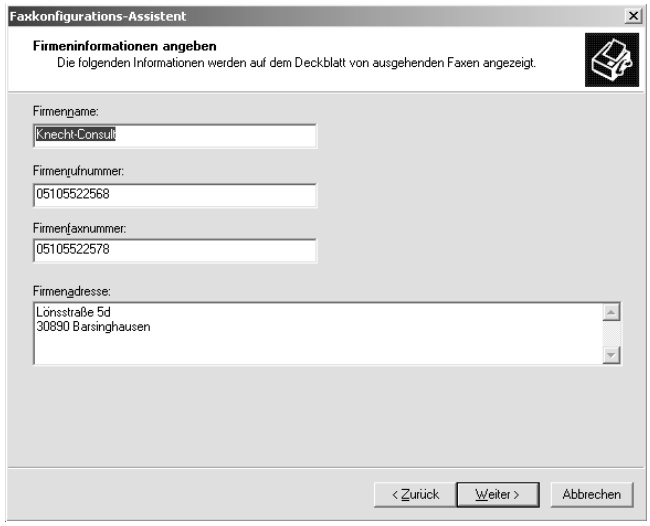


Abbildung 2.59: Das Festlegen der Firmeninformationen für das Faxdeckblatt

Füllen Sie dazu die Felder Firmenname, Firmenrufnummer, Firmenfaxnummer sowie Firmenadresse aus. Die bereits eingetragenen Werte beruhen auf den Angaben, die Sie während der Konfiguration des Servers (siehe Abbildung 2.5) angegeben haben. Die Angaben können hier jedoch modifiziert werden. Klicken Sie dann auf WEITER.

2. Im Fenster GERÄTE FÜR AUSGEHENDE FAXE (siehe Abbildung 2.60) sehen Sie eine Liste der von Windows erkannten Faxgeräte.

Abbildung 2.60: Die Liste der installierten Faxgeräte

Aktivieren Sie die Checkboxen der Geräte, die Sie verwenden möchten. Sind mehrere Faxmodems installiert, so können Sie die Reihenfolge der Verwendung ändern. Ist ein Faxgerät gerade in Benutzung, wird automatisch das nächste Gerät in der Liste verwendet. Klicken Sie dann auf WEITER.

3. Danach werden die Geräte bestimmt, die für den Faxempfang benutzt werden sollen (siehe Abbildung 2.61).

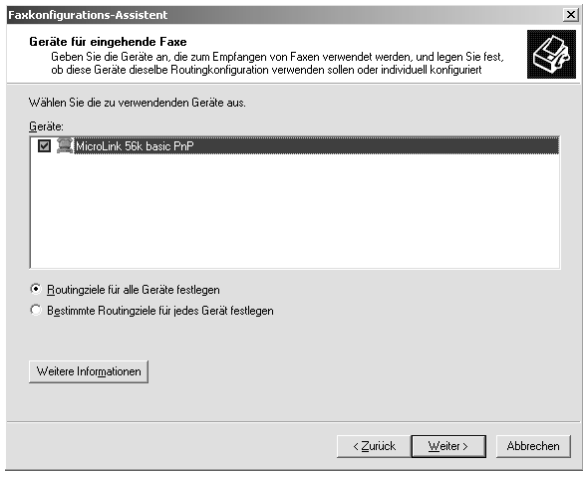


Abbildung 2.61: Die Auswahl der Geräte für eingehende Faxe

Aktivieren Sie hier die Checkbox vor den Geräten, die Sie für den Faxempfang verwenden möchten. Sind mehrere Geräte vorhanden, können Sie bestimmen, ob Sie für alle Geräte dieselbe Routingmethode verwenden möchten (Option ROUTINGZIELE FÜR ALLE GERÄTE FESTLEGEN) oder ob die Geräte separat konfiguriert werden sollen (Option BESTIMMTE ROUTINGZIELE FÜR JEDES GERÄT FESTLEGEN). Klicken Sie dann auf WEITER.

4. Im Fenster ROUTING VON EINGEHENDEN FAXEN (siehe Abbildung 2.62) legen Sie die Routingmethode für das Faxgerät fest. Achten Sie darauf, für jedes Gerät mindestens eine Methode zu bestimmen.

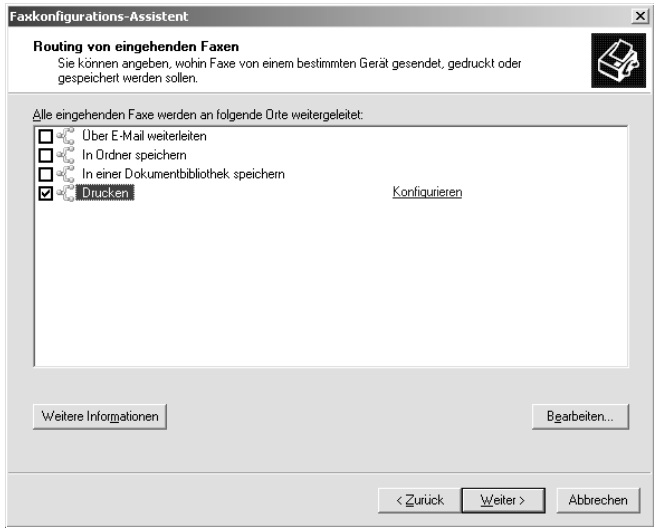


Abbildung 2.62: Die Routingmethode für die Faxgeräte festlegen

Es stehen vier verschiedene Routingmethoden zur Verfügung:

ÜBER E-MAIL WEITERLEITEN: Die Faxe werden an eine E-Mail-Adresse weitergeleitet. Dabei kann es sich um eine Adresse innerhalb oder außerhalb des SBS-Netzwerks handeln.

IN ORDNER SPEICHERN: Bei dieser Option werden die Faxe an einen Ordner weitergeleitet. Dieser Ordner muss über eine Freigabe verfügen.

IN EINER DOKUMENTENBIBLIOTHEK SPEICHERN: Hiermit werden die Faxe an die Dokumentenbibliothek der internen Firmenwebsite weitergeleitet. Unter SBS 2003 ist für eingehende Faxe standardmäßig der Ordner *http://SBSServername/companyweb/incoming%20faxes* vorgesehen.

DRUCKEN: Die Faxe werden direkt an einen installierten Drucker weitergeleitet und ausgedruckt.

Beim ersten Ausführen des Assistenten erscheint der Link KONFIGURIEREN, sobald Sie eine Routingmethode auswählen. Wird der Assistent später erneut durchgeführt, markieren Sie die Methode und klicken auf BEARBEITEN, um den vorhandenen Eintrag zu modifizieren. Klicken Sie dann auf WEITER.

5. Zum Schluss erhalten Sie wieder eine Zusammenfassung der Einstellungen. Bestätigen Sie diese mit FERTIG STELLEN.

2.7.9 Verwaltungsaufgabe: Überwachung konfigurieren

Mit Hilfe dieses Assistenten können Sie Warnungsbenachrichtigungen sowie Serverleistungs- und Nutzungsberichte konfigurieren. Es wird hier ein Zeitplan eingerichtet, gemäß dem die Berichte und Benachrichtigungen per Mail gesendet werden. Die Berichte können auch über die Serververwaltung angezeigt werden.

1. Im Fenster BERICHTERSTATTUNGSOPTIONEN (siehe Abbildung 2.63) bestimmen Sie, wie die einzelnen Berichte angezeigt und empfangen werden sollen.

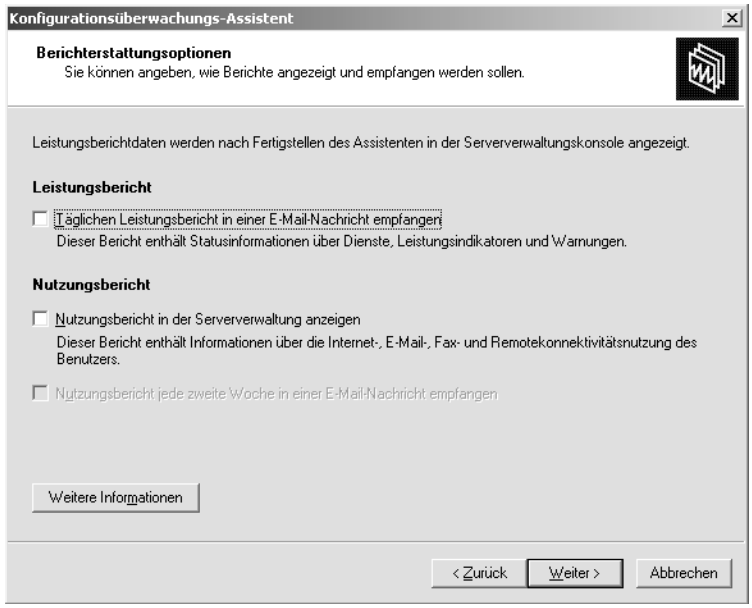


Abbildung 2.63: Die Berichterstattungsoptionen für die Leistungs- und Nutzungsberichte

Die Leistungsberichte werden automatisch nach Abschluss des Assistenten in der Serververwaltung unter Überwachung und Berichterstattung angezeigt. Die Leistungsdaten werden stündlich gesammelt. Zusätzlich können Sie über die Option TÄGLICHEN LEISTUNGSBERICHT IN EINER E-MAIL-NACHRICHT EMPFANGEN bestimmen, dass der Bericht auch per Mail gesendet wird.

In den Nutzungsberichten sind Informationen zu der Internet-, E-Mail-, Fax- sowie Remote-Nutzung des Servers enthalten. Ist die Option NUTZUNGSBERICHT IN DER SERVERVERWALTUNG ANZEIGEN gewählt, können Sie zusätzlich noch Folgendes festlegen: NUTZUNGSBERICHT JEDE ZWEITE WOCHE IN EINER E-MAIL-NACHRICHT EMPFANGEN. Klicken Sie dann auf WEITER.

2. Im Fenster E-MAIL-OPTIONEN (siehe Abbildung 2.64) bestimmen Sie eine oder mehrere E-Mail-Adressen, an welche die Berichte gesendet werden sollen. Möchten Sie mehrere Adressen angeben, so trennen Sie diese jeweils durch ein Semikolon (;). Die Auswahl der E-Mail-Adresse wird nur angezeigt, wenn Sie im vorherigen Schritt für einen oder beide Berichte die E-Mail-Funktion aktiviert haben.

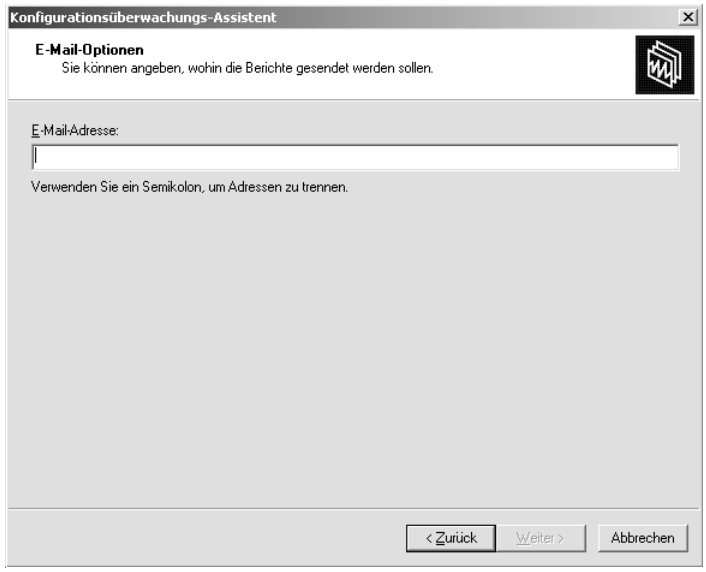


Abbildung 2.64: Festlegen der E-Mail-Adresse(n), an welche die Berichte gesendet werden sollen

Klicken Sie dann auf WEITER.

3. Unter NUTZUNGSBERICHT FÜR DIE GESCHÄFTSINHABER (siehe Abbildung 2.65) können Sie bestimmen, welche Personen die Nutzungsberichte auf einer Seite der Intranet-Webseite ansehen dürfen. Standardmäßig dürfen nur Mitglieder der Gruppe Domänen-Admins diese Berichte ansehen.

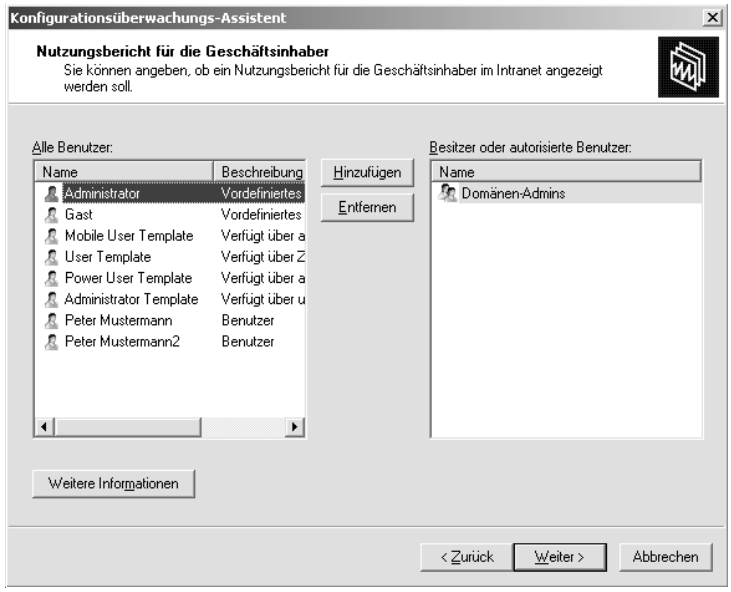


Abbildung 2.65: Auswahl der Personen für die Ansicht der Nutzungsberichte

Um weiteren Benutzern die Ansicht der Berichte zu gestatten, wählen Sie aus der Liste ALLE BENUTZER die gewünschten aus und klicken auf HINZUFÜGEN. Alle ausgewählten Personen erhalten automatisch eine E-Mail, in denen sie über die Funktion der Nutzungsberichte sowie der Zugriffsmöglichkeit darauf informiert werden. Der Nutzungsbericht steht unter *http://SBSServername/monitoring* bereit. Klicken Sie dann auf WEITER.

4. Im Fenster WARNUNGEN (siehe Abbildung 2.66) können Sie festlegen, ob Sie über eine Leistungswarnung sofort per E-Mail informiert werden möchten.

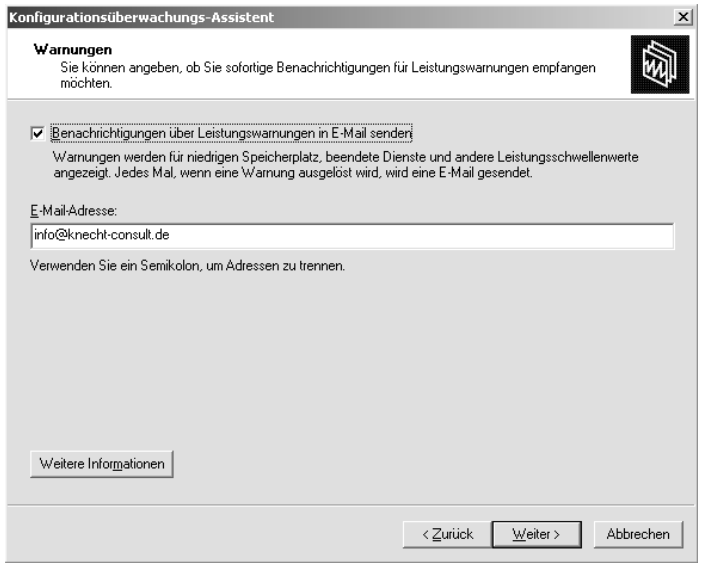


Abbildung 2.66: Festlegen der Benachrichtigung für Leistungswarnungen

Für die sofortige Information bei der Überschreitung eines Leistungsschwellenwerts tragen Sie eine oder mehrere E-Mail-Adressen ein. Mehrere Adressen werden durch ein Semikolon (;) voneinander getrennt. Standardmäßig ist im Feld E-MAIL-ADRESSE bereits die Adresse eingetragen, die Sie in Schritt 2 festgelegt haben.

Die Schwellenwerte für die verschiedenen Leistungsbereiche können Sie nach Abschluss des Assistenten in der Serververwaltung unter ÜBERWACHUNG UND BERICHTERSTATTUNG/WARNUNGSBENACHRICHTIGUNGEN KONFIGURIEREN festlegen. Dieses Verfahren wird in Kapitel 8.8 näher beschrieben. Klicken Sie dann auf WEITER.

5. Damit ist der Assistent abgeschlossen. Klicken Sie zum Beenden auf FERTIG STELLEN.

2.7.10 Verwaltungsaufgabe: Sicherung konfigurieren

Dieser Assistent führt Sie durch die Planung und Konfiguration der Sicherung für den SBS 2003.

1. Nach dem Willkommensfenster erhalten Sie das Fenster SICHERUNGSORT (siehe Abbildung 2.67). Hier können Sie entscheiden, ob Sie die Sicherung auf einem Bandlaufwerk oder einer Festplatte bzw. Netzwerkfreigabe erstellen möchten. Die erste Option steht Ihnen nur zur Verfügung, wenn vom Sicherungsassistenten ein Band-

laufwerk gefunden wurde. Anderenfalls erhalten Sie unten im Fenster einen entsprechenden Hinweis, da die Sicherung auf einem Bandlaufwerk oder einem anderen Wechselmedium empfohlen ist.

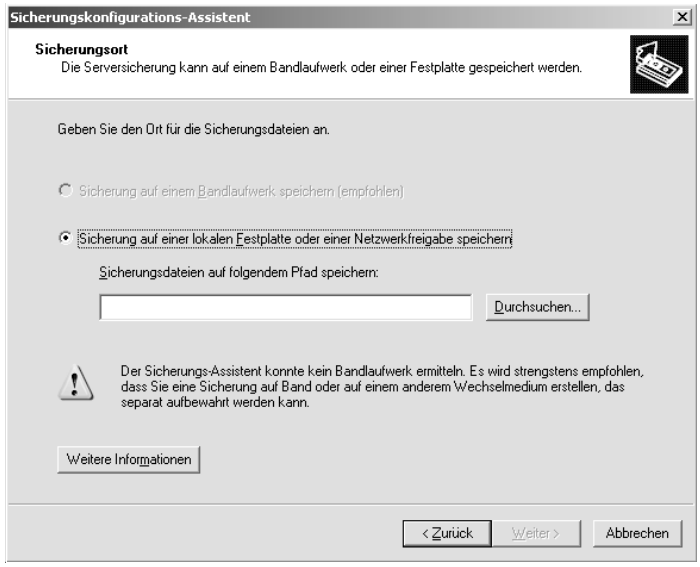


Abbildung 2.67: Die Auswahl des Sicherungsortes

Möchten Sie die Sicherung auf einer Festplatte durchführen, wählen Sie über DURCHSUCHEN den Pfad aus, in dem Sie die Daten sichern möchten. Klicken Sie dann auf WEITER.

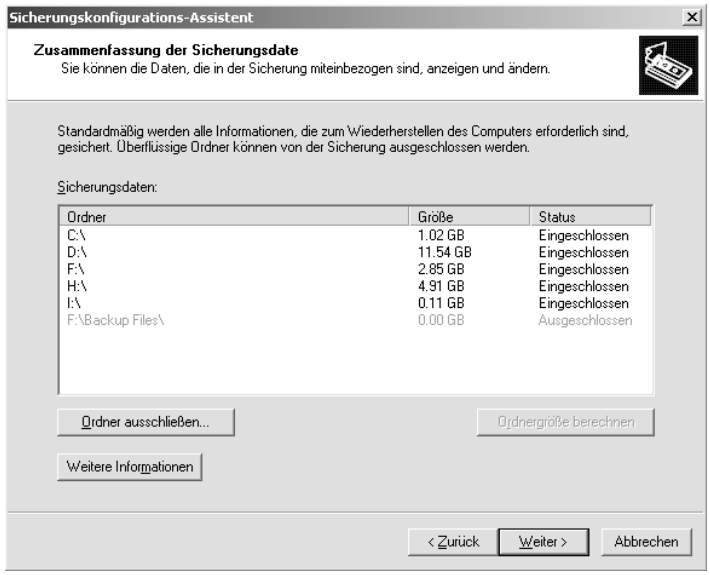


Abbildung 2.68: Die Auswahl der zu sichernden Serverdaten

2. Im Fenster ZUSAMMENFASSUNG DER SICHERUNGSDATEN (siehe Abbildung 2.68) sehen Sie, welche Daten des Servers in der Sicherung enthalten sein sollen. Standardmäßig sind sämtliche Daten aller Partitionen in die Sicherung eingeschlossen. Bei der Sicherung auf einer Festplatte wird lediglich das Verzeichnis, das Sie unter Schritt 1 als Ort für die Sicherung ausgewählt haben, ausgeschlossen.

Möchten Sie weitere Ordner von der Sicherung ausschließen, so klicken Sie auf ORDNER AUSSCHLIESSEN. Im gleichnamigen sich öffnenden Fenster ist lediglich der Ordner enthalten, der die Sicherung enthält. Möchten Sie weitere Ordner ausschließen, klicken Sie auf ORDNER HINZUFÜGEN und wählen die gewünschten Ordner aus. Bereits hinzugefügte Ordner können auch wieder entfernt werden. Klicken Sie dann auf OK.

Befindet sich im Fenster ZUSAMMENFASSUNG der Sicherungsdaten ein Ordner, dessen Größe nicht in der Spalte GRÖSSE angegeben ist, so können Sie diese über ORDNERGRÖSSE BERECHNEN ermitteln lassen. Je nach Größe des Ordners kann dieser Vorgang einige Minuten in Anspruch nehmen.

3. Danach erscheint das Fenster SICHERUNGSZEITPLAN DEFINIEREN (siehe Abbildung 2.69). Wählen Sie hier die Tage aus, an denen eine Sicherung durchgeführt werden soll. Standardmäßig sind lediglich die Werktage von Montag bis Freitag ausgewählt.

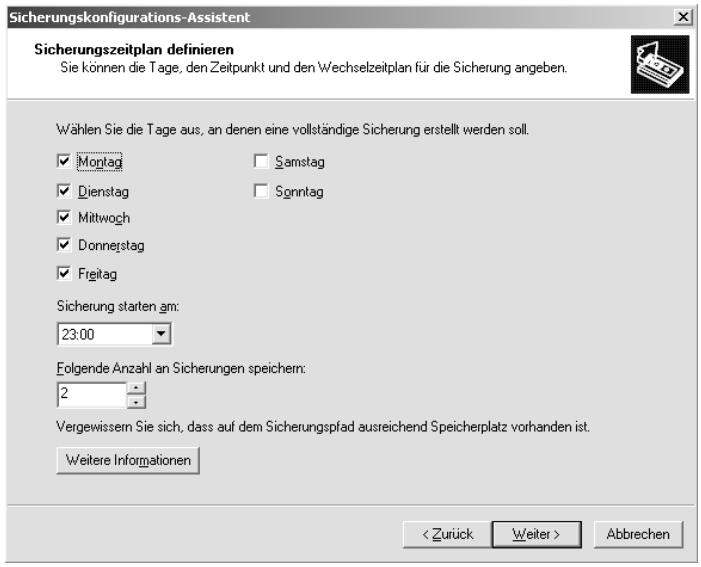


Abbildung 2.69: Erstellen des Sicherungszeitplans

Unter SICHERUNG STARTEN AM legen Sie die Uhrzeit fest. In der Regel wird diese in den Abend- oder Nachtstunden erfolgen.

Idealerweise sollte die Sicherung vor 02:00h gestartet sein, damit Sie sicher sein können, dass die Sicherung beendet ist, bevor der Serverstatusbericht gesendet wird. So können Sie schnell erkennen, ob bei der Sicherung Probleme aufgetreten sind.

Unter FOLGENDE ANZAHL AN SICHERUNGEN SPEICHERN legen Sie die Anzahl der aufzubewahrenden Sicherungen fest. Bei der Sicherung auf einem Wechseldatenträger ist in der Regel nur eine Sicherung erforderlich, bei der Sicherung auf einer Festplatte sollten zwei Sicherungen gespeichert werden.

Klicken Sie dann auf WEITER.

4. Als Nächstes erhalten Sie das Fenster SPEICHERPLATZZUWEISUNG FÜR GELÖSCHTE DATEIEN UND E-MAIL (siehe Abbildung 2.70).

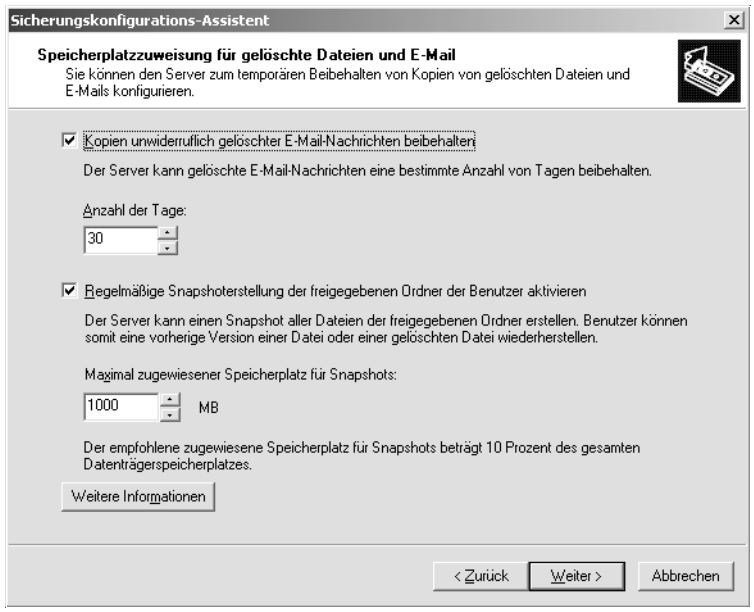


Abbildung 2.70: Die Zuweisung von Speicherplatzgrenzwerten für gelöschte Dateien und E-Mails

Hier legen Sie unter ANZAHL DER TAGE fest, wie lange auf dem Server die von den Benutzern gelöschten E-Mails aufbewahrt werden sollen. Die Standardeinstellung liegt bei 30 Tagen. So lange haben die Benutzer die Möglichkeit, die E-Mails unter Outlook 2003 wiederherzustellen. Diese Funktion ist nur in Verbindung mit Exchange verfügbar. Haben Sie die Checkbox KOPIEN UNWIDERRUFLICH GELÖSCHTER E-MAIL-NACHRICHTEN BEIBEHALTEN deaktiviert, werden die gelöschten E-Mails nicht auf dem Server vorgehalten.

Über die Checkbox REGELMÄSSIGE SNAPSHOT-ERSTELLUNG DER FREIGEGEBENEN ORDNER DER BENUTZER AKTIVIEREN schalten Sie die neue Funktionalität der Schattenkopien ein und aus. Der Server ist dadurch in der Lage, für sämtliche Dateien in den freigegebenen Benutzerordnern einen Snapshot zu erstellen, so dass der Benutzer eine gelöschte Datei wiederherstellen oder von einer vorhandenen Datei einen früheren Versionsstand wiederherstellen kann.

Die automatische Erstellung der Snapshots erfolgt täglich um 07:00h und um 12:00h. Beim Zurückgreifen auf einen früheren Versionsstand wird immer die Datei verwendet, die während des letzten Snapshots erstellt worden ist. Die Standardeinstellung für den für die Snapshots zugewiesenen Speicherplatz beträgt 1.000 MB. Sie sollten jedoch einen

Wert festlegen, der zehn Prozent des Datenträgers beträgt. Damit das Feature der Schattenkopie verfügbar ist, müssen mindestens 310 MB freier Festplattenspeicher vorhanden sein. Klicken Sie dann auf WEITER.

Das Feature der Schattenkopie ist nicht verfügbar, wenn ein freigegebener Ordner umbenannt oder gelöscht wurde. Sollte der gesamte Ordner Users Shared Folders gelöscht worden sein, müssen Sie das Setup des SBS erneut ausführen und die Komponente neu installieren.

5. Sie können nun den Assistenten fertig stellen oder über ZURÜCK noch Änderungen an der Konfiguration vornehmen. Klicken Sie dann auf FERTIG STELLEN.

2.8 Installierte Hotfixes

Bei der Installation des SBS 2003 wird eine Reihe von Patches und Hotfixes automatisch mitinstalliert. Im Einzelnen handelt es sich dabei um die folgenden Hotfixes:

- QFE#47846 – KB822745
- QFE#47937 – KB822744
- QFE#47987 – KB822743
- QFE#47990 – KB822742
- QFE#48802 – KB824073
- QFE#47607 – KB822132
- QFE#50566 – KB824146
- QFE#49367 – KB824139
- QFE#48628 – KB823559
- QFE#48713 – KB823980
- QFE#46104 – KB819696
- QFE#50449 – KB826238
- QFE#50009 – KB826936
- QFE#50147 – KB825117
- QFE#48165 – KB822925
- QFE#48087 – KB824105

Weitere Informationen zu den Inhalten dieser Hotfixes finden Sie in der Microsoft Knowledge Base. Die Bezeichnung QFE#xxxxx gibt jeweils die Bezeichnung des Patches an, KBxxxxxx steht für den entsprechenden Artikel in der Microsoft Knowledge Base, unter dem Sie spezifische Informationen finden.

3 Update und Migration

Dieses Kapitel beschäftigt sich mit der Migration älterer Produktversionen des SBS auf die aktuelle Version 2003. Generell ist eine Migration von den Versionen SBS 4.5 sowie SBS 2000 sowie auch vom Windows Server 2000, 2003 sowie NT 4.0 auf die Version SBS 2003 möglich. Ein Update auf den SBS 2003 ist vom SBS 2000 sowie vom Windows Server 2000 und 2003 möglich. In diesem Kapitel finden Sie zunächst einige Hinweise, um zu entscheiden, ob ein Update oder eine Migration sinnvoller ist.

Danach erhalten Sie zunächst eine detaillierte Anleitung für die Migration eines SBS 2000/Windows Server 2000 und eines SBS 4.5/Windows Server NT 4.0 sowie seines Clients auf SBS 2003 und danach Hinweise für ein Update eines SBS 2000/Windows Server 2000 auf SBS 2003. Ein Update älterer Systeme ist nicht möglich.

3.1 Vorüberlegungen

Bevor Sie mit dem Wechsel auf SBS 2003 beginnen, müssen Sie entscheiden, ob Sie ein Update oder eine Migration durchführen möchten. Sofern Sie SBS 4.5 oder Windows NT 4.0 Server einsetzen, ist lediglich eine Migration, aber kein Update möglich.

Bei einer Migration wird der SBS 2003 auf einem neuen Rechner installiert, und anschließend werden sämtliche Daten und Einstellungen des alten Systems auf das neue migriert. Bei einem Update wird die neue Version über die alte installiert. Dabei bleiben – sofern denn alles gut läuft – sämtliche Daten und Einstellungen erhalten. Eine Update-Installation verläuft nicht viel anders als eine herkömmliche Neuinstallation und erfordert weniger Planung und Aufwand.

3.1.1 Update-Möglichkeiten vorhandener Betriebssysteme

Die folgende Tabelle zeigt Ihnen eine Übersicht über die Update-Möglichkeiten vorhandener Betriebssysteme auf SBS 2003. Bei den Betriebssystemen, die kein Update unterstützen, können Sie lediglich eine Migration durchführen.

Betriebssystem	Update möglich auf
Windows NT Server 3.51	Kein Update möglich
Windows NT Server 3.51 Enterprise	Kein Update möglich
Windows NT Server 3.51 mit Citrix	Kein Update möglich
Windows NT Server 4.0	Windows Server 2003 Standard und Enterprise

Betriebssystem	Update möglich auf
Windows NT Server 4.0 Enterprise	Windows Server 2003 Enterprise
Windows NT Server 4.0 Terminal Server Edition	Windows Server 2003 Enterprise
BackOffice SBS 4.0/4.5	Kein Update möglich
Windows 2000 Server	Windows Server 2003 Standard und Enterprise, SBS 2003 Standard und Enterprise
Windows 2000 Advanced Server	Windows Server 2003 Enterprise
Windows 2000 Datacenter Server	Windows Server 2003 Datacenter
SBS 2000	SBS 2003 Standard und Premium
SBS 2003 Standard	SBS 2003 Premium
Windows Server 2003 Standard	Windows Server 2003 Enterprise, SBS 2003 Standard und Premium

Tabelle 3.1: Update-Möglichkeiten vorhandener Betriebssysteme auf SBS 2003

3.1.2 Schlagwörter

Im Laufe dieses Kapitels werden Sie immer wieder mit einer Reihe von Schlagwörtern konfrontiert. Diese werden zur Verdeutlichung einmal kurz erläutert.

Migration

Bei einer Migration wird der SBS 2003 auf einem neuen Rechner installiert. Danach werden Daten und Einstellungen des ursprünglichen Systems auf den neuen SBS migriert. Man spricht auch von einer Migration, wenn die Daten und Einstellungen von einem bestehenden SBS 2003 auf einen anderen SBS 2003 transferiert werden.

Verwechseln Sie nicht die Begriffe Migration und Update miteinander!

Quellserver

Der Quellserver ist derjenige Server, von dem aus die bestehenden Daten und Einstellungen auf das neue System gebracht werden sollen. Dabei kann es sich um einen SBS 2000 oder SBS 4.5 handeln. Auch ein Windows Server 2000 oder Windows Server NT 4.0 kann der Quellserver sein. Sie müssen sicherstellen, dass der Quellserver während des Migrationsprozesses online ist.

Zielserver

Der Zielserver ist derjenige, auf den die Daten und Einstellungen des Quellservers gebracht werden sollen. In unserem Zusammenhang ist der Zielserver ein SBS 2003.

Active Directory Migration Tool (ADMT)

Das Active Directory Migration Tool (ADMT) ist ein Programm, das Sie beim Verschieben von Benutzern, Gruppen und Computern zwischen Active Directory-Domänen oder auch von einer Windows 2000-Domäne zu einer Active Directory-Domäne unterstützt. Dieses Programm sollte auch bei der Migration des SBS eingesetzt werden.

3.1.3 Die Arbeitsschritte des Migrationsprozesses

Die Migration des SBS ist ein gut zu planender Vorgang, der sich nicht auf die Schnelle und unkonzipiert in einer produktiven Umgebung umsetzen lässt. Idealerweise verfügen Sie über eine Testumgebung, in der Sie über einen identischen Quell- und Zielserver verfügen. Die Vorbereitung der Migration lässt sich in insgesamt sieben Schritte zusammenfassen. Detaillierte Anweisungen für die einzelnen Schritte finden Sie in den Kapiteln Abbildung 3.2 (für SBS 2000 und Windows Server 2000) sowie Abbildung 3.3 (für SBS 4.5 und Windows Server NT 4.0).

1. Vorbereiten der Migration

   In diesem Schritt werden zunächst sämtliche Informationen gesammelt, die für das weitere Vorgehen erforderlich sind. Dazu zählen Informationen bezüglich des Namens, des Domänennamens, der IP-Adresse und sämtlicher Freigaben. Auf dem alten Exchange-Server exportieren Sie das Mailkonto des Administrators inklusive aller erstellten Regeln und speichern die öffentlichen Ordner in einer pst-Datei. Zudem sollten Sie sämtliche Benutzer auffordern, nicht mehr benötigte Mails und Ordner zu löschen. Führen Sie dann ein Backup des Quellservers durch und prüfen, ob auf diesem die aktuellen Service Packs und Patches installiert sind. Während der Migration darf kein Benutzer im Netzwerk mehr mit der Domäne verbunden sein.

2. Vorbereiten des Zielservers für die Installation

   Um den Zielserver für die Installation des SBS 2003 vorzubereiten, müssen Sie zunächst auf dem Quellserver den DHCP-Serverdienst beenden. Danach werden der Quell- und Zielserver miteinander verbunden und die Installation des SBS 2003 auf dem Zielserver durchgeführt. Nachdem Sie im Zuge der Installation die zu erledigenden Netzwerkschritte abgeschlossen haben (siehe Kapitel 2.7), trennen Sie die Netzwerkkarte für den Internetzugang vom Kabel und installieren auf dem Quell- und Zielserver eine geeignete Antiviren-Software. Damit ist sichergestellt, dass dieser Vorgang nicht den Datentransfer zwischen den beiden Servern bei der Migration stört.

3. Vorbereiten der Clients für die Migration

   Als Nächstes werden die Clients für den Einsatz des SBS 2003 vorbereitet. Die Vorbereitung bezieht sich auf alle Clients mit den Betriebssystemen Windows NT 4.0, 2000 Professional, XP Professional sowie Windows Server 2003. Dasselbe gilt für Mitgliedserver der Betriebssysteme Windows Server NT 4.0, 2000 und 2003. Die Migration selbst der Computerkonten erfolgt mit Hilfe des ADMT (siehe Schritt 4), das nur die eben genannten Betriebssysteme unterstützt. Verwenden Sie die Betriebssysteme Windows 95, 98 oder ME, müssen die Computerkonten entweder manuell konfiguriert werden (siehe Schritt 6), oder aber Sie aktualisieren zuvor das Client-Betriebssystem.

4. Durchführung der Migration

   Die Durchführung der Migration erfolgt mit Hilfe des ADMT. ADMT wird auf dem Zielserver installiert und migriert bestehende Computer-, Benutzer- sowie Gruppenkonten. Sind auf dem Quell- und Zielserver DNS-Forwarder installiert, kann ADMT mit beiden Servern arbeiten. Wird auf dem Quellserver Exchange 2000 ausgeführt, können Sie eventuell bestehende Mail-Quotas auf dem neuen Server geändert werden sollen. Danach werden die Exchange-Postfächer migriert. Zusätzlich müssen sämtliche freigegebenen Ordner, Applikationsdaten sowie SQL-Datenbanken auf den Zielserver migriert werden.

5. Konfiguration des Zielservers

   Nachdem Sie die bestehenden Daten auf den Zielserver migriert haben, muss dieser noch konfiguriert werden. Dazu verbinden Sie Benutzerkonten mit den Kontenvorlagen des SBS 2003 und verteilen Applikationen an die Clientcomputer. Weiterhin muss auf dem Zielserver die Aufgabenliste (siehe Kapitel 2.7) abgearbeitet werden. Mögliche benutzerdefinierte Einstellungen des Quellservers müssen übernommen werden. Zudem müssen Sie die Mail-Verteilerlisten, Empfangsrichtlinien sowie den Microsoft Connector für POP3-Mailboxen konfigurieren.

6. Konfiguration der Clients

   Für Windows 2000- und XP-Clients müssen dann die E-Mail- und Proxy-Einstellungen konfiguriert werden. Bei allen älteren Betriebssystemen als Windows 2000 Professional müssen Sie diese Einstellungen für den Zielserver sowie die Installation der Software manuell vornehmen. Auch die öffentlichen Exchange-Ordner können nun importiert werden, so dass der Client den neuen Exchange-Server verwenden kann. In jedem Fall sollten Sie prüfen, ob die Clients Verbindungen zu allen notwendigen Daten und Ressourcen herstellen können.

7. Abschluss der Migration

   Um die Migration abzuschließen, deinstallieren Sie ADMT wieder vom Zielserver. Legen Sie dann eine Kennwortrichtlinie fest, die alle Benutzer bei der ersten Anmeldung auffordert, ein neues Passwort festzulegen. Nachdem Sie sich überzeugt haben, dass sämtliche Daten und Einstellungen vollständig vom Quellserver migriert worden sind, können Sie diesen endgültig außer Betrieb setzen. Denken Sie auch daran, sämtliche Berechtigungen zu entfernen, die im Zuge der Migration gesetzt wurden, für den laufenden Betrieb jedoch ein Sicherheitsrisiko darstellen könnten.

3.1.4 Die Zeitplanung der Migration

Der Migrationsvorgang ist ein relativ aufwändiger Vorgang, der einige Tage in Anspruch nehmen wird. Idealerweise führen Sie zunächst eine Migration in einer Testumgebung durch. Hierzu ist es jedoch erforderlich, separate Hardware bereitzustellen und auf dieser den Quell- und Zielserver sowie verschiedene Typen von Clients zu installieren. Die Errichtung einer Testumgebung mag jedoch in vielen kleinen und mittleren Unternehmen aus Kosten- und Zeitgründen nicht durchführbar sein. Umso wichtiger ist in diesem Fall eine sorgfältige Planung der einzelnen Schritte.

Sie sollten einen kompletten Tag dafür verwenden, den oben genannten ersten Schritt durchzuführen, indem Sie Informationen sammeln, die Benutzer zum Löschen nicht mehr benötigter Daten auffordern und den Quellserver mit aktuellen Patches versehen. Parallel dazu kann bereits auf dem neuen Rechner die Installation des SBS 2003 erfolgen.

Am nächsten Tag sollten Sie darangehen, vom Exchange-Server die oben genannten Daten zu exportieren. Anschließend führen Sie ein vollständiges Backup des Quellservers durch. Idealerweise geschieht dies nach der regulären Arbeitszeit, so dass Sie sicher sein können, den aktuellsten Stand der Daten zu sichern. Da die Migration an sich am besten an einem Wochenende vorgenommen werden sollte, kann das Backup auch zu diesem Zeitpunkt durchgeführt werden.

Für die folgenden Aufgaben können Sie je nach Größe des Unternehmens ein oder zwei Tage kalkulieren. In dieser Zeit verbinden Sie die beiden Server miteinander und führen auf dem Quellserver alle notwendigen Schritte aus. Mit Hilfe des ADMT werden die Konten migriert und möglicherweise Clientcomputer manuell konfiguriert.

Nachdem die Umstellung auf das neue System erfolgt ist, sollte der verantwortliche Administrator auf jeden Fall greifbar sein, damit er mögliche Probleme im laufenden Betrieb beheben kann und für Fragen der Benutzer bereitsteht.

3.1.5 Fallstricke während der Migration

Damit die Migration ohne Probleme durchgeführt werden kann, sollten Sie auf eine Reihe von Dingen achten, die hier nochmals separat vorgestellt werden, da sie im Falle einer Misskonfiguration schnell zu Fallstricken im Zuge der Migration werden können.

Beachten Sie ferner, dass Sie die einzelnen Migrationsschritte unbedingt in der oben angegebenen Reihenfolge ausführen.

Namen der beiden Server

Der Quell- und Zielserver müssen über unterschiedliche Namen verfügen. Dies gilt sowohl für die DNS-Namen der internen Domäne als auch für den NetBIOS-Domänennamen. Bedenken Sie, dass deshalb auf allen Clients die Verknüpfungen mit dem alten Namen gelöscht und durch den des neuen SBS-Servers ersetzt werden müssen.

Deaktivieren des DHCP-Serverdienstes

Damit der DHCP-Serverdienst korrekt auf dem Zielserver installiert werden kann, muss der Dienst auf dem Quellserver deaktiviert werden, bevor dieser mit dem Zielserver verbunden wird. Wenn der DHCP-Dienst auf einem Router im Netzwerk ausgeführt wird, müssen Sie sicherstellen, dass dieser während der Installation mit dem SBS 2003 verbunden ist.

Rund um ADMT und Exchange Migration Wizard

Sie verwenden das Programm ADMT für die Migration von Computer-, Benutzer- und Gruppenkonten. Dabei werden die Security Identifier (SIDs) beibehalten. Eine ausführliche Hilfe zu ADMT finden Sie im Installationsverzeichnis in der Datei *DomainMig.chm*. Der Exchange Migration Wizard hingegen ist für die Migration der Benutzer-Postfächer zuständig. Er ist jedoch nicht in der Lage, die Mailbox des Administratorkontos, die Regeln für die öffentlichen Ordner sowie Regeln für die Postfächer zu exportieren. Diese drei Schritte müssen Sie manuell vornehmen, indem Sie diese vom Quellserver exportieren und auf dem Zielserver importieren. Weitere Hinweise dazu finden Sie im Microsoft KB-Artikel 328871.

Übernehmen benutzerdefinierter Einstellungen

Am Ende der Migration müssen Sie sämtliche benutzerdefinierten Einstellungen des Quellservers manuell auf dem Zielserver durchführen. Dazu zählen etwa die folgenden Konfigurationen: DHCP-Bereichsoptionen, DNS Records, Einstellungen für Routing- und RAS-Dienste, Gruppenrichtlinieneinstellungen, SMTP Connector des Exchange-Servers und Einstellungen des ISA-Server 2000. Haben Sie zusätzlich noch Webseiten über den IIS laufen, so müssen Sie die Dateien auf den Zielserver kopieren und die Webseiten neu erstellen. Alternativ können Sie das *IIS 6.0-Migrationstool* benutzen. Dieses finden Sie auch auf der Begleit-CD.

Desktop-Profile

Während der Migration werden zwar die Desktop-Profile unter Windows 2000 und Windows XP beibehalten, aber sämtliche darin enthaltenen Verweise auf den Quellserver sind nach der Migration ungültig und müssen geändert werden.

Verfrühtes Anlegen neuer Computer- und Benutzerkonten

Das Anlegen neuer Computer-, Benutzer- und Gruppenkonten ist erst möglich, nachdem Sie im Zuge der Migration in Schritt 5, Konfiguration des Zielservers, die Verwaltungsaufgaben abgeschlossen haben. Versuchen Sie bereits vordem, neue Konten anzulegen, schlägt dieser Vorgang fehl.

DNS-Forwarder

Sowohl auf dem Quellserver als auch auf dem Zielserver müssen Sie DNS-Forwarder einrichten. Die DNS-Forwarder sind erforderlich, weil ADMT mit beiden Servern arbeiten muss.

3.2 Migration des Small Business Server 2000 und Windows Server 2000

Dieses Kapitel beschreibt detailliert die verschiedenen Arbeitsschritte der Migration mit einem SBS 2000 oder Windows Server 2000 als Quellserver.

3.2.1 Schritt 1 – Vorbereiten der Migration

Im Zuge der Migrationsvorbereitung sammeln Sie zunächst die folgenden Informationen verschiedener Bereiche:

Serverbezogene Informationen

- Name des Quell- und Zielservers. Diese beiden Namen müssen unterschiedlich sein. Sie finden den Computernamen unter den Eigenschaften des Arbeitsplatzes auf der Registerkarte COMPUTERNAME.
- Vollständiger DNS-Name der internen Domäne und NetBIOS-Domänenname: Auch diese beiden Namen müssen sich auf dem Quell- und Zielserver unterscheiden. Standardmäßig können Sie die während der Installation vorgeschlagenen Werte für die interne DNS-Domäne übernehmen. Um den NetBIOS-Domänennamen des Quellservers zu ermitteln, geben Sie unter AUSFÜHREN `dsa.msc` ein. In der mmc *Active Directory-Benutzer und -Computer* wählen Sie das Kontextmenü EIGENSCHAFTEN der Domäne. Der NetBIOS-Domänenname ist der erste Teil des kompletten Domänennamens. Bei einem Domänennamen *firma.de* lautet der NetBIOS-Name *FIRMA*.
- Ermitteln Sie die IP-Adresse des Quellservers, und bestimmen Sie eine noch nicht vergebene Adresse für den Zielserver. Um die Adresse des Quellservers zu bestimmen, geben Sie unter AUSFÜHREN `cmd` ein und dann den Befehl `ipconfig /all`. Die IP-Adresse für den Zielserver muss sich selbstverständlich in demselben Adressbereich befinden wie die des Quellservers. Verwenden Sie einen Router als DHCP-Server, muss die Adresse im Bereich der vom Router vergebenen Adressen liegen. Fungiert der Quellserver als DHCP-Server, so ermitteln Sie in dessen Bereichsoptionen gültige IP-Adressen. In der DHCP-Konsole doppelklicken Sie den Quellserver und danach den Eintrag BEREICH. Klicken Sie dann auf ADDRESS LEASES. Hier finden Sie alle aktuell verwendeten IP-Adressen.
- Administratorkonto: Haben Sie auf dem Quellserver das Administratorkonto umbenannt, so müssen Sie dieses wieder auf den ursprünglichen Namen Administrator zurücksetzen. Eine Umbenennung des Kontos kann nach Abschluss der Migration auf dem Zielserver wieder erfolgen. Außerdem müssen Sie sicherstellen, dass das Administratorpasswort auf dem Quell- und Zielsystem identisch ist. Es muss dabei ein Passwort gesetzt sein, anderenfalls kann die Migration nicht durchgeführt werden.

Informationen über gemeinsam genutzte Ordner, Applikationen und Einstellungen

- Gemeinsam genutzte Ordner der Benutzer (Users Shared Folder): Notieren Sie sich den Namen des Benutzerordners. Standardmäßig lautet er unter SBS 2000 und SBS 2003 USERS.
- Ordner für Client-Applikationen (ClientApps Folder): Befinden sich hier Applikationen, die auch nach der Migration verwendet werden sollen, so kopieren Sie den Inhalt in das Verzeichnis auf dem Zielserver. Standardmäßig heißt das Verzeichnis für Client-Applikationen unter SBS 2000 CLIENTAPPS5, unter SBS 2003 CLIENTAPPS.

Die Applikation *Modem Sharing Client* ist nach der Migration jedoch nicht mehr verfügbar, da SBS 2003 diese Funktion nicht mehr unterstützt.

- Gemeinsam genutzte Ordner der Firma (Company Shared Folder): Unter SBS 2000 lautet der Name des Ordners COMPANY. Unter SBS 2003 hingegen wird eine eigene Firmenwebsite über die SharePoint Services bereitgestellt. Der Speicherort ist hier *http://companyweb*.
- Weitere gemeinsam genutzte Ordner: Die Inhalte folgender gemeinsam genutzter Ordner können nicht migriert werden: DRUCKER, GEPLANTE TASKS und SYSVOL. Migrieren Sie auch nicht den Ordner NETLOGON, sofern Sie keine angepassten Login-Skripte verwenden. Diese Ordner dürfen weder bei einer Migration von SBS 2000 noch von Windows Server 2000 migriert werden. Bei einer Migration von SBS 2000 aus dürfen zusätzlich folgende Ordner nicht migriert werden, da der SBS 2003 aktualisierte Versionen beinhaltet: MSPCINT, MPCLIENTS sowie FAX CLIENTS.
- Auch der Ordner TSCLIENT kann nicht migriert werden, da unter SBS 2003 die Terminaldienste im Applikationsmodus nicht verfügbar sind. Wollen Sie diese Funktionalität dennoch verwenden, müssen Sie einen separaten Server einrichten.
- Sind noch weitere gemeinsam genutzte Ordner vorhanden, so prüfen Sie deren Inhalte und notieren sich die Namen der Freigaben, um diese auf dem Zielsystem neu einzurichten. Um einen Überblick über alle Freigaben des Quellservers zu erhalten, geben Sie unter AUSFÜHREN Folgendes ein: \\Quellserver-Name.
- Als Nächstes notieren Sie sich den Namen und Installationspfad sämtlicher Applikationen, die Sie auch nach der Migration wieder benutzen möchten.
- Haben Sie unter Exchange 2000 Verteilergruppen eingerichtet, so notieren Sie sich deren Namen. Beim Verschieben der Gruppen auf den Zielserver müssen Sie diese in die Organisationseinheit (OU) Verteilergruppen verschieben. Befinden sich in den Verteilergruppen vordefinierte Gruppen (wie z.B. Administratoren) als Mitglieder, so müssen Sie diese Gruppenmitgliedschaft ebenfalls vermerken, da die Mitgliedschaften der vordefinierten Gruppen nicht migriert werden können. Des Weiteren müssen Sie unter Exchange 2000 benutzerdefinierte Berechtigungen für die öffentlichen Ordner sowie benutzerdefinierte Empfänger aufschreiben und nach Abschluss der Migration neu konfigurieren.
- Prüfen Sie dann, ob Sie sämtliche benutzerdefinierten Einstellungen der folgenden Bereiche gesichert haben: DNS-Einträge, DHCP-Bereichsoptionen, Routing und RAS, Gruppenrichtlinien, Webseiten auf dem IIS, Exchange und ISA-Server 2000. Diese Einstellungen werden auf dem Zielserver nach Abschluss der Migration neu konfiguriert. Die öffentlichen Ordner sowie das Postfach des Administratorkontos werden in eine .pst-Datei exportiert. Sind für das Administrator-Postfach bestimmte Regeln festgelegt, so müssen Sie diese ebenfalls exportieren. Eine Migration dieser Einstellungen mit dem Exchange Server-Migrationsassistenten ist nicht möglich.

Haben Sie keine benutzerdefinierten Einstellungen auf dem Quellsystem zugelassen, sondern die Standardeinstellungen beibehalten, so müssen Sie für diese Bereiche die Konfiguration nicht notieren, da die Standardeinstellungen des SBS 2003 übernommen werden können.

Löschen nicht mehr benötigter Dateien und E-Mails

In jedem Fall sollten Sie vor Beginn der Migration sämtliche nicht mehr benötigte Dateien und E-Mails löschen. Fordern Sie hierzu alle Benutzer auf, unter Outlook ihre Mails aus den Ordnern GELÖSCHTE OBJEKTE sowie GESENDETE OBJEKTE zu löschen. Dasselbe gilt auch für nicht mehr benötigte Dateien in den einzelnen Benutzerverzeichnissen. Weiterhin sollten Sie auch sämtliche gemeinsam genutzte Verzeichnisse auf Dateileichen hin durchsuchen.

Ist ein Postfach eines Benutzers auch nach dem Löschen sämtlicher überflüssiger E-Mails noch größer als 200 MB, müssen Sie auf dem Zielserver unbedingt die Quota-Einstellungen ändern. Standardmäßig liegt der Schwellenwert für die Postfachgröße bei 200 MB. Ist diese Größe überschritten, können keine E-Mails mehr gesendet und empfangen werden. Eine Warnung wird standardmäßig bei 175 MB Postfachgröße ausgegeben.

Ein Limit gilt auch für die Benutzerordner. Der Grenzwert für Benutzerordner liegt unter SBS 2003 standardmäßig bei 1 GB. Ist der Ordner eines Benutzers größer als 1 GB, so müssen Sie die Quota-Einstellungen für alle Benutzer anpassen. Weitere Hinweise dazu finden Sie in der Hilfe des SBS 2003.

Um die Postfachgröße der einzelnen Benutzer zu ermitteln, führen Sie unter SBS 2000 die folgenden Schritte aus:

1. Öffnen Sie die Administrationskonsole. Doppelklicken Sie dort EXCHANGE ORGANISATION und danach SERVER.
2. Doppelklicken Sie hier ERSTE SPEICHERGRUPPE und dann POSTFACHSPEICHER.
3. Klicken Sie dann auf POSTFÄCHER. In der Spalte K im rechten Fensterabschnitt finden Sie die Postfachgröße für jeden Benutzer.

Werden unter Outlook von den Benutzern Regeln verwendet, so müssen Sie diese sichern, da bei der Migration der Postfächer keine Outlook Regeln auf den Zielserver migriert werden.

Kompatibilität von Hard- und Software

Haben Sie die Absicht, Hardware, z.B. ein eingebautes Faxmodem, oder Software des Quellsystems auch auf dem Zielserver zu verwenden, so müssen Sie sicherstellen, dass eine Kompatibilität mit SBS 2003 gegeben ist. Benutzen Sie hierzu die Windows Server-Katalogseite unter *http://www.microsoft.com/windows/catalog/server/.*

Einspielen aktueller Service Packs

Zusätzlich sollten Sie sicherstellen, dass auf dem Quellsystem das aktuelle Service Pack installiert ist. Für die reibungslose Migration müssen mindestens folgende Service Packs installiert sein:

SBS 2000: Service Pack 1 Um zu überprüfen, welches Service Pack installiert ist, öffnen Sie die Administratorkonsole. Dort klicken Sie auf SERVERSTATUS. In der rechten Fensterhälfte klicken Sie auf ÜBER. Dort finden Sie die aktuelle Version. Weitere Hinweise zum Bezug und zur Installation des Service Packs 1 für SBS 2000 finden Sie im Microsoft KB-Artikel 326924.

Exchange Server 2000: Service Pack Um zu überprüfen, welches Service Pack installiert ist, öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT EXCHANGE/SYSTEM MANAGER. Doppelklicken Sie auf SERVER und klicken dann Ihren Exchange-Server an. Im Menü AKTION wählen Sie den Eintrag EIGENSCHAFTEN. Hier wird die Service Pack-Version angezeigt. Das Service Pack können Sie unter *http://www.microsoft.com/Exchange/Downloads/2000/Sp3/default.asp* downloaden.

SQL Server 2000: Service Pack 3 Um zu überprüfen, welches Service Pack installiert ist, öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT SQL SERVER/ENTERPRISE MANAGER. Doppelklicken Sie die SQL SERVERGRUPPE und wählen aus dem Kontextmenü des Servernamens den Eintrag EIGENSCHAFTEN. Die Versionsnummer muss 8.00.760 lauten. Diese Versionsnummer entspricht einem installierten Service Pack 3. Das Service Pack können Sie unter *http://www.microsoft.com/sql/downloads/2000/sp3.asp* downloaden.

Windows Server 2000: Service Pack 4 Um zu überprüfen, welches Service Pack installiert ist, geben Sie unter AUSFÜHREN den Befehl `Winver` ein. Um das Service Pack 4 zu installieren, legen Sie die CD 3 des SBS 2003 ein, wechseln in das Verzeichnis \SBS\CLIENTAPPS\WIN2K_SP4\I386\ und führen die Datei *Update.exe* aus.

Sicherung des Quellservers

Eine Sicherung des Quellservers sollte durchgeführt werden, nachdem sämtliche Benutzer ihre Arbeit beendet haben. Idealerweise geschieht dies also abends oder an einem Wochenende. Vor Beginn des Backups sollten Sie sämtliche Laufwerke auf Viren hin scannen.

Beachten Sie unbedingt, dass Sie während des Virenscans nicht das Exchange-Laufwerk M: mitscannen. Dies kann zu Schäden an der Exchange-Datenbank führen. Standardmäßig wird unter Exchange 2000 das IFS (Installable File System) auf das Laufwerk M: gemapt.

Führen Sie dann ein vollständiges Backup mit den Systemdaten sowie Exchange durch.

Beachten Sie unbedingt, dass Sie im Zuge des Exchange-Backup nicht das Exchange-Laufwerk M: sichern. Dies kann zu Schäden an der Exchange-Datenbank führen. Standardmäßig wird unter Exchange 2000 das IFS (Installable File System) auf das Laufwerk M: gemapt.

Um sicherzustellen, dass das Backup ordnungsgemäß durchgeführt wurde, sollten Sie beliebige Dateien des Backups an einem anderen Speicherort wiederherstellen und prüfen, ob die Originaldatei und die der Sicherung identisch sind.

Benachrichtigung über die anstehende Migration

Eine Benachrichtigung der Benutzer über die anstehende Migration ist nur in dem Moment relevant, wenn noch Benutzer an der Domäne angemeldet sind. Führen Sie die Migration hingegen zu einem Zeitpunkt aus, zu dem keine Benutzer mehr arbeiten, so ist dieser Punkt unerheblich. Anderenfalls können Sie die Benutzer über den *Net send*-Befehl erreichen. Voraussetzung dafür ist, dass auf dem Server und den Clients der Nachrichtendienst ausgeführt wird. Verwenden Sie beispielsweise folgenden Befehl an der Eingabeaufforderung:

```
Net send * Bitte melden Sie sich innerhalb der nächsten 5 Minuten von der
Domäne ab. Es sind dann keine Netzwerk- und Internetverbindungen mehr
verfügbar. ↵
```

Dabei bedeutet das Symbol *, dass die Nachricht an alle Mitglieder der Domäne geschickt wird.

3.2.2 Schritt 2 – Vorbereiten des Servers für die Installation

Dieses Kapitel beschreibt sämtliche Schritte, die Sie vor der Installation des SBS 2003 auf dem Quell- und Zielsystem durchführen müssen. Die Installation des SBS 2003 selbst wurde bereits ausführlich in Kapitel 2.4 beschrieben.

DHCP-Konfiguration

Vor Beginn der Installation des SBS 2003 müssen Sie auf dem Quellserver den DHCP-Serverdienst beenden, sofern dieser dort ausgeführt wird. Sobald der Quell- und Zielserver miteinander verbunden werden, darf nur der auf dem Zielserver konfigurierte DHCP-Serverdienst aktiv sein. Um den Dienst auf dem Quellserver zu beenden, geben Sie unter AUSFÜHREN den Befehl Services.msc ein. Doppelklicken Sie dann den Eintrag DHCP-SERVER. Im dann erscheinenden Fenster EIGENSCHAFTEN klicken Sie auf BEENDEN. Danach setzen Sie den STARTTYP auf DEAKTIVIERT.

Sofern Sie einen Router benutzen, der als DHCP-Server dient, müssen Sie den eben beschriebenen Vorgang nicht durchführen. Dieser Router muss bereits während der Installation des SBS 2003 mit dem Zielserver verbunden sein, damit die DHCP-Einstellungen korrekt konfiguriert werden können. Sie können dabei entscheiden, ob Sie den Router oder den SBS 2003 als DHCP-Server verwenden möchten.

Netzwerk- und Internetverbindung

Weiterhin ist es empfohlen, dass Sie aus dem Netzwerkgerät, das für die Internetverbindung zuständig ist, das Kabel entfernen. Dabei ist es unerheblich, ob es sich um eine Netzwerkkarte bei einem Breitbandzugang oder um ein Modem bei einer Wählverbindung handelt.

Als Nächstes verbinden Sie den Netzwerkadapter des Zielservers, den Sie für interne Netzwerkverbindungen benutzen möchten, mit dem Netzwerk des Quellservers.

Faxmodem

Soll aus dem Quellserver ein Faxmodem ausgebaut und im Zielserver eingebaut werden, so müssen Sie dieses ebenfalls vor Beginn der Installation austauschen.

Administratorkennwort

Bedenken Sie bei einer Migration, dass das Administratorkennwort auf dem Zielserver dem Kennwort des Quellservers entsprechen muss und erst nach Abschluss der Migration neu festgelegt werden kann.

Netzwerkinformationen

Bei der Eingabe der internen Domäneninformationen müssen Sie sicherstellen, dass der NetBIOS-Domänenname nicht gleich dem NetBIOS-Domänennamen des Quellservers ist. Ansonsten wird die Migration fehlschlagen.

Die IP-Adressen des Quell- und Zielservers müssen sich in demselben Adressbereich befinden. Haben Sie versehentlich eine falsche IP-Adresse für den Zielserver angegeben, so können Sie diese nur über das Tool *Change Server Address* ändern. Öffnen Sie dazu in der Serververwaltung den Link INTERNET UND E-MAIL und klicken auf CHANGE SERVER IP ADDRESS. Nur so ist sichergestellt, dass die Umstellung der IP-Adresse für alle Dienste auf dem Zielserver ordnungsgemäß durchgeführt werden kann.

Sofern Sie über die Premium-Edition des SBS 2003 verfügen, können Sie nach Abarbeitung der Aufgabenliste den SQL-Server und den ISA-Server installieren. Allerdings sollten Sie jetzt noch nicht die Firewall Clients verteilen. Dieser Arbeitsgang sollte erst erfolgen, nachdem die Clients wie in Schritt 6 beschrieben ebenfalls migriert worden ist.

Bevor der Zielserver das erste Mal eine Verbindung zum Internet herstellt, sollten Sie eine Antiviren-Software installieren und konfigurieren.

Durchführen der Netzwerkaufgaben

Nachdem Sie die Installation auf dem Zielserver abgeschlossen haben, führen Sie auf diesem, wie im Kapitel 2 der Neuinstallation beschrieben, die Netzwerkaufgaben durch. Dazu zählen die Konfiguration der Internetverbindung, von Sicherheitseinstellungen und Remote Access, die Aktivierung des Servers sowie das Hinzufügen zusätzlicher Clientlizenzen. Hierzu müssen Sie das Netzwerkgerät für die Internetverbindung vorübergehend verkabeln. Nach Durchführung dieser Schritte sollten Sie die Internetverbindung wieder deaktivieren, um ein ungestörtes Migrieren der Daten zu gewährleisten. Hierzu sollte auch der Echtzeit-Virenschutz vorübergehend wieder ausgeschaltet werden.

3.2.3 Schritt 3 – Vorbereiten der Clients

Im nächsten Schritt müssen die Clients der folgenden Betriebssysteme für die Migration auf SBS 2003 vorbereitet werden:

- Windows NT 4.0 Workstation
- Windows 2000 Professional

- Windows XP Professional
- Windows Server 2000
- Windows Server 2003
- Mitgliedserver ab Windows Server NT 4.0

Alle diese Clientcomputer werden mit Hilfe des ADMT migriert. Bei Windows NT 4.0-Clients (Workstation und Server) muss unbedingt das Service Pack 6a installiert sein. Um zu prüfen, ob dieses installiert ist, geben Sie unter AUSFÜHREN den Befehl Winver ein. In der Dialogbox ÜBER WINDOWS NT wird das installierte Service Pack angezeigt. Das Service Pack können Sie unter der Adresse *http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp* downloaden.

Verwenden Sie hingegen Clients mit den Betriebssystemen Windows 95, 98 oder ME, so müssen Sie diese manuell migrieren. Dieses Verfahren wird unter Schritt 6 beschrieben. Sollen bei der Migration eines Windows Server 2000 als zusätzliche Domänencontroller eingerichtete migriert werden, so müssen Sie von diesen zunächst das Active Directory deinstallieren. Geben Sie dazu unter AUSFÜHREN den Befehl DCPROMO ein. Danach kann das Computerkonto zur Zieldomäne migriert und der Computer als zweiter Server hinzugefügt werden. Bedenken Sie, dass Sie für jeden Mitgliedserver innerhalb der SBS 2003-Domäne eine SBS 2003-CAL benötigen.

Im Detail führen Sie jetzt die folgenden Aufgaben aus:

- Sofern die Benutzer nicht ihre Outlook-Postfachregeln exportiert haben, müssen Sie dieses jetzt durchführen.
- Stellen Sie sicher, dass auf dem Quellserver die Gruppe der Domänenadministratoren zur vordefinierten Gruppe der Administratoren gehört. Sollten Sie die Gruppe auf einem beliebigen Client aus der vordefinierten Gruppe gelöscht haben, so müssen Sie diese wieder hinzufügen.
- Sofern auf den Clientcomputern noch Firewalls, z.B. die Internetverbindungs-Firewall unter Windows XP, aktiv sind, müssen diese nun ebenfalls deaktiviert werden.
- Bei einem Update des SBS 2000 müssen Sie auch den Microsoft Shared Modem Service Client entfernen. Sofern Sie unter SBS 2000 den ISA-Server verwendet haben und dieses nun nicht mehr möchten, so müssen Sie auch den Microsoft Firewall Client entfernen.
- Um die korrekte DHCP-Konfiguration zu gewährleisten, müssen Sie für jeden Client die IP-Adresse freigeben und danach wieder erneuern. Damit ist sichergestellt, dass sämtliche Clients ihre IP-Adresse nun vom neuen DHCP-Server auf dem SBS 2003 beziehen.
- Als Nächstes löschen Sie die Desktop-Verknüpfungen der gemeinsam genutzten Benutzerordner und des Firmenordners. Weiterhin müssen Sie sämtliche Verknüpfungen löschen oder aktualisieren, die noch auf den Quellserver verweisen. Dasselbe gilt auch für Einträge im Ordner Internet Favoriten, die auf den Quellserver verweisen, so z.B. die Microsoft Small Business Server-Webseite oder die Small Business-Serververwaltung.

- Auch Netzwerkdrucker oder Faxdrucker, die auf den Quellserver verweisen, müssen gelöscht werden. Die Drucker werden stattdessen auf dem Zielserver neu konfiguriert (siehe Schritt 5) und stehen dann wieder für die Clients zur Verfügung.
- Abschließend sollten Sie auf jedem Computer eine Virenprüfung durchführen und danach den Echtzeit-Virenschutz deaktivieren. Melden Sie sich zum Schluss vom jeweiligen Client ab.

3.2.4 Schritt 4 – Durchführung der Migration

Zur Durchführung der Migration wird das Programm ADMT auf dem Zielserver installiert, um damit die bestehenden Computer-, Benutzer- und Gruppenkonten zu migrieren. Da ADMT auch mit dem Quellserver arbeitet, müssen Sie DNS-Forwarder auf beiden Servern einrichten. Anhand der unter Schritt 1oder 2 gesammelten Clientinformationen müssen Sie entscheiden, ob die Kontingente für Exchange angepasst werden müssen oder nicht. Zusätzlich müssen gemeinsam genutzte Ordner und Applikationsdaten auf den Zielserver verschoben werden. Beim Einsatz des SQL-Servers müssen auch die SQL-Datenbanken auf den Zielserver verschoben werden. Spätestens jetzt sollten Sie ein Backup des Quellservers durchführen, sofern dies nicht bereits geschehen ist.

Installation des ADMT

Zunächst installieren Sie ADMT auf dem Zielserver. Sie finden das Programm auf der CD 1 des SBS 2003 im Verzeichnis \I386\ADMT\ADMIGRATION.MSI. Folgen Sie zur Installation den Hinweisen des Installationsassistenten.

DNS-Weiterleitungen

Für die Funktionalität von ADMT müssen Sie auf beiden Servern DNS-Weiterleitungen einrichten. Führen Sie dazu folgende Schritte aus:

1. Öffnen Sie auf dem Quellserver START/PROGRAMME/VERWALTUNG/DNS.
2. Wählen Sie aus dem Kontextmenü des Servers den Eintrag EIGENSCHAFTEN. Auf der Registerkarte WEITERLEITUNGEN geben Sie dann die IP-Adresse des Zielservers ein und klicken auf HINZUFÜGEN.
3. Öffnen Sie dann auf dem Zielserver wie eben beschrieben die Registerkarte WEITERLEITUNGEN. Klicken Sie hier auf NEU.
4. Geben Sie im Fenster NEUE WEITERLEITUNG den vollständigen Domänennamen der Quelldomäne an, z.B. sbs2000.local.
5. Geben Sie dann in das Feld WEITERLEITUNGS-IP-ADRESSLISTE die IP-Adresse des Quellservers ein und klicken auf HINZUFÜGEN.

ADMT-Konfiguration auf dem Zielserver

Sofern sich in Ihrer Domäne Clients mit dem Betriebssystem Windows NT 4.0 Workstation oder Mitgliedserver unter Windows Server NT 4.0 befinden, müssen Sie zunächst die folgenden Schritte ausführen:

1. Geben Sie auf dem Zielserver unter AUSFÜHREN den Befehl cmd ein. An der Eingabeaufforderung geben Sie die beiden folgenden Zeilen ein:

```
Net local group "Pre-Windows 2000 Compatible Access" everyone /add ↵
Net local group "Pre-Windows 2000 Compatible Access" "anonymus logon" /
add ↵
```

Beachten Sie, dass Sie in den beiden Befehlszeilen unbedingt die Anführungszeichen angeben.

2. Führen Sie danach einen Neustart des Zielservers durch.

Migration von Benutzerkonten

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein:

```
Runas /netonly /user:NameQuelldomäne\Administrator "mmc\"%ProgramFiles%\
Active Directory Migration Tool\Migrator.msc\"" ↵
```

Ersetzen Sie dabei NameQuelldomäne durch den entsprechenden NetBIOS-Domänennamen.

Wenn Sie ADMT schließen, dürfen Sie es nur über den eben genannten Befehl öffnen und nicht über den Eintrag im Startmenü.

2. Geben Sie nach Aufforderung das Kennwort für das Administratorkonto an. Danach erscheint die GUI des ADMT.
3. Im Menü ACTION klicken Sie auf USER ACCOUNT MIGRATION WIZARD. Konfigurieren Sie dort den Wizard mit den folgenden Informationen:

Bei der Migration werden Benutzerkonten, deren Name mehr als 20 Zeichen umfasst, automatisch auf 20 Zeichen eingekürzt und somit möglicherweise auf dem Zielserver nur noch verstümmelt dargestellt.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Test or Make changes	Klicken Sie hier auf TEST THE MIGRATION SETTINGS AND MIGRATE LATER?. So können Sie anhand der Log-Dateien mögliche Fehler erkennen und beheben. Zum endgültigen Migrationslauf klicken Sie hier auf MIGRATE NOW.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Domain Selection	Setzen Sie hier die Namen der Quell- und Zieldomäne. Erhalten Sie nach dem Klick auf NEXT die Fehlermeldung Access denied (Error=5), beenden Sie den ADMT-Wizard und überprüfen, ob die Kennwörter für das Administratorkonto auf dem Quell- und Zielsystem identisch sind und das Passwort beim Neustart des ADMT an der Kommandozeile korrekt eingegeben wurde.
User Selection	Klicken Sie hier auf ADD und dann ADVANCED. Der Eintrag SELECT THIS OBJECT TYPE wird automatisch für die Suche nach Benutzerkonten gesetzt. Klicken Sie dann auf FIND NOW. Sie sehen eine Liste sämtlicher Benutzerkonten. Wählen Sie hier sämtliche Benutzerkonten aus, die Sie migrieren möchten, und klicken dann auf OK. Beachten Sie, dass die folgenden Benutzerkonten nicht migriert werden können: Administrator, Gast, IUSR_Servername, IWAM_Servername, Krbtg sowie die TsInternetUser-Konten. Bei einer Migration des SBS 2000 dürfen zusätzlich nicht die folgenden Konten migriert werden: Small Business Administrator, Small Business Power User sowie Small Business-Benutzerkonten. Bei einer Migration des Exchange Server 2000 darf nicht das Konto SystemMailbox und beim SQL Server 2000 nicht das Konto SQLDebugger und SQLAgentCmdExec migriert werden. Bei weiteren Applikationen, die ein eigenes Benutzerkonto erfordern, wenden Sie sich an die Dokumentation oder den Hersteller der Applikation, ob eine Migration des Exchange Server 2000 möglich ist.
Organizational Unit Selection	Als Ziel-OU (Target OU) navigieren Sie zu MYBUSINESS\USERS\SBBUSERS.
Password Options	Klicken Sie hier SAME AS USER NAME. Damit wird das Passwort automatisch auf die 14 ersten Zeichen des Benutzernamens gesetzt. Diese Einträge werden standardmäßig in die folgende Datei gespeichert: \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT. Diese temporären Passwörter können nach Abschluss der Migration wieder umgesetzt werden. Möchten Sie hingegen die ursprünglichen Passwörter migrieren, so klicken Sie MIGRATE PASSWORDS. Eine Anleitung für die entsprechende Konfiguration zur Passwortmigration finden Sie im Artikel KB 325851 der Microsoft Knowledge Base.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Account Transition Options	Klicken Sie hier auf TARGET SAME AS SOURCE. Aktivieren Sie dann die Checkbox MIGRATE USER SIDS TO TARGET DOMAIN. Klicken Sie dann auf NEXT und danach auf YES. Danach müssen Sie den Quellserver neu starten und sich mit dem Administratorkonto anmelden. Erst dann können Sie auf dem Zielserver auf OK klicken, um fortzufahren.
User Account	Unter USER NAME geben Sie das vordefinierte Administratorkonto an und geben das Passwort ein. Stellen Sie sicher, dass unter DOMAIN der Name der Quelldomäne gesetzt ist.
User Options	Aktivieren Sie hier die Checkbox TRANSLATE ROAMING PROFILES sowie UPDATE USER RIGHTS. Stellen Sie sicher, dass auch die Checkboxen FIX USERS' GROUP MEMBERSHIPS sowie DO NOT RENAME ACCOUNTS markiert sind.
Object Property Exclusion	Standardmäßig werden keine bestimmten Eigenschaften von Objekten von der Migration ausgeschlossen. Um diese Einstellung beizubehalten, klicken Sie auf NEXT.
Naming Conflicts	Hier sollte die Option IGNORE CONFLICTING ACCOUNTS AND DON'T MIGRATE ausgewählt sein.
Completing the User Account Migration Wizards	Sobald Sie zum Abschluss des Wizards auf FINISH geklickt haben, erhalten Sie ein Statusfenster über die Migration. Die Migration der Benutzerkonten ist abgeschlossen, wenn als Status COMPLETED angezeigt wird. Um zu sehen, ob Fehler aufgetreten sind, klicken Sie auf VIEW LOG. Die Log-Datei ist sowohl bei der Simulation der Migration als auch bei der realen Migration verfügbar.

Tabelle 3.2: Der ADMT-Assistent zur Migration von Benutzerkonten

Migration von Gruppenkonten

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein, sofern ADMT nicht noch geöffnet ist:

```
Runas /netonly /user:NameQuelldomäne\Administrator "mmc\"%ProgramFiles%\
Active Directory Migration Tool\Migrator.msc\"" ↵
```

Ersetzen Sie dabei NameQuelldomäne durch den entsprechenden NetBIOS-Domänennamen.

Wenn Sie ADMT schließen, dürfen Sie es nur über den eben genannten Befehl öffnen und nicht über den Eintrag im Startmenü.

2. Geben Sie nach Aufforderung das Kennwort für das Administratorkonto an. Danach erscheint die GUI des ADMT.
3. Im Menü ACTION klicken Sie auf GROUP ACCOUNT MIGRATION WIZARD. Konfigurieren Sie dort den Wizard mit den folgenden Informationen:

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Test or Make Changes	Klicken Sie hier auf TEST THE MIGRATION SETTINGS AND MIGRATE LATER?. So können Sie anhand der Log-Dateien mögliche Fehler erkennen und beheben. Zum endgültigen Migrationslauf klicken Sie hier auf MIGRATE NOW?.
Domain Selection	Unter SOURCE DOMAIN muss der Domänenname der Quelldomäne eingetragen sein, z.B. sbs2000.local, unter TARGET DOMAIN der Name der Zieldomäne, z.B. sbs2003.local.
Group Selection	Klicken Sie hier auf ADD und danach auf ADVANCED. Der Eintrag SELECT THIS OBJECT TYPE wird automatisch für die Suche nach Gruppenkonten gesetzt. Klicken Sie dann auf OBJECT TYPES und deaktivieren die Checkbox BUILTIN SECURITY PRINCIPALS. Klicken Sie dann auf FIND NOW. Sie sehen eine Liste sämtlicher Gruppenkonten. Wählen Sie hier sämtliche Gruppenkonten aus, die Sie migrieren möchten, und klicken dann auf OK. Beachten Sie, dass die folgenden Benutzerkonten nicht migriert werden können: Vordefinierte Sicherheitsgruppen, Cert Publishers, DHCP-Administratoren, DHCP Users, DnsAdmins, DnsUpdateProxy, Domänenadministratoren, Domänencomputer, Domänencontroller, Domänengäste, Domänenbenutzer, Enterprise Admins, Group Policy Creator Owners, RAS und IAS Server, Schema Admins sowie WINS-Benutzer. Bei der Migration eines SBS 2000 dürfen Sie zusätzlich die folgenden Gruppen nicht migrieren: Back Office Fax-Operatoren, Back Office Folder-Operatoren, Back Office-Internetbenutzer, Back Office-Mailoperatoren, Back Office Remote-Operatoren sowie Back Office Template-Benutzer. Bei der Migration des Exchange 2000 Servers dürfen Sie nicht die Gruppen Exchange Domain Servers und Exchange Enterprise Servers migrieren, beim SQL Server 2000 nicht die Gruppe OLAP-Administratoren sowie die Gruppe Domänenname$$$.
Organizational Unit Selection	Für sämtliche Sicherheitsgruppen navigieren Sie nach MYBUSINESS\SECURITYGROUPS, für Verteilergruppen nach MYBUSINESS\DISTRIBUTIONGROUPS als jeweilige Ziel-OU.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Group Options	Wählen Sie hier die Einträge UPDATE USER RIGHTS, FIX MEMBERSHIP OF GROUPS, MIGRATE GROUP SIDS TO TARGET DOMAIN sowie DO NOT RENAME ACCOUNTS.
Object Property Exclusion	Standardmäßig werden keine bestimmten Eigenschaften von Objekten von der Migration ausgeschlossen. Um diese Einstellung beizubehalten, klicken Sie auf NEXT.
User Account	Unter USER NAME geben Sie das vordefinierte Administratorkonto an und geben das Passwort ein. Stellen Sie sicher, dass unter DOMAIN der Name der Quelldomäne gesetzt ist.
Naming Conflicts	Hier sollte die Option IGNORE CONFLICTING ACCOUNTS AND DON'T MIGRATE ausgewählt sein.
Completing the Group Account Migration Wizard	Sobald Sie zum Abschluss des Wizards auf FINISH geklickt haben, erhalten Sie ein Statusfenster über die Migration. Die Migration der Gruppenkonten ist abgeschlossen, wenn als Status COMPLETED angezeigt wird. Um zu sehen, ob Fehler aufgetreten sind, klicken Sie auf VIEW LOG. Die Log-Datei ist sowohl bei der Simulation der Migration als auch bei der realen Migration verfügbar.

Tabelle 3.3: Der ADMT-Assistent zur Migration von Gruppenkonten

Migration von Computerkonten

Eine Migration von Computerkonten kann nur für Computer mit den Betriebssystemen Windows NT 4.0 Workstation und Server, Windows 2000 Professional und Server sowie Windows XP Professional und Windows Server 2003 durchgeführt werden.

Sofern sich in Ihrer Domäne Clients mit dem Betriebssystem Windows NT 4.0 Workstation oder Mitgliedserver unter Windows Server NT 4.0 befinden, müssen Sie zunächst die folgenden Schritte ausführen:

1. Geben Sie auf dem Zielserver unter AUSFÜHREN den Befehl cmd ein. An der Eingabeaufforderung geben Sie die beiden folgenden Zeilen ein:

```
Net local group "Pre-Windows 2000 Compatible Access" everyone /add ↵
Net local group "Pre-Windows 2000 Compatible Access" "anonymus logon" /
add ↵
```

Beachten Sie, dass Sie in den beiden Befehlszeilen unbedingt die Anführungszeichen angeben.

2. Führen Sie danach einen Neustart des Zielservers durch.

Nachdem Sie den Quellserver neu gestartet haben, warten Sie ca. 15 Minuten, damit die DNS-Einträge auf dem Quellserver aktualisiert werden. Wenn Sie diesen Zeitraum nicht abwarten, wird die Konfiguration der Clients für die Zieldomäne nicht funktionieren. Stellen Sie zudem sicher, dass die Gruppe der Domänenadministratoren auf dem Quellserver Mitglied der vordefinierten Administratorengruppe ist. Ist diese Standardeinstellung nicht mehr vorhanden, müssen Sie die Gruppe wieder hinzufügen. Außerdem sollten auf sämtlichen Clientcomputern Echtzeit-Virenschutzprogramme sowie Software-Firewalls deaktiviert werden.

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein, sofern ADMT nicht noch geöffnet ist:

   ```
   Runas /netonly /user:NameQuelldomäne\Administrator "mmc\"%ProgramFiles%\
   Active Directory Migration Tool\Migrator.msc\"" ↵
   ```

   Ersetzen Sie dabei NameQuelldomäne durch den entsprechenden NetBIOS-Domänennamen.

Wenn Sie ADMT schließen, dürfen Sie es nur über den eben genannten Befehl öffnen und nicht über den Eintrag im Startmenü.

2. Geben Sie nach Aufforderung das Kennwort für das Administratorkonto an. Danach erscheint die GUI des ADMT.
3. Im Menü ACTION klicken Sie auf COMPUTER ACCOUNT MIGRATION WIZARD. Konfigurieren Sie dort den Wizard mit den folgenden Informationen:

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Test or Make Changes	Klicken Sie hier auf TEST THE MIGRATION SETTINGS AND MIGRATE LATER?. So können Sie anhand der Log-Dateien mögliche Fehler erkennen und beheben. Zum endgültigen Migrationslauf klicken Sie hier MIGRATE NOW?.
Domain Selection	Unter SOURCE DOMAIN muss der Domänenname der Quelldomäne eingetragen sein, z.B. sbs2000.local, unter TARGET DOMAIN der Name der Zieldomäne, z.B. sbs2003.local.
Computer Selection	Klicken Sie hier auf ADD und danach auf ADVANCED. Der Eintrag SELECT THIS OBJECT TYPE wird automatisch für die Suche nach Computerkonten gesetzt. Klicken Sie dann auf OBJECT TYPES und deaktivieren die Checkbox BUILTIN SECURITY PRINCIPALS. Klicken Sie dann auf FIND NOW. Sie sehen eine Liste sämtlicher Computerkonten. Wählen Sie hier sämtliche Computerkonten aus, die Sie migrieren möchten, und klicken dann auf OK. Beachten Sie, dass Sie nicht das Computerkonto des Quellservers sowie Computerkonten auswählen, auf denen die Betriebssysteme Windows 95, 98 oder ME ausgeführt werden.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
	Zudem müssen Sie sicherstellen, dass sämtliche zu migrierenden Computer eingeschaltet und mit dem Netzwerk verbunden sind. Für sämtliche Server-Computerkonten (außer dem Quellserver, der nicht migriert wird), führen Sie den Computer Migration Wizard erneut aus und fügen die Server auf der Seite ORGANIZATIONAL UNIT SELECTION der OU SBS SERVERS hinzu.
Organizational Unit Selection	Für sämtliche Clientcomputer navigieren Sie nach MYBUSINESS\COMPUTER\SBSCOMPUTER, für Server nach MYBUSINESS\COMPUTER\SBSSERVER als jeweilige Ziel-OU.
Translate Objects	Stellen Sie sicher, dass sämtliche Checkboxen auf dieser Seite aktiviert sind.
Security Translation Object	Hier muss die Option REPLACE aktiviert sein. Klicken Sie dann auf NEXT. Klicken Sie auf OK, wenn die folgende Meldung angezeigt wird: USER RIGHTS TRANSLATION WILL BE PERFORMED IN ‚ADD' MODE ONLY. ANY OTHER OBJECTS WILL BE TRANSLATED IN ADHERENCE TO YOUR MODE SELECTION.
Computer Options	Aktivieren Sie hier die Option DO NOT RENAME COMPUTERS und setzen die Anzahl der Minuten für einen Neustart nach Abschluss des Migrations-Wizards auf 1.
Object Property Exclusion	Standardmäßig werden keine bestimmten Eigenschaften von Objekten von der Migration ausgeschlossen. Um diese Einstellung beizubehalten, klicken Sie auf NEXT.
Naming Conflicts	Hier sollte die Option IGNORE CONFLICTING ACCOUNTS AND DON'T MIGRATE ausgewählt sein.
Completing the User Account Migration Wizard	Sobald Sie zum Abschluss des Wizards auf FINISH geklickt haben, erhalten Sie ein Statusfenster über die Migration. Die Migration der Computerkonten ist abgeschlossen, wenn als Status COMPLETED angezeigt wird. Um zu sehen, ob Fehler aufgetreten sind, klicken Sie auf VIEW LOG. Die Log-Datei ist sowohl bei der Simulation der Migration als auch bei der realen Migration verfügbar. Nachdem Sie auf CLOSE geklickt haben, erhalten Sie im Fenster MIGRATION TOOL AGENT MONITOR eine Statusbox über die Verbindung zu den Clientcomputern.

Tabelle 3.4: Der ADMT-Assistent zur Migration von Computerkonten

Schlägt die Migration eines Computerkontos oder nach der Migration der Agent während der Konfiguration des Clients fehl, führen Sie zur Lösung des Problems die folgenden Schritte durch:

1. Prüfen Sie sämtliche Einträge in den Log-Dateien.
2. Stellen Sie sicher, dass das Computerkonto nicht im Active Directory erstellt worden ist. Öffnen Sie dazu auf dem Zielserver die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
3. Führen Sie den Computer Migration Wizard ein zweites Mal aus, und migrieren Sie das Konto erneut.

Solange Sie die Migration der Computerkonten nur im Testmodus durchführen, erhalten Sie in der Ereignisanzeige eine Meldung mit der Ereignis-ID 37075. Diese ist im Testmodus normal, da bei der Kontenmigration im Test die Domäne nicht geändert wurde.

Nachdem Sie sämtliche Clients erfolgreich migriert haben, dürfen Sie sich jedoch noch nicht an diesen anmelden. Eine Anmeldung ist erst möglich, wenn Schritt 6 – Konfiguration der Clients – abgeschlossen worden ist. Anderenfalls werden die Outlook-Profile nicht migriert.

Änderung von Exchange-Kontingenten

Wenn bei einer Migration von Exchange 2000 auf dem Quellserver ein Mailkontingent für das Senden und Empfangen von E-Mails von 200 MB (200.000 KB) und der Warnwert auf 175 MB (175.000 KB) gesetzt ist, müssen Sie die Einstellungen auf dem Zielsystem nicht ändern. Sind auf dem Quellsystem jedoch höhere Werte gesetzt, so müssen Sie diese Kontingentwerte für das Zielsystem anpassen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie auf dem Quellserver die SERVERVERWALTUNG aus dem STARTMENÜ und klicken auf ERWEITERTE VERWALTUNG.
2. Doppelklicken Sie auf ORGANISATIONSNAME (EXCHANGE), ADMINISTRATIVE GRUPPEN, ERSTE ADMINISTRATIVE GRUPPE, dann auf SERVER und IHREN SERVER. Doppelklicken Sie dann auf ERSTE SPEICHERGRUPPE und wählen aus dem Kontextmenü von POSTFACHSPEICHER den Eintrag EIGENSCHAFTEN.
3. Öffnen Sie die Registerkarte GRENZWERTE, und notieren Sie sich die Werte für die maximale Postfachgröße sowie den Warnwert.
4. Öffnen Sie dann die Registerkarte GRENZWERTE wie eben beschrieben auf dem Zielserver und tragen die Werte des Quellservers entsprechend ein.

Verschieben von Exchange-Postfächern

Die Postfächer des Exchange Server 2000 werden mit Hilfe des *Exchange Server-Migrationsassistenten* auf den Zielserver migriert. Zu diesem Zeitpunkt dürfen Sie sich an keinem der Clients anmelden und Outlook öffnen. Ansonsten wird das Outlook-Profil nicht migriert. Das Starten von Outlook ist erst nach Abschluss von Schritt 6 – Konfiguration der Clients – möglich.

Während der Migration des Exchange-Servers sollten auf diesem ebenfalls Echtzeit-Virenschutzprogramme sowie und Disk Utilities beendet werden.

Um die Postfächer zu migrieren, führen Sie die folgenden Schritte aus:

1. Auf dem Zielserver öffnen Sie START/PROGRAMME/MICROSOFT EXCHANGE/BEREITSTELLUNG/ASSISTENT FÜR DIE MIGRATION. Geben Sie im Laufe des Migrationsassistenten die folgenden Informationen ein:

Seite des Migrationsassistenten	Vorzunehmender Eintrag
Migration	Wählen Sie hier MIGRATION VON MICROSOFT EXCHANGE.
Migration von Exchange Server	Klicken Sie hier auf WEITER.
Migrationsziel	Hier können Sie nur die Standardeinstellung MIGRATION AUF EINEN COMPUTER, DER EXCHANGE SERVER AUSFÜHRT akzeptieren.
Quell-Exchange Server	Deaktivieren Sie hier die Checkbox EXCHANGE 5.5 SERVER. Geben Sie den Computernamen, das Administratorkonto sowie dessen Passwort an.
Migrationsinformationen	Bestätigen Sie die Standardeinstellung ERSTELLEN VON E-MAIL-KONTEN.
Kontenmigration	Wählen Sie hier sämtliche Konten aus, die Sie migrieren möchten. Mit Hilfe des Assistenten kann jedoch nicht das Postfach des Administrators migriert werden. Um dieses Konto zu exportieren, sichern Sie von einem Outlook-Client aus die Mails in eine pst-Datei und spielen diese später wieder zurück. Auch die Regeln für das Administrator-Postfach müssen exportiert werden. Die Migration der Postfächer für die Benutzerkonten kann erst durchgeführt werden, nachdem Sie die Benutzerkonten mit Hilfe des ADMT auf das Zielsystem migriert haben.
Container for New Windows Account	Navigieren Sie hier zu DOMÄNENNAME\MYBUSINESS\USERS\SBSUSERS.

Tabelle 3.5: Der Microsoft Exchange-Migrationsassistent

2. Folgen Sie den Anweisungen, um den Migrationsassistenten abzuschließen.

Verschieben der gemeinsam genutzten Benutzerordner

Die gemeinsam genutzten Benutzerordner verschieben Sie am einfachsten mit dem Befehl xcopy an der Kommandozeile. Alternativ können Sie auch das Programm *Robo Copy* benutzen. Dieses Programm ist Bestandteil der Windows Server 2003 Resource Kit-Tools und kann unter *http://go.microsoft.com/fwlink/?LinkId=20249* downgeloadet werden.

Stellen Sie vor dem Kopiervorgang sicher, dass die Benutzerordner nicht größer als 1 GB sind. Standardmäßig ist unter SBS 2003 das Kontingent für die Größe des Benutzerordners auf 1 GB festgelegt.

1. Zum Verschieben der Benutzerordner öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein:

```
Xcopy \\Quellserver\Users \\Zielserver\Users /e /o /d /h /v /c>>c:\
Kopier.txt ↵
```

In dieser Befehlszeile haben die Parameter die folgende Bedeutung:

`/e`: Es werden alle Unterverzeichnisse kopiert, auch wenn diese ohne Inhalt sind.

`/o`: Es werden die Informationen der Discretionary Access Control List (DACL) sowie die Informationen über den Besitzer der Dateien kopiert.

`/d`: Es werden nur die Dateien kopiert, deren Quellzeit neuer ist als die Zielzeit. Sollen nur die Dateien kopiert werden, die nach einem bestimmten Zeitpunkt erstellt worden sind, so verwenden Sie die Option /d: m-t-j, wobei das Datum im Format Monat-Tag-Jahr angegeben werden muss.

`/h`: Es werden auch versteckte Dateien sowie Systemdateien kopiert.

`/v`: Jede neu geschriebene Datei wird überprüft.

`/c`: Sämtliche Fehler werden ignoriert.

`>>C:\Kopier.txt`: Die Ergebnisse der Kopieraktion werden in die Datei *Kopier.txt* auf Laufwerk C geschrieben. Prüfen Sie diese Datei nach Abschluss des Kopiervorgangs darauf, ob in ihr Fehlermeldungen verzeichnet sind. Zudem können Sie auch die Anzahl und Größe der Dateien in den Benutzerordnern auf dem Quell- und Zielserver miteinander vergleichen.

Benutzerdefinierte Login-Skripte

Haben Sie auf dem Quellsystem benutzerdefinierte Login-Skripte verwendet, so kopieren Sie diese vom Ordner NETLOGON des Quellservers in den Ordner NETLOGON des Zielservers. Wird in den Skripten auf weitere Dateien verwiesen, so müssen Sie diese selbstverständlich auch auf den Zielserver kopieren.

Verschieben weiterer gemeinsam genutzter Ordner

Erstellen Sie auf dem Zielserver für jeden zu verschiebenden Ordner eine gleichnamige Freigabe, und vergeben Sie an diese dieselben Berechtigungen wie auf dem Quellserver. Danach verschieben Sie die Inhalte der Ordner, wie unter „Verschieben gemeinsam genutzter Benutzerordner“ weiter oben in diesem Kapitel beschrieben.

Bedenken Sie beim Erstellen der Freigaben auf dem Zielserver, sofern Sie diese auf derselben Partition erstellen wie die Benutzerordner, dass die gesetzten Kontingenteinstellungen auch für die weiteren Ordner greifen.

Verschieben des Ordners Company an die Intranet-Webseite

Der unter SBS 2000 verwendete Ordner COMPANY ist unter SBS 2003 in diesem Format nicht mehr vorhanden. Vielmehr werden die Inhalte an die interne Webseite geleitet, die von den SharePoint Services bereitgestellt wird. Führen Sie zum Verschieben des Ordners die folgenden Schritte aus:

1. Öffnen Sie auf dem Zielserver die SERVERVERWALTUNG und klicken auf INTERNE WEBSEITE.
2. In der Detailansicht klicken Sie auf DATEIEN IMPORTIEREN. Es erscheint ein Assistent.
3. Auf der Seite DATEI- UND DOKUMENTBIBLIOTHEKSPFAD geben Sie unter DATEIEN KOPIEREN VON den Pfad *Quellserver**Company* ein. Unter DATEIEN KOPIEREN NACH können Sie entweder die Standardeinstellung HTTP://COMPANYWEB/GENERAL DOCUMENTS akzeptieren oder über DURCHSUCHEN eine andere Bibliothek bestimmen oder erstellen.
4. Beim Kopieren werden standardmäßig alle Dateien, die größer als 50 MB sind, nicht kopiert. Um diese Einstellung zu ändern, öffnen Sie ein Browserfenster und geben die Adresse *http://Zielserver:8081* ein. Klicken Sie hier auf KONFIGURIEREN DER VIRTUELLEN SERVEREINSTELLUNGEN, dann auf COMPANYWEB und danach auf GENERELLE EINSTELLUNGEN. Hier können Sie die Maximalgröße bestimmen.
5. Weiterhin werden standardmäßig auch keine Dateien mit bestimmten Dateiendungen, wie z.B. *.exe* oder *.vbs* blockiert. Um diese Einstellungen zu ändern, geben Sie in einem Browserfenster ebenfalls die Adresse *http://Zielserver:8081* ein. Klicken Sie dann auf GESPERRTE DATEITYPEN VERWALTEN, um die Einstellungen zu modifizieren.

Generell werden nur Dateien kopiert, die auch Daten enthalten.

Verschieben weiterer Daten

Sollen noch weitere Daten verschoben werden, die sich nicht in den bisher beschriebenen Ordnern befinden, so müssen Sie diese ebenfalls kopieren. Dies gilt auch für Applikationsdaten. Spielen bei diesen Daten die Berechtigungen keine Rolle, so können Sie diese einfach kopieren. Sollen hingegen die Informationen über die Besitzer der Dateien sowie die Einträge der DACL beibehalten werden, so verwenden Sie das Programm *Xcopy* oder *Robo Copy*. Das genaue Vorgehen finden Sie weiter oben beschrieben.

Verwenden Sie SQL-Datenbanken, die ebenfalls migriert werden müssen, so führen Sie die folgenden Schritte aus:

1. Geben Sie an der Eingabeaufforderung des Zielservers folgenden Befehl ein: \\ Quellserver\Laufwerksbuchstabe$
2. Navigieren Sie auf diesem Laufwerk zum Speicherort der gewünschten Dateien, und kopieren Sie diese an den gewünschten Ort auf dem Zielserver. Wiederholen Sie diesen Vorgang für die Datenverzeichnisse sämtlicher Applikationen.

Haben Sie auf dem Quellserver eigene Webseiten unter dem IIS (Internet Information Server) erstellt, so müssen Sie diese Dateien auf den Zielserver kopieren und danach die Webseiten unter IIS 6.0 neu erstellen. Für diesen Vorgang können Sie auch das *IIS 6.0-Migrationstool* benutzen. Dieses befindet sich auf der Begleit-CD.

Zu diesem Zeitpunkt können Sie bereits alle erforderlichen Applikationen auf dem Zielserver installieren.

Verschieben von SQL-Datenbanken

Sofern Sie die Premium-Version des SBS 2003 verwenden und bestehende Datenbanken des SQL Servers migrieren wollen, führen Sie die folgenden Schritte aus:

1. Wenn auf dem Zielserver der SQL Server 2000 noch nicht installiert ist, führen Sie die Installation jetzt durch.

Weitere Informationen zum Verschieben von SQL-Datenbanken zwischen SQL-Servern finden Sie im Microsoft Knowledge-Base-Artikel 314546 sowie zum Thema Wiederherstellung in Kapitel 7.6.4.

3.2.5 Schritt 5 – Konfiguration des Zielservers

In diesem Arbeitsschritt verbinden Sie die Benutzerkonten mit einer Benutzervorlage des SBS 2003 und verteilen Applikationen an die Clients, so dass diese bei der ersten Anmeldung bereits auf das SBS 2003-Netzwerk zugreifen können. Zusätzlich müssen auf dem Zielserver weitere Konfigurationseinstellungen vorgenommen werden. Ferner werden Exchange-Einstellungen vervollständigt, wie z.B. das Erstellen von Verteilerleisten oder die Konfiguration des Microsoft Connectors für POP3-Postfächer. Im Detail führen Sie die folgenden Schritte durch:

Berechtigungen für die migrierten Konten

Damit die Benutzer für den Zugriff auf die Ressourcen des SBS 2003-Netzwerks über die korrekten Berechtigungen verfügen, müssen die Benutzerrechte auf dem Zielserver festlegen.

Im Zuge dieser Einstellungen legen Sie auch – sofern erforderlich – die Berechtigungen für Remote-Zugriff fest. Sie können auch das Connection Manager Configuration Package verteilen. Hiermit werden die erforderlichen Einstellungen für die Verbindung von mobilen und Remote-Clients konfiguriert.

Für das Festlegen der Benutzerrechte führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf dem Zielserver die SERVERVERWALTUNG. Klicken Sie dort auf BENUTZER und dann auf BENUTZERVERWALTUNG.
2. Auf der Seite der VORLAGENAUSWAHL wählen Sie für jedes migrierte Konto eine Kontenvorlage des SBS 2003 aus. Die Standardeinstellung zum Beibehalten der Benutzerrechte sollten Sie übernehmen.

Erscheint ein Benutzerkonto nicht auf der Seite der Benutzerauswahl, so stellen Sie sicher, dass dieses Konto nicht deaktiviert ist. Um dies zu prüfen, öffnen Sie die SERVERVERWALTUNG auf dem Zielserver, klicken auf BENUTZER, und in der Detailansicht wählen Sie aus dem Kontextmenü des deaktivierten Kontos den Eintrag AKTIVIEREN.

3. Folgen Sie dann den Anweisungen, um den Assistenten abzuschließen.

Haben Sie vor der Migration noch keinen Exchange Server verwendet, so wird jetzt für jeden Benutzer automatisch ein Postfach angelegt.

Verteilen von Applikationen

Die Verteilung von Applikationen kann nur an Clients mit den Betriebssystemen Windows 2000 und XP Professional erfolgen. Für alle anderen Betriebssysteme muss die Installation manuell auf dem Client durchgeführt werden. Für Mitgliedserver unter Windows Server NT 4.0 finden Sie weitere Hinweise in der Serververwaltung unter SERVERCOMPUTER/WEITERE INFORMATIONEN/KONFIGURIEREN ZUSÄTZLICHER SERVER.

Bevor Sie die folgenden Schritte ausführen und über mehr als fünf Clients verfügen, müssen Sie zunächst zusätzliche Lizenzen hinzufügen. Im SBS 2003 sind lediglich fünf CALs inbegriffen.

1. Öffnen Sie auf dem Zielserver die SERVERVERWALTUNG und klicken auf CLIENTCOMPUTER.
2. In der rechten Fensterhälfte klicken Sie auf ZUWEISEN VON APPLIKATIONEN AN CLIENTCOMPUTER. Es erscheint ein Assistent, bei dem Sie die folgenden Informationen eingeben:

Seite des Assistenten	Vorzunehmender Eintrag
Clientcomputer	Wählen Sie hier sämtliche Clients aus, an die Sie Client-Applikationen verteilen möchten.
Client-Applikationen	Bestätigen Sie hier die Standardeinstellungen. Verwenden Sie auf dem Zielsystem den ISA-Server 2000, müssen Sie den Firewall-Client an alle Clients verteilen. Klicken Sie hierzu auf APPLIKATIONEN ÄNDERN. Auf der Seite VERFÜGBARE APPLIKATIONEN klicken Sie auf HINZUFÜGEN. Geben Sie dann den Applikationsnamen Firewall-Client ein oder navigieren über DURCHSUCHEN zu \\ZIELSERVER\MSPCLNT\SETUP.EXE

Tabelle 3.6: Der Assistent zum Zuweisen von Client-Applikationen

3. Folgen Sie zum Abschluss den Anweisungen des Assistenten.

Die Aufgabenliste der Verwaltungsaufgaben abschließen

Sofern Sie diese Liste zwischendurch geschlossen haben, können Sie sie wieder öffnen, indem Sie in der SERVERVERWALTUNG die AUFGABENLISTE anklicken. Sie können jetzt die folgenden Verwaltungsaufgaben durchführen:

- Hinzufügen eines neuen Druckers: Hier können Sie sämtliche Drucker neu einrichten.
- Hinzufügen von Benutzern und Computern. Dieser Schritt ist nur notwendig, wenn Sie zu den migrierten Konten noch neue hinzufügen möchten.
- Faxkonfiguration: Verfügen Sie über ein Faxmodem, so können Sie dieses jetzt einrichten.
- Konfiguration der Überwachung: Hier können Sie Berichte über die Server-Performance sowie die Auslastung konfigurieren. Auch die Benachrichtigungen für Alarmoptionen werden hier bestimmt.
- Konfiguration des Backups: Hier können Sie die Optionen für das Windows-Backup festlegen. Verwenden Sie das Backup-Programm eines Drittanbieters, so müssen Sie hier keine Einstellungen vornehmen.

Diese Verwaltungsaufgaben wurden bereits ausführlich in Kapitel 2 abgehandelt.

Übernahme benutzerdefinierter Einstellungen vom Quellserver

In diesem Schritt werden sämtliche benutzerdefinierten Konfigurationen wie z.B. DHCP-Bereichsoptionen, Einstellungen für Routing und RAS, Einstellungen an den Gruppenrichtlinien oder DNS auf dem Zielserver eingestellt. Kurz gesagt, werden in diesem Schritt sämtliche relevanten Einstellungen manuell auf den Zielserver übertragen, die durch keinerlei Assistenten migriert werden können.

E-Mail-Verteilerlisten und Empfangsrichtlinien

Auf dem Zielserver müssen Sie sämtliche benutzerdefinierte Empfangsrichtlinien wieder herstellen. Dasselbe gilt auch für migrierte Verteilergruppen, in denen sich vordefinierte Gruppen wie z.B. die Administratorengruppe als Mitglied befanden. Sie müssen nun die vordefinierten Gruppen des Zielservers wieder zur Verteilergruppe hinzufügen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die SERVERVERWALTUNG und dort den Eintrag VERTEILERGRUPPEN.
2. Klicken Sie in der rechten Fensterhälfte auf die gewünschte Verteilergruppe. Auf der Registerkarte MITGLIEDER können Sie die gewünschten vordefinierten Gruppenkonten wieder hinzufügen.

Microsoft Connector für POP3-Postfächer

Diese Konfiguration müssen Sie vornehmen, wenn Sie über POP3-Postfächer verfügen, die Sie auf den Exchange-Server downloaden möchten. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie in der SERVERVERWALTUNG den Eintrag INTERNET UND E-MAIL.
2. Klicken Sie in der rechten Fensterhälfte auf POP3 E-MAIL VERWALTEN. Klicken Sie dann auf POP3 CONNECTOR-MANAGER ÖFFNEN.
3. Die weitere Konfiguration von POP3-E-Mail entspricht den im Rahmen der Aufgabenliste in Kapitel 2 beschriebenen Schritten.

Aktualisieren benutzerdefinierter Login-Skripte

Nachdem Sie die benutzerdefinierten Login-Skripte bereits im Laufe der Migration in das Verzeichnis NETLOGON des Zielservers kopiert haben, müssen diese nun für die Benutzer nutzbar gemacht werden. Dazu müssen Sie jedes Benutzerkonto aktualisieren, so dass es auf das Login-Skript auf dem Zielserver referenziert. Zusätzlich müssen Sie im Login-Skript sämtliche Verweise auf den Quellserver mit den Verweisen auf den Zielserver aktualisieren.

3.2.6 Schritt 6 – Konfiguration der Clients

In diesem Schritt erhalten die Windows 2000- und XP Professional-Clients automatisch die Konfigurationseinstellungen für E-Mail und Proxy. Auf allen anderen Client-Betriebssystemen müssen Sie die Konfiguration manuell vornehmen. Weiterhin können Sie nun auch die öffentlichen Exchange-Ordner importieren, so dass die Clients vollständig für die Verbindung mit dem neuen Exchange-Server konfiguriert sind. Im Detail führen Sie die folgenden Schritte durch:

Konfiguration von Windows 2000- bzw. XP-Clients

1. Melden Sie sich an jedem Clientcomputer mit dem jeweiligen Benutzerkonto an. Sie werden bei der Anmeldung aufgefordert, für das Konto ein neues Passwort festzulegen. Notieren Sie sich jeweils das vergebene Passwort. Achten Sie hierbei bereits auf die Passwortsicherheit, da Sie den Zielserver nach Abschluss der Migration mit dem Internet verbinden. Sofern Sie die alten Benutzerpasswörter nicht migriert haben, sind die Passwörter standardmäßig alle in der Datei \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT. Wie bereits erwähnt, besteht das Passwort aus den ersten 14 Zeichen des Benutzernamens.
2. Haben Sie den Client unter Schritt 5 (siehe Kapitel 3.2.5) für die Verteilung von Applikationen ausgewählt, so erscheint nach dem Start der Client-Installations-Wizard. Klicken Sie in diesem auf JETZT STARTEN.
3. Öffnen Sie dann die SYSTEMSTEUERUNG und doppelklicken auf MAIL. Aktualisieren Sie dann die E-Mail-Eigenschaften gemäß dem Zielserver.

Verwenden Sie auch den ISA-Server, müssen Sie auch die Proxy-Einstellungen des Internet Explorers konfigurieren.

1. Öffnen Sie dazu den Internet Explorer. Im Menü EXTRAS klicken Sie auf INTERNETOPTIONEN.
2. Auf der Registerkarte VERBINDUNGEN klicken Sie unter LAN-EINSTELLUNGEN auf EINSTELLUNGEN.
3. Aktivieren Sie die Checkbox PROXY-SERVER FÜR LAN VERWENDEN und tragen unter ADRESSE den Namen des Zielservers und unter PORT 8080 ein.
4. Haben Sie lediglich auf dem Quellserver den ISA-Server verwendet, jedoch nicht auf dem Zielserver, so stellen Sie sicher, dass die Proxy-Checkbox in den LAN-EINSTELLUNGEN sowie dort auch die Checkbox AUTOMATISCHE SUCHE DER EINSTELLUNGEN unter AUTOMATISCHE KONFIGURATION deaktiviert ist.

Danach können Sie auf dem Client wieder den Echtzeit-Virenschutz aktivieren. Fahren Sie dann im Abschnitt „Herstellung der Internetverbindung“ fort.

Konfiguration älterer Windows-Clients

Clientcomputer mit älteren Betriebssystemen als Windows 2000 müssen manuell für die Zieldomäne konfiguriert werden, danach werden manuell die Applikationen auf ihnen installiert.

1. Nachdem Sie diese beiden Vorbereitungen abgeschlossen haben, melden Sie sich an jedem Clientcomputer mit dem jeweiligen Benutzerkonto an. Sie werden bei der Anmeldung aufgefordert, für das Konto ein neues Passwort festzulegen.

Notieren Sie sich jeweils das vergebene Passwort. Achten Sie hierbei bereits auf die Passwortsicherheit, da Sie den Zielserver nach Abschluss der Migration mit dem Internet verbinden. Sofern Sie die alten Benutzerpasswörter nicht migriert haben, sind die Passwörter standardmäßig alle in der Datei \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT. Wie bereits erwähnt, besteht das Passwort aus den ersten 14 Zeichen des Benutzernamens.

2. Öffnen Sie dann die SYSTEMSTEUERUNG und doppelklicken auf MAIL. Aktualisieren Sie dann die E-Mail-Eigenschaften gemäß dem Zielserver.
3. Löschen Sie sämtliche Favoriten des Internet Explorers, die auf den Quellserver verweisen, da diese nicht länger gültig sind.
4. Löschen oder aktualisieren Sie sämtliche Desktop-Verknüpfungen mit den gemeinsam genutzten Benutzer- und Firmenordnern. Dies gilt auch für Verknüpfungen mit Netzlaufwerken und weiteren Verknüpfungen, die sich auf den Quellserver beziehen.
5. Sind hier Drucker und Faxgeräte konfiguriert, die auf den Quellserver verweisen, so löschen Sie diese. Aktualisierte Drucker und Faxgeräte wurden bereits in Schritt 5 – Konfiguration des Zielservers – eingerichtet.
6. Ist der Firewall-Client des ISA-Servers bereits installiert, müssen Sie den Namen des ISA-Servers gemäß dem des Zielservers auf den Clients anpassen. Doppelklicken Sie dazu das FIREWALL CLIENT-Icon im System-Tray. In den dann erscheinenden Optionen tragen Sie den neuen Servernamen ein.

Verwenden Sie auch den ISA-Server, müssen Sie auch die Proxy-Einstellungen des Internet Explorers konfigurieren.

1. Öffnen Sie dazu den Internet Explorer. Im Menü EXTRAS klicken Sie auf INTERNETOPTIONEN.
2. Auf der Registerkarte VERBINDUNGEN klicken Sie unter LAN-EINSTELLUNGEN auf EINSTELLUNGEN.
3. Aktivieren Sie die Checkbox PROXY-SERVER FÜR LAN VERWENDEN und tragen unter ADRESSE den Namen des Zielservers und unter PORT 8080 ein.
4. Haben Sie lediglich auf dem Quellserver den ISA-Server verwendet, jedoch nicht auf dem Zielserver, so stellen Sie sicher, dass die Proxy-Checkbox in den LAN-EINSTELLUNGEN sowie dort auch die Checkbox AUTOMATISCHE SUCHE DER EINSTELLUNGEN unter AUTOMATISCHE KONFIGURATION deaktiviert ist.

Danach können Sie auf dem Client wieder den Echtzeit-Virenschutz aktivieren.

Überprüfen der Netzwerkverbindung

Abschließend müssen Sie prüfen, ob die migrierten Clients einen funktionierenden Netzwerkzugang haben. Um dies zu testen, trennen Sie den Quellserver vom Netzwerk und senden eine Test-E-Mail an die Benutzer. Erreicht die Mail ihre Empfänger, sind die Interneteinstellungen korrekt konfiguriert.

Zusätzlich müssen Sie auch testen, ob freigegebene Ordner, gemeinsam genutzte Applikationen sowie Netzwerkdrucker verfügbar sind und funktionieren.

Nach Abschluss dieser Schritte können Sie sich an einem Client als Administrator einloggen und das Postfach sowie Regeln für das Administratorkonto auf den Zielserver importieren.

Offline-Adressbücher stehen frühestens eine Stunde nach der Installation des SBS 2003 zur Verfügung. Versuchen Sie bereits früher einen Zugriff, so wird dieser fehlschlagen, da das Offline-Adressbuch zu diesem Zeitpunkt noch nicht generiert ist.

Import öffentlicher Ordner

Als Nächstes werden die in eine .pst-Datei exportierten öffentlichen Ordner des Quellservers wieder importiert. Führen Sie dazu die folgenden Schritte durch:

1. Melden Sie sich auf einem Client mit dem Administratorkonto an und starten *Outlook*.
2. Doppelklicken Sie ÖFFENTLICHE ORDNER und dann ALLE ÖFFENTLICHEN ORDNER.
3. Importieren Sie dann die .pst-Datei in den aktuell ausgewählten Ordner.

Waren für einen der öffentlichen Ordner spezielle Berechtigungen konfiguriert, so müssen Sie diese wieder herstellen.

1. Öffnen Sie dazu auf dem Zielserver die SERVERVERWALTUNG. Doppelklicken Sie dort auf ERWEITERTE VERWALTUNG, ADMINISTRATIVE GRUPPEN, ERSTE ADMINISTRATIVE GRUPPE, SERVER, IHR SERVER, ERSTE SPEICHERGRUPPE, INFORMATIONSSPEICHER FÜR ÖFFENTLICHE ORDNER, ÖFFENTLICHE ORDNER.
2. In der rechten Fensterhälfte wählen Sie aus dem Kontextmenü des gewünschten Ordners den Eintrag EIGENSCHAFTEN.
3. Auf der Registerkarte BERECHTIGUNGEN klicken Sie auf CLIENT-BERECHTIGUNGEN. Aktualisieren Sie dann die Felder NAME, ROLLE und BERECHTIGUNGEN mit den gewünschten Einträgen.

3.2.7 Schritt 7 – Abschluss der Migration

Nach Abschluss der Migration können Sie den Quellserver außer Betrieb setzen. Es ist jedoch sinnvoll, diesen für eine Übergangszeit noch bereitzuhalten, um so mögliche Konfigurationsprobleme des neuen Servers beheben zu können, sofern es sich dabei um Informationen handelt, die vom alten Server manuell übernommen werden können. Erst nach dieser Übergangszeit sollten Sie den alten Server ganz außer Betrieb nehmen und formatieren. Sie können dieses Gerät beispielsweise als zweiten Server einrichten.

Weiterhin wird das ADMT wieder vom Zielserver deinstalliert, und alle Prä-Windows 2000-Berechtigungen, die im Verlauf der Migration möglicherweise temporär heraufgesetzt wurden, müssen aus Sicherheitsgründen wieder auf die Ursprungswerte zurückgesetzt werden.

Löschen der DNS-Weiterleitungen

Für die Benutzung des ADMT mussten Sie auf dem Zielserver DNS-Forwarder auf den Quellserver eintragen. Diese Einträge sind jetzt überflüssig und müssen gelöscht werden.

1. Öffnen Sie dazu auf dem Zielserver die *DNS-mmc*. Aus dem Kontextmenü des Zielservers wählen Sie den Eintrag EIGENSCHAFTEN.
2. Auf der Registerkarte WEITERLEITUNGEN klicken Sie unter DNS-DOMÄNE den Namen der Quelldomäne an und klicken dann auf ENTFERNEN.

Zurücksetzen von Berechtigungen

Diesen Schritt müssen Sie nur ausführen, wenn Sie unter Schritt 4 – Durchführung der Migration – auf dem Quellserver erweiterte Berechtigungen für den Prä-Windows 2000-kompatiblen Zugriff konfiguriert haben. Verwenden Sie Mitgliedserver unter Windows Server NT 4.0, so überspringen Sie diesen Schritt, damit für diese Server der Zugriff auf die neue Domäne gewährleistet ist.

1. Um die Berechtigungen zurückzusetzen, öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgende Befehle ein:

   ```
   Net localgroup "pre-windows 2000 compatible access" everyone /delete ↵
   Net localgroup "pre-windows 2000 compatible access" "anonymus logon" /
   delete ↵
   ```

2. Starten Sie danach den Zielserver neu, und melden Sie sich unter dem Administratorkonto an.

Deinstallation des ADMT

Nach der Migration sämtlicher Konten sollten Sie ADMT vom Zielserver wieder deinstallieren. Erledigen Sie dies wie gewohnt über SYSTEMSTEUERUNG/SOFTWARE/PROGRAMME HINZUFÜGEN ODER ENTFERNEN.

Festlegen von Kennwortrichtlinien

Sofern Sie nicht die alten Benutzerpasswörter ebenfalls migriert haben, sollten Sie jetzt eine Kennwortrichtlinie bestimmen, die alle Benutzer auffordert, bei der ersten Anmeldung ein neues Kennwort festzulegen.

1. Öffnen Sie dazu in der SERVERVERWALTUNG den Eintrag BENUTZER.
2. Klicken Sie in der rechten Fensterhälfte auf FESTLEGEN VON KENNWORT-RICHTLINIEN. Nach Möglichkeit sollten Sie alle drei angebotenen Optionen auswählen.
3. Klicken Sie dann auf KENNWORT-RICHTLINIEN KONFIGURIEREN, und klicken Sie dann auf SOFORT.

Sofern Sie Zugriff auf den Server über das Internet zulassen, sollten Sie in jedem Fall die Komplexität der Kennwörter aktivieren. Die Anforderungen für ein komplexeres Kennwort treten dabei erst nach drei Tagen in Kraft, so dass genügend Zeit verbleibt, um in Ruhe weitere Benutzerkonten einrichten zu können.

4. Zusätzlich sollten Sie die im Zuge der Kontenmigration angelegte Passwortdatei löschen. Dabei handelt es sich um die Datei \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT.

Ferner ist zu überlegen, ob Sie den Benutzern die Möglichkeit geben möchten, ihr Kennwort ändern zu können oder nicht. Für ein Zulassen des Änderns spricht eine höhere Sicherheit, dagegen möglicherweise, dass der Administrator ständig Kennwörter zurücksetzen muss, da die Benutzer diese vergessen. Im Einzelfall – auch abhängig von Ihren Benutzern – müssen Sie entscheiden, für welche Option Sie sich entscheiden.

Um die Änderung von Kennwörtern zu aktivieren oder deaktivieren, öffnen Sie in der SERVERVERWALTUNG den Eintrag BENUTZER. Doppelklicken Sie auf das gewünschte Konto. Auf der Registerkarte KONTO können Sie die Checkbox BENUTZER KÖNNEN IHR KENNWORT NICHT ÄNDERN aktivieren oder deaktivieren.

Verbindung des Zielservers mit dem Internet

Verbinden Sie abschließend das Netzwerkgerät des Zielservers für die Internetverbindung wieder mit dem entsprechenden Kabel. Um die Verbindung ins Internet zu testen, öffnen Sie von einem beliebigen Client aus eine Webseite. Verschicken Sie auch eine Test-E-Mail an ein Mailkonto im Internet. Haben Sie auch die Faxdienste konfiguriert, so sollten Sie auch ein Testfax senden.

3.3 Migration des Small Business Server 4.5 und Windows Server NT 4.0

Wie bereits erwähnt, können Sie eine Aktualisierung auf SBS 2003 vom SBS 4.5 oder Windows Server NT 4.0 nur durch eine Migration erreichen. Eine Update-Funktion dieser Betriebssysteme auf SBS 2003 ist nicht gegeben. In vielen Schritten ähnelt oder gleicht diese Migration der von Windows Server 2000 bzw. SBS 2000. Um jedoch den Lesefluss innerhalb dieses Kapitels nicht zu unterbrechen und ein ständiges Umblättern in die entsprechenden Kapitel der SBS 2000-Migration zu verhindern, wird im Folgenden die komplette Migration eines SBS 4.5 oder Windows Server NT 4.0 beschrieben.

Die hier aufgeführten Schritte beziehen sich nicht auf den SBS in der Version 4.0. Sollten Sie noch diese Version verwenden, müssen Sie den Server neu installieren und eine Migration komplett manuell durchführen.

Dieses Kapitel beschreibt detailliert die verschiedenen Arbeitsschritte der Migration mit einem SBS 4.5 oder Windows NT 4.0 Server als Quellserver.

3.3.1 Schritt 1 – Vorbereiten der Migration

Im Zuge der Migrationsvorbereitung sammeln Sie zunächst die folgenden Informationen verschiedener Bereiche:

Serverbezogene Informationen

- Name des Quell- und Zielservers. Diese beiden Namen müssen unterschiedlich sein. Um den Computernamen zu ermitteln, öffnen Sie die SYSTEMSTEUERUNG und doppelklicken dann auf NETZWERK. Auf der Registerkarte IDENTIFIKATION finden Sie den Computernamen.
- Vollständiger NetBIOS-Domänenname: Auch dieser Name muss sich auf dem Quell- und Zielserver unterscheiden. Standardmäßig können Sie die während der Installation vorgeschlagenen Werte für die interne DNS-Domäne übernehmen. Um den Net-

BIOS-Namen zu ermitteln, öffnen Sie die SYSTEMSTEUERUNG und doppelklicken dann auf NETZWERK. Auf der Registerkarte IDENTIFIKATION finden Sie den DNS- und NetBIOS-Domänennamen. Der NetBIOS-Domänenname wird unter Domäne angezeigt. Ein vollständiger DNS-Domänenname ist unter Windows NT noch nicht verfügbar.

- Ermitteln Sie die IP-Adresse des Quellservers, und bestimmen Sie eine noch nicht vergebene Adresse für den Zielserver. Um die Adresse des Quellservers zu bestimmen, geben Sie unter AUSFÜHREN `cmd` ein und dann den Befehl `ipconfig /all`. Die IP-Adresse für den Zielserver muss sich selbstverständlich in demselben Adressbereich befinden wie die des Quellservers. Verwenden Sie einen Router als DHCP-Server, muss die Adresse im Bereich der vom Router vergebenen Adressen liegen. Fungiert der Quellserver als DHCP-Server, so ermitteln Sie in dessen Bereichsoptionen gültige IP-Adressen. Öffnen Sie dazu STARTMENÜ/PROGRAMME/VERWALTUNG (ALLGEMEIN)/DHCP-MANAGER. Doppelklicken Sie hier den lokalen Server und danach BEREICH. Hier finden Sie alle aktuell verwendeten IP-Adressen.
- Administratorkonto: Haben Sie auf dem Quellserver das Administratorkonto umbenannt, so müssen Sie dieses wieder auf den ursprünglichen Namen Administrator zurücksetzen. Eine Umbenennung des Kontos kann nach Abschluss der Migration auf dem Zielserver wieder erfolgen. Außerdem müssen Sie sicherstellen, dass das Administratorpasswort auf dem Quell- und Zielsystem identisch ist. Es muss dabei ein Passwort gesetzt sein, anderenfalls kann die Migration nicht durchgeführt werden.

Informationen über gemeinsam genutzte Ordner, Applikationen und Einstellungen

- Gemeinsam genutzte Ordner der Benutzer (Users Shared Folder): Notieren Sie sich den Namen des Benutzerordners. Standardmäßig lautet er unter SBS 4.5 wie auch unter SBS 2003 USERS.
- Ordner für Client-Applikationen (ClientApps Folder): Befinden sich hier Applikationen, die auch nach der Migration verwendet werden sollen, so kopieren Sie den Inhalt in das Verzeichnis auf dem Zielserver. Standardmäßig heißt das Verzeichnis für Client-Applikationen unter SBS 4.5 und SBS 2003 CLIENTAPPS.

Die Applikation *Modem Sharing Client* ist nach der Migration jedoch nicht mehr verfügbar, da SBS 2003 diese Funktion nicht mehr unterstützt.

- Gemeinsam genutzte Ordner der Firma (Company Shared Folder): Unter SBS 4.5 lautet der Name des Ordners COMPANY. Unter SBS 2003 hingegen steht eine eigene Firmenwebsite über die SharePoint Services bereit. Der Speicherort ist hier *http://companyweb*.
- Weitere gemeinsam genutzte Ordner: Die Inhalte der gemeinsam genutzten Ordner DRUCKER und GEPLANTE TASKS können nicht migriert werden:. Migrieren Sie auch nicht den Ordner NETLOGON, sofern sie keine angepassten Login-Skripte verwenden. Diese Ordner dürfen weder bei einer Migration von SBS 4.5 noch von Windows Server NT 4.0 migriert werden. Bei einer Migration von SBS 4.5 aus dürfen zusätzlich

folgende Ordner nicht migriert werden, da der SBS 2003 aktualisierte Versionen beinhaltet: MSPCINT sowie die gemeinsam genutzten Client-Ordner. Die einzelnen Benutzerordner müssen nicht separat migriert werden, da ihre Inhalte im Zuge der Migration des gemeinsam genutzten Ordners Users automatisch folgen.

- Sofern Exchange 5.5 installiert ist, dürfen Sie nicht die gemeinsam genutzten Ordner ADD-INS, ADDRESS, RESSOURCEN und TRACKING.LOG migrieren.
- Sind noch weitere gemeinsam genutzte Ordner vorhanden, so prüfen Sie deren Inhalte und notieren sich die Namen der Freigaben, um diese auf dem Zielsystem neu einzurichten. Um einen Überblick über alle Freigaben des Quellservers zu erhalten, geben Sie unter AUSFÜHREN Folgendes ein: \\Quellserver-Name.
- Als Nächstes notieren Sie sich den Namen und Installationspfad sämtlicher Applikationen, die Sie auch nach der Migration wieder benutzen möchten.
- Haben Sie unter Exchange 5.5 Verteilergruppen eingerichtet, so notieren Sie sich deren Namen. Beim Verschieben der Gruppen auf den Zielserver müssen Sie diese in die Organisationseinheit (OU) Verteilergruppen verschieben. Befinden sich in den Verteilergruppen vordefinierte Gruppen (wie z.B. Administratoren) als Mitglieder, so müssen Sie diese Gruppenmitgliedschaft ebenfalls vermerken, da die Mitgliedschaften der vordefinierten Gruppen nicht migriert werden können. Des Weiteren müssen Sie unter Exchange 5.5 benutzerdefinierte Berechtigungen für die öffentlichen Ordner sowie benutzerdefinierte Empfänger aufschreiben und nach Abschluss der Migration neu konfigurieren.
- Prüfen Sie dann, ob Sie sämtliche benutzerdefinierten Einstellungen der folgenden Bereiche gesichert haben: DNS, DHCP-Bereichsoptionen, Routing und RAS, Gruppenrichtlinien, Webseiten auf dem IIS 4.0 und Exchange 5.5. Diese Einstellungen werden auf dem Zielserver nach Abschluss der Migration neu konfiguriert. Die öffentlichen Ordner sowie das Postfach des Administratorkontos werden in eine .pst-Datei exportiert. Sind für das Administrator-Postfach bestimmte Regeln festgelegt, so müssen Sie diese ebenfalls exportieren. Eine Migration dieser Einstellungen mit dem Exchange Server-Migrationsassistenten ist nicht möglich.

Haben Sie keine benutzerdefinierten Einstellungen auf dem Quellsystem zugelassen, sondern die Standardeinstellungen beibehalten, so müssen Sie für diese Bereiche die Konfiguration nicht notieren, da die Standardeinstellungen des SBS 2003 übernommen werden können.

Löschen nicht mehr benötigter Dateien und E-Mails

In jedem Fall sollten Sie vor Beginn der Migration sämtliche nicht mehr benötigten Dateien und E-Mails löschen. Fordern Sie hierzu sämtliche Benutzer auf, unter Outlook ihre Mails aus den Ordnern GELÖSCHTE OBJEKTE sowie GESENDETE OBJEKTE zu löschen. Dasselbe gilt auch für nicht mehr benötigte Dateien in den einzelnen Benutzerverzeichnissen. Weiterhin sollten Sie auch sämtliche gemeinsam genutzte Verzeichnisse auf Dateileichen hin durchsuchen.

Ist ein Postfach eines Benutzers auch nach dem Löschen sämtlicher überflüssiger E-Mails noch größer als 200 MB, müssen Sie auf dem Zielserver unbedingt die Quota-Einstellungen ändern. Standardmäßig liegt der Schwellenwert für die Postfachgröße bei 200 MB. Ist diese Größe überschritten, können keine E-Mails mehr gesendet und empfangen werden. Eine Warnung wird standardmäßig bei 175 MB ausgegeben.

Ein Limit gilt auch für die Benutzerordner. Der Grenzwert für Benutzerordner liegt unter SBS 2003 standardmäßig bei 1 GB. Ist der Ordner eines Benutzers größer als 1 GB, so müssen Sie die Quota-Einstellungen für alle Benutzer anpassen. Weitere Hinweise dazu finden Sie in der Hilfe des SBS 2003.

Um die Postfachgröße der einzelnen Benutzer zu ermitteln, führen Sie unter SBS 4.5 die folgenden Schritte aus:

1. Öffnen Sie START/PROGRAMME/MICROSOFT EXCHANGE/MICROSOFT EXCHANGE ADMINISTRATOR.
2. Doppelklicken Sie dort den EXCHANGE STANDORT und danach unter SERVERS Ihren Exchange-Server. Doppelklicken Sie hier PRIVATER INFORMATIONSSPEICHER und dann POSTFACHRESSOURCEN.
3. In der Spalte GESAMT KB finden Sie die Postfachgröße für jeden Benutzer.

Werden unter Outlook von den Benutzern Regeln verwendet, so müssen Sie diese sichern, da bei der Migration der Postfächer keine Outlook-Regeln auf den Zielserver migriert werden.

Kompatibilität von Hard- und Software

Haben Sie die Absicht, Hardware, z.B. ein eingebautes Faxmodem, oder Software des Quellsystems auch auf dem Zielserver zu verwenden, so müssen Sie sicherstellen, dass eine Kompatibilität mit SBS 2003 gegeben ist. Benutzen Sie hierzu die Windows Server-Katalogseite unter *http://www.microsoft.com/windows/catalog/server/*.

Einspielen aktueller Service Packs

Zusätzlich sollten Sie sicherstellen, dass auf dem Quellsystem die aktuellen Service Packs installiert sind. Für die reibungslose Migration müssen mindestens folgende Service Packs installiert sein:

Exchange Server 5.5: Service Pack 4 Um zu überprüfen, welches Service Pack installiert ist, öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT EXCHANGE/MICROSOFT EXCHANGE ADMINISTRATOR. Im Menü HILFE klicken Sie auf den Eintrag ÜBER MICROSOFT EXCHANGE SERVER. Hier wird die Service Pack-Version angezeigt. Das Service Pack können Sie unter *http://www.microsoft.com/exchange/downloads/55/sp4dl_de.asp* downloaden.

Haben Sie das Exchange SA-Kenwort geändert, so dass dieses nicht mehr mit dem des vordefinierten Administratorkontos übereinstimmt, erhalten Sie bei der Installation des Service Packs eine Fehlermeldung, dass keine Bindung zwischen den Kontennamen und der Security ID (SID) hergestellt werden konnte. In diesem Fall müssen Sie das Exchange SA-Kennwort wieder ändern. Weitere Hinweise finden Sie in Artikel 285297 in der Microsoft Knowledge Base.

SQL Server 7.0: Service Pack 4 Um zu überprüfen, welches Service Pack installiert ist, öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT SQL SERVER 7.0/ENTERPRISE MANAGER. Doppelklicken Sie die SQL SERVERGRUPPE und wählen aus dem Kontextmenü des Servernamens den Eintrag EIGENSCHAFTEN. Die Versionsnummer muss 7.00.1063 lauten. Diese Versionsnummer entspricht einem installierten Service Pack 4. Das Service Pack können Sie unter *http://www.microsoft.com/sql/downloads/sp4GER.asp* downloaden.

Windows Server NT 4.0: Service Pack 6a Um zu überprüfen, welches Service Pack installiert ist, geben Sie unter AUSFÜHREN den Befehl `Winver` ein. Das Service Pack 6a können Sie unter *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=e396d059-e402-46ef-b095-a74399e25737* downloaden.

Windows Server NT 4.0: Internet Explorer High Encryption Pack Weiterhin muss das High Encryption Pack installiert sein. Um dies zu überprüfen, doppelklicken Sie den Internet Explorer auf dem Desktop. Öffnen Sie im Menü HILFE den Eintrag ÜBER INTERNET EXPLORER. Unter VERSCHLÜSSELUNGSSTÄRKE sollte der Wert 128 Bit angezeigt werden. Wird die Verschlüsselungsstärke dort nicht angezeigt, so navigieren Sie im Windows Explorer zur Datei \SYSTEM32\SCHANNEL.DLL und öffnen deren EIGENSCHAFTEN. Auf der Registerkarte VERSION sollten Sie unter BESCHREIBUNG den Eintrag TLS/SSL SECURITY PROVIDER (US AND CANADA) sehen.

Sie können das High Encryption Pack für den Internet Explorer unter *http://www.microsoft.com/downloads/details.aspx?FamilyID=bbcaae86-f80d-4d0c-8fa2-78a8868652e0&displaylang=de* downloaden.

Sicherung des Quellservers

Eine Sicherung des Quellservers sollte durchgeführt werden, nachdem sämtliche Benutzer ihre Arbeit beendet haben. Idealerweise geschieht dies also abends oder an einem Wochenende.

1. Vor Beginn des Backups sollten Sie sämtliche Laufwerke auf Viren hin scannen. Legen Sie auch eine Notfalldiskette für den Quellserver an oder aktualisieren eine bereits vorhandene.
2. Führen Sie dann ein vollständiges Backup des Quellservers durch.
3. Um sicherzustellen, dass das Backup ordnungsgemäß durchgeführt wurde, sollten Sie beliebige Dateien des Backups an einem anderen Speicherort wiederherstellen und prüfen, ob die Originaldatei und die der Sicherung identisch sind.

Benachrichtigung über die anstehende Migration

Eine Benachrichtigung der Benutzer über die anstehende Migration ist nur in dem Moment relevant, wenn noch Benutzer an der Domäne angemeldet sind. Führen Sie die Migration hingegen zu einem Zeitpunkt aus, zu dem keine Benutzer mehr arbeiten, so ist dieser Punkt unerheblich. Anderenfalls können Sie die Benutzer über den *Net send*-Befehl erreichen. Voraussetzung dafür ist, dass auf dem Server und den Clients der Nachrichtendienst ausgeführt wird. Verwenden Sie beispielsweise folgenden Befehl an der Eingabeaufforderung:

```
Net send * Bitte melden Sie sich innerhalb der nächsten 5 Minuten von der
Domäne ab. Es sind dann keine Netzwerk- und Internetverbindungen mehr
verfügbar. ↵
```

Dabei bedeutet das Symbol *, dass die Nachricht an alle Mitglieder der Domäne geschickt wird.

3.3.2 Schritt 2 – Vorbereiten des Servers für die Installation

Dieses Kapitel beschreibt sämtliche Schritte, die Sie vor der Installation des SBS 2003 auf dem Quell- und Zielsystem durchführen müssen.

DHCP-Konfiguration

Vor Beginn der Installation des SBS 2003 müssen Sie auf dem Quellserver den DHCP-Serverdienst beenden, sofern dieser dort ausgeführt wird. Sobald der Quell- und Zielserver miteinander verbunden werden, darf nur der auf dem Zielserver konfigurierte DHCP-Serverdienst aktiv sein.

1. Um den Dienst auf dem Quellserver zu beenden, öffnen Sie unter STARTMENÜ/EINSTELLUNGEN/SYSTEMSTEUERUNG und doppelklicken dort DIENSTE.
2. Markieren Sie dort den Eintrag MICROSOFT DHCP-SERVER und klicken auf BEENDEN. Setzen Sie danach den STARTTYP auf DEAKTIVIERT.

Sofern Sie einen Router benutzen, der als DHCP-Server dient, müssen Sie den eben beschriebenen Vorgang nicht durchführen. Dieser Router muss bereits während der Installation des SBS 2003 mit dem Zielserver verbunden sein, damit die DHCP-Einstellungen korrekt konfiguriert werden können. Sie können dabei entscheiden, ob Sie den Router oder den SBS 2003 als DHCP-Server verwenden möchten.

Netzwerk- und Internetverbindung

Weiterhin ist es empfohlen, dass Sie aus dem Netzwerkgerät, das für die Internetverbindung zuständig ist, das Kabel entfernen. Dabei ist es unerheblich, ob es sich um eine Netzwerkkarte bei einem Breitbandzugang oder um ein Modem bei einer Wählverbindung handelt.

Als Nächstes verbinden Sie den Netzwerkadapter des Zielservers, den Sie für interne Netzwerkverbindungen benutzen möchten, mit dem Netzwerk des Quellservers.

Faxmodem

Soll aus dem Quellserver ein Faxmodem ausgebaut und im Zielserver eingebaut werden, so müssen Sie dieses ebenfalls vor Beginn der Installation austauschen. Stellen Sie zudem sicher, dass die Hardware mit dem SBS 2003 kompatibel ist.

Dateisystem

Während der Installation des Zielservers müssen Sie das Dateisystem bestimmen. Wählen Sie hier in jedem Fall NTFS und nicht FAT oder FAT32.

Administratorkennwort

Bedenken Sie bei einer Migration, dass das Administratorkennwort auf dem Zielserver dem Kennwort des Quellservers entsprechen muss und erst nach Abschluss der Migration neu festgelegt werden kann.

Computername

Der zu wählende Computername für den Zielserver darf im Netzwerk noch nicht vorhanden sein. Gültige Zeichen für einen Computernamen sind A–Z, 0–9 sowie der Bindestrich (-). Der Name darf maximal 15 Zeichen umfassen.

Netzwerkinformationen

Bei der Eingabe der internen Domäneninformationen müssen Sie sicherstellen, dass der NetBIOS-Domänenname nicht gleich dem NetBIOS-Domänennamen des Quellservers ist. Ansonsten wird die Migration fehlschlagen.

Die IP-Adressen des Quell- und Zielservers müssen sich in demselben Adressbereich befinden. Haben Sie versehentlich eine falsche IP-Adresse für den Zielserver angegeben, so können Sie diese nur über das Tool *Change Server Address* ändern. Öffnen Sie dazu in der Serververwaltung des SBS 2003 den Link INTERNET UND E-MAIL und klicken auf CHANGE SERVER IP ADDRESS. Nur so ist sichergestellt, dass die Umstellung der IP-Adresse für alle Dienste auf dem Zielserver ordnungsgemäß durchgeführt werden kann.

Sofern Sie über die Premium-Edition des SBS 2003 verfügen, können Sie nach Abarbeitung der Aufgabenliste den SQL-Server und den ISA-Server installieren. Allerdings sollten Sie jetzt noch nicht die Firewall-Clients verteilen. Dieser Arbeitsgang sollte erst erfolgen, nachdem die Clients wie in Schritt 6 beschrieben ebenfalls migriert worden sind.

Bevor der Zielserver das erste Mal eine Verbindung zum Internet herstellt, sollten Sie eine Antiviren-Software installieren und konfigurieren.

Durchführen der Netzwerkaufgaben

Nachdem Sie die Installation auf dem Zielserver abgeschlossen haben, führen Sie auf diesem, wie im Kapitel der Neuinstallation beschrieben, die Netzwerkaufgaben durch. Dazu zählen die Konfiguration der Internetverbindung, von Sicherheitseinstellungen und Remote Access, die Aktivierung des Servers sowie das Hinzufügen zusätzlicher Clientlizenzen. Hierzu müssen Sie das Netzwerkgerät für die Internetverbindung vorüberge-

hend verkabeln. Nach Abschluss der Netzwerkaufgaben sollten Sie die Internetverbindung wieder deaktivieren, um ein ungestörtes Migrieren der Daten zu gewährleisten. Hierzu sollte auch der Echtzeit-Virenschutz vorübergehend wieder ausgeschaltet werden.

3.3.3 Schritt 3 – Vorbereiten der Clients

Im nächsten Schritt müssen die Clients der folgenden Betriebssysteme für die Migration auf SBS 2003 vorbereitet werden:

- Windows NT 4.0 Workstation
- Windows 2000 Professional
- Windows XP Professional
- Windows Server 2000
- Windows Server 2003
- Mitgliedserver ab Windows Server NT 4.0

Alle diese Client Computer werden mit Hilfe des ADMT migriert. Bei Windows NT 4.0 Clients (Workstation und Server) muss unbedingt das Service Pack 6a installiert sein. Um zu prüfen, ob dieses installiert ist, geben Sie unter AUSFÜHREN den Befehl Winver ein. In der Dialogbox ÜBER WINDOWS NT wird das installierte Service Pack angezeigt. Das Service Pack können Sie unter *http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp* downloaden.

Verwenden Sie hingegen Clients mit den Betriebssystemen Windows 95, 98 oder ME, so müssen Sie diese manuell migrieren. Dieses Verfahren wird unter Schritt 6 dieses Kapitels beschrieben. Sollen bei der Migration eines Windows Server 2000 als zusätzliche Domänencontroller eingerichtete Server migriert werden, so müssen Sie von diesen zunächst das Active Directory deinstallieren. Geben Sie dazu unter AUSFÜHREN den Befehl DCPROMO ein. Danach kann das Computerkonto zur Zieldomäne migriert und der Computer als zweiter Server hinzugefügt werden. Bedenken Sie, dass Sie für jeden Mitgliedserver innerhalb der SBS 2003-Domäne eine SBS 2003-CAL benötigen.

Die Migration eines Backup-Domänencontrollers (BDC) unter Windows Server NT 4.0 ist nicht möglich, da der SBS 2003 den Active Directory-Funktionsmodus Windows 2000 nativ verwendet. Dieser Modus lässt keine NT-basierten BDCs zu. Um einen BDC weiter zu benutzen, müssen Sie diesen neu installieren und danach als Mitgliedserver zur SBS 2003-Domäne hinzufügen.

Im Detail führen Sie jetzt die folgenden Aufgaben aus:

- Sofern die Benutzer nicht ihre Outlook Postfach-Regeln exportiert haben, müssen Sie dieses jetzt durchführen.
- Stellen Sie sicher, dass auf dem Quellserver die Gruppe der Domänenadministratoren zur vordefinierten Gruppe der Administratoren gehört. Sollten Sie die Gruppe auf einem beliebigen Client aus der vordefinierten Gruppe gelöscht haben, so müssen Sie diese wieder hinzufügen.

- Sofern auf den Clientcomputern noch Firewalls, z.B. die Internetverbindungs-Firewall unter Windows XP, aktiv sind, müssen diese nun ebenfalls deaktiviert werden.
- Bei einem Update des SBS 4.5 müssen Sie auch die Applikationen *Modem Sharing Client*, *Microsoft Fax Server Client* sowie *WinSock Proxy Client* entfernen. Letzterer wird bisweilen auch als *Microsoft Proxy Client* bezeichnet.
- Um die korrekte DHCP-Konfiguration zu gewährleisten, müssen Sie für jeden Client die IP-Adresse freigeben und danach wieder erneuern. Damit ist sichergestellt, dass sämtliche Clients ihre IP-Adresse nun vom neuen DHCP-Server auf dem SBS 2003 beziehen.
- Stellen Sie sicher, dass auf sämtlichen Windows NT 4.0 Workstations und Mitgliedservern das Service Pack 6a installiert ist.
- Als Nächstes löschen Sie die Desktop-Verknüpfungen der gemeinsam genutzten Benutzerordner und des Firmenordners. Weiterhin müssen Sie sämtliche Verknüpfungen löschen oder aktualisieren, die noch auf den Quellserver verweisen. Dasselbe gilt auch für Einträge im Ordner Internet-Favoriten, die auf den Quellserver verweisen, so z.B. die Microsoft Small Business Server Webseite.
- Auch Netzwerkdrucker oder Faxdrucker, die auf den Quellserver verweisen, müssen gelöscht werden. Die Drucker werden stattdessen auf dem Zielserver neu konfiguriert (siehe Schritt 5) und stehen dann wieder für die Clients zur Verfügung.
- Abschließend sollten Sie auf jedem Computer eine Virenprüfung durchführen und danach den Echtzeit-Virenschutz deaktivieren. Melden Sie sich zum Schluss vom jeweiligen Client ab.

3.3.4 Schritt 4 – Durchführung der Migration

Zur Durchführung der Migration wird das Programm ADMT (Active Directory Migration Tool) auf dem Zielserver installiert, um damit die bestehenden Computer-, Benutzer- und Gruppenkonten zu migrieren. Anhand der unter Schritt 1 oder 2 gesammelten Clientinformationen müssen Sie entscheiden, ob die Kontingente für Exchange angepasst werden müssen oder nicht. Zusätzlich müssen gemeinsam genutzte Ordner und Applikationsdaten auf den Zielserver verschoben werden. Beim Einsatz des SQL-Servers müssen auch die SQL-Datenbanken auf den Zielserver verschoben werden. Spätestens jetzt sollten Sie ein Backup des Quellservers durchführen, sofern dies nicht bereits geschehen ist.

Installation des ADMT

Zunächst installieren Sie ADMT auf dem Zielserver. Sie finden das Programm auf der CD 1 des SBS 2003 im Verzeichnis \I386\ADMT\ADMIGRATION.MSI. Folgen Sie zur Installation den Hinweisen des Installationsassistenten.

ADMT-Konfiguration auf dem Zielserver

Sofern sich in Ihrer Domäne Clients mit dem Betriebssystem Windows NT 4.0 Workstation oder Mitgliedserver unter Windows Server NT 4.0 befinden, müssen Sie zunächst die folgenden Schritte ausführen:

1. Geben Sie auf dem Zielserver unter AUSFÜHREN den Befehl cmd ein. An der Eingabeaufforderung geben Sie die beiden folgenden Zeilen ein:

```
Net local group "Pre-Windows 2000 Compatible Access" everyone /add ↵
Net local group "Pre-Windows 2000 Compatible Access" "anonymus logon" /
add ↵
```

Beachten Sie, dass Sie in den beiden Befehlszeilen unbedingt die Anführungszeichen angeben.

2. Führen Sie danach einen Neustart des Zielservers durch.

Migration von Benutzerkonten

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein:

```
Runas /netonly /user:NameQuelldomäne\Administrator "mmc\"%ProgramFiles%\
Active Directory Migration Tool\Migrator.msc\"" ↵
```

Ersetzen Sie dabei NameQuelldomäne durch den entsprechenden NetBIOS-Domänennamen.

Wenn Sie ADMT schließen, dürfen Sie es nur über den eben genannten Befehl öffnen und nicht über den Eintrag im Startmenü.

2. Geben Sie nach Aufforderung das Kennwort für das Administratorkonto an. Danach erscheint die GUI des ADMT.
3. Im Menü ACTION klicken Sie auf USER ACCOUNT MIGRATION WIZARD. Konfigurieren Sie dort den Wizard mit den folgenden Informationen:

Bei der Migration werden Benutzerkonten, deren Name mehr als 20 Zeichen umfasst, automatisch auf 20 Zeichen eingekürzt und somit möglicherweise auf dem Zielserver nur noch verstümmelt dargestellt.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Test or Make Changes	Klicken Sie hier auf TEST THE MIGRATION SETTINGS AND MIGRATE LATER?. So können Sie anhand der Log-Dateien mögliche Fehler erkennen und beheben. Zum endgültigen Migrationslauf klicken Sie hier MIGRATE NOW?.
Domain Selection	Setzen Sie hier die Namen der Quell- und Zieldomäne. Erhalten Sie nach dem Klick auf NEXT die Fehlermeldung Access is denied (Error=5), beenden Sie den ADMT-Wizard und überprüfen, ob die Kennwörter für das Administratorkonto auf dem Quell- und Zielsystem identisch sind und das Passwort beim Neustart des ADMT an der Kommandozeile korrekt eingegeben wird.
User Selection	Klicken Sie hier auf ADD und dann ADVANCED. Der Eintrag SELECT THIS OBJECT TYPE wird automatisch für die Suche nach Benutzerkonten gesetzt. Klicken Sie dann auf FIND NOW. Sie sehen eine Liste sämtlicher Benutzerkonten. Wählen Sie hier sämtliche Benutzerkonten aus, die Sie migrieren möchten, und klicken dann auf OK. Beachten Sie, dass die folgenden Benutzerkonten nicht migriert werden können: Administrator, Gast, IUSR_ Servername sowie IWAM_Servername. Bei einer Migration des SQL Server 7.0 darf nicht das Konto SQLAgentCmdExec migriert werden. Bei weiteren Applikationen, die ein eigenes Benutzerkonto erfordern, wenden Sie sich an die Dokumentation oder den Hersteller der Applikation, ob eine Migration des Kontos möglich ist.
Organizational Unit Selection	Als Ziel-OU (Target OU) navigieren Sie zu MYBUSINESS\USERS\SBSUSERS.
Password Options	Klicken Sie hier SAME AS USER NAME. Damit wird das Passwort automatisch auf die 14 ersten Zeichen des Benutzernamens gesetzt. Diese Einträge werden standardmäßig in die folgende Datei gespeichert: \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT. Diese temporären Passwörter können nach Abschluss der Migration wieder umgesetzt werden. Möchten Sie hingegen die ursprünglichen Passwörter migrieren, so klicken Sie MIGRATE PASSWORDS. Eine Anleitung für die entsprechende Konfiguration zur Passwortmigration finden im Microsoft Knowledge Base-Artikel KB 325851.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Account Transition Options	Klicken Sie hier auf TARGET SAME AS SOURCE. Aktivieren Sie dann die Checkbox MIGRATE USER SIDS TO TARGET DOMAIN. Klicken Sie dann auf NEXT und danach auf YES. Danach müssen Sie den Quellserver neu starten und sich mit dem Administratorkonto anmelden. Erst dann können Sie auf dem Zielserver auf OK klicken, um fortzufahren.
User Account	Unter USER NAME geben Sie das vordefinierte Administratorkonto an und geben das Passwort ein. Stellen Sie sicher, dass unter DOMAIN der Name der Quelldomäne gesetzt ist.
User Options	Aktivieren Sie hier die Checkbox TRANSLATE ROAMING PROFILES sowie die Checkbox UPDATE USER RIGHTS. Stellen Sie sicher, dass auch die Checkboxen FIX USERS' GROUP MEMBERSHIPS sowie DO NOT RENAME ACCOUNTS markiert sind.
Naming Conflicts	Hier sollte die Option IGNORE CONFLICTING ACCOUNTS AND DON'T MIGRATE ausgewählt sein.
Completing the User Account Migration Wizard	Sobald Sie zum Abschluss des Wizards auf FINISH geklickt haben, erhalten Sie ein Statusfenster über die Migration. Die Migration der Benutzerkonten ist abgeschlossen, wenn als Status COMPLETED angezeigt wird. Um zu sehen, ob Fehler aufgetreten sind, klicken Sie auf VIEW LOG. Die Log-Datei ist sowohl bei der Simulation der Migration als auch bei der realen Migration verfügbar.

Tabelle 3.7: Der ADMT-Migrationsassistent für Benutzerkonten

Migration von Gruppenkonten

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein, sofern ADMT nicht noch geöffnet ist:

```
Runas /netonly /user:NameQuelldomäne\Administrator "mmc\"%ProgramFiles%\
Active Directory Migration Tool\Migrator.msc\"" ↵
```

Ersetzen Sie dabei NameQuelldomäne durch den entsprechenden NetBIOS-Domänennamen.

Wenn Sie ADMT schließen, dürfen Sie es nur über den eben genannten Befehl öffnen und nicht über den Eintrag im Startmenü.

2. Geben Sie nach Aufforderung das Kennwort für das Administratorkonto an. Danach erscheint die GUI des ADMT.

3. Im Menü ACTION klicken Sie auf GROUP ACCOUNT MIGRATION WIZARD. Konfigurieren Sie dort den Wizard mit den folgenden Informationen:

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Test or Make Changes	Klicken Sie hier auf TEST THE MIGRATION SETTINGS AND MIGRATE LATER?. So können Sie anhand der Logdateien mögliche Fehler erkennen und beheben. Zum endgültigen Migrationslauf klicken Sie hier MIGRATE NOW?.
Domain Selection	Unter SOURCE DOMAIN muss der Domänenname der Quelldomäne eingetragen sein, z.B. SBS45, unter TARGET DOMAIN der Name der Zieldomäne, z.B. sbs2003.local.
Group Selection	Klicken Sie hier auf ADD und danach auf ADVANCED. Der Eintrag SELECT THIS OBJECT TYPE wird automatisch für die Suche nach Gruppenkonten gesetzt. Klicken Sie dann auf FIND NOW. Sie sehen eine Liste sämtlicher Gruppenkonten. Wählen Sie hier sämtliche Gruppenkonten aus, die Sie migrieren möchten, und klicken dann auf OK. Beachten Sie, dass die folgenden vordefinierten Gruppenkonten nicht migriert werden können: Administratoren, Benutzer, Domänenadministratoren, Domänenbenutzer, Domänengäste, Druckoperatoren, Gäste, Kontenoperatoren, Replicator, Server-Operatoren und Sicherungsoperatoren. Weiterhin dürfen Sie auch nicht die Gruppen Domänenname$$$ sowie MTS Impersonators migrieren.
Organizational Unit Selection	Für die Gruppen wählen Sie MYBUSINESS\SECURITYGROUPS als Ziel-OU.
Group Options	Wählen Sie hier die Einträge UPDATE USER RIGHTS, FIX MEMBERSHIP OF GROUPS, MIGRATE GROUP SIDS TO TARGET DOMAIN sowie DO NOT RENAME ACCOUNTS.
User Account	Unter USER NAME geben Sie das vordefinierte Administratorkonto an und geben das Passwort ein. Stellen Sie sicher, dass unter Domain der Name der Quelldomäne gesetzt ist.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Naming Conflicts	Hier sollte die Option IGNORE CONFLICTING ACCOUNTS AND DON'T MIGRATE ausgewählt sein.
Completing the Group Account Migration Wizard	Sobald Sie zum Abschluss des Wizards auf FINISH geklickt haben, erhalten Sie ein Statusfenster über die Migration. Die Migration der Gruppenkonten ist abgeschlossen, wenn als Status COMPLETED angezeigt wird. Um zu sehen, ob Fehler aufgetreten sind, klicken Sie auf VIEW LOG. Die Log-Datei ist sowohl bei der Simulation der Migration als auch bei der realen Migration verfügbar.

Tabelle 3.8: Tabelle 3.8: Der ADMT-Migrationsassistent für Gruppenkonten

Migration von Computerkonten

Eine Migration von Computerkonten kann nur für Computer mit den Betriebssystemen Windows NT 4.0 Workstation und Server, Windows 2000 Professional und Server sowie Windows XP Professional und Windows Server 2003 durchgeführt werden. Bedenken Sie, dass Sie beim Einsatz von Windows NT 4.0 Clients bzw. Mitgliedservern zunächst, wie unter Kapitel Abbildung 3.3.4 beschrieben, vor dem Start des ADMT den Befehl eingegeben haben.

Stellen Sie zudem sicher, dass die Gruppe der Domänenadministratoren auf dem Quellserver Mitglied der vordefinierten Administratorengruppe ist. Ist diese Standardeinstellung nicht mehr vorhanden, müssen Sie die Gruppe wieder hinzufügen. Außerdem sollten auf sämtlichen Clientcomputern Echtzeit-Virenschutzprogramme sowie Software-Firewalls deaktiviert werden.

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein, sofern ADMT nicht noch geöffnet ist:

```
Runas /netonly /user:NameQuelldomäne\Administrator "mmc\"%ProgramFiles%\
Active Directory Migration Tool\Migrator.msc\"" ↵
```

Ersetzen Sie dabei NameQuelldomäne durch den entsprechenden NetBIOS-Domänennamen.

Wenn Sie ADMT schließen, dürfen Sie es nur über den eben genannten Befehl öffnen und nicht über den Eintrag im Startmenü.

2. Geben Sie nach Aufforderung das Kennwort für das Administratorkonto an. Danach erscheint die GUI des ADMT.
3. Im Menü ACTION klicken Sie auf COMPUTER ACCOUNT MIGRATION WIZARD. Konfigurieren Sie dort den Wizard mit den folgenden Informationen:

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Test or Make Changes	Klicken Sie hier auf TEST THE MIGRATION SETTINGS AND MIGRATE LATER?. So können Sie anhand der Log-Dateien mögliche Fehler erkennen und beheben. Zum endgültigen Migrationslauf klicken Sie hier MIGRATE NOW?.
Domain Selection	Unter SOURCE DOMAIN muss der Domänenname der Quelldomäne eingetragen sein, z.B. SBS45, unter TARGET DOMAIN der Name der Zieldomäne, z.B. sbs2003.local.
Computer Selection	Klicken Sie hier auf ADD und danach auf ADVANCED. Der Eintrag SELECT THIS OBJECT TYPE wird automatisch für die Suche nach Computerkonten gesetzt. Klicken Sie dann auf FIND NOW. Sie sehen eine Liste sämtlicher Computerkonten. Wählen Sie hier sämtliche Computerkonten aus, die Sie migrieren möchten, und klicken dann auf OK. Beachten Sie, dass Sie nicht das Computerkonto des Quellservers sowie Computerkonten auswählen, auf denen die Betriebssysteme Windows 95, 98 oder ME ausgeführt werden. Zudem müssen Sie sicherstellen, dass sämtliche zu migrierenden Computer eingeschaltet und mit dem Netzwerk verbunden sind. Für sämtliche Server-Computerkonten (außer dem Quellserver, der nicht migriert wird) führen Sie den Computer Migration Wizard erneut aus und fügen die Server auf der Seite ORGANIZATIONAL UNIT SELECTION der OU SBS Servers hinzu.
Organizational Unit Selection	Für sämtliche Clientcomputer navigieren Sie nach MYBUSINESS\COMPUTER\SBSCOMPUTER, für Server nach MYBUSINESS\COMPUTER\SBSSERVER und wählen dort jeweils die Ziel-OU.
Translate Objects	Stellen Sie sicher, dass sämtliche Checkboxen auf dieser Seite aktiviert sind.
Security Translation Object	Hier muss die Option REPLACE aktiviert sein. Klicken Sie dann auf NEXT. Klicken Sie auf OK, wenn die folgende Meldung angezeigt wird: Userrights translation will be performed in ‚Add' mode only. Any other objects will be translated in adherence to your mode selection.
Computer Options	Aktivieren Sie hier die Option DO NOT RENAME COMPUTERS und setzen die Anzahl der Minuten für einen Neustart nach Abschluss des Migrationswizards auf 1.

Seite des ADMT-Wizards	Vorzunehmender Eintrag
Naming Conflicts	Hier sollte die Option IGNORE CONFLICTING ACCOUNTS AND DON'T MIGRATE ausgewählt sein.
Completing the User Account Migration Wizard	Sobald Sie zum Abschluss des Wizards auf FINISH geklickt haben, erhalten Sie ein Statusfenster über die Migration. Die Migration der Computerkonten ist abgeschlossen, wenn als Status COMPLETED angezeigt wird. Um zu sehen, ob Fehler aufgetreten sind, klicken Sie auf VIEW LOG. Die Log-Datei ist sowohl bei der Simulation der Migration als auch bei der realen Migration verfügbar. Nachdem Sie auf CLOSE geklickt haben, erhalten Sie im Fenster MIGRATION TOOL AGENT MONITOR eine Statusbox über die Verbindung zu den Clientcomputern.

Tabelle 3.9: Der ADMT-Migrationsassistent für Computerkonten

Schlägt die Migration eines Computerkontos oder nach der Migration der Agent während der Konfiguration des Clients fehl, führen Sie zur Lösung des Problems die folgenden Schritte durch:

1. Prüfen Sie sämtliche Einträge in den Log-Dateien.
2. Stellen Sie sicher, dass das Computerkonto nicht im Active Directory erstellt worden ist. Öffnen Sie dazu auf dem Zielserver die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
3. Führen Sie den Computer Migration Wizard ein zweites Mal aus, und migrieren Sie das Konto erneut.

Solange Sie die Migration der Computerkonten nur im Testmodus durchführen, erhalten Sie in der Ereignisanzeige eine Meldung mit der Ereignis-ID 37075. Diese ist im Testmodus normal, da bei der Kontenmigration im Test die Domäne nicht geändert wurde.

Nachdem Sie sämtliche Clients erfolgreich migriert haben, dürfen Sie sich jedoch noch nicht an diesen anmelden. Eine Anmeldung ist erst möglich, wenn Schritt 6 – Konfiguration der Clientcomputer – abgeschlossen worden ist. Anderenfalls werden die Outlook-Profile nicht migriert.

Änderung von Exchange-Kontingenten

Wenn bei einer Migration von Exchange 5.5 auf dem Quellserver ein Mailkontingent für das Senden und Empfangen von E-Mails von 200 MB (200.000 KB) und der Warnwert auf 175 MB (175.000 KB) gesetzt ist, müssen Sie die Einstellungen auf dem Zielsystem nicht ändern. Sind auf dem Quellsystem jedoch höhere Werte gesetzt, so müssen Sie diese Kontingentwerte für das Zielsystem anpassen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie auf dem Quellserver STARTMENÜ/PROGRAMME/MICROSOFT EXCHANGE/MICROSOFT EXCHANGE ADMINISTRATOR.
2. Doppelklicken Sie auf den EXCHANGE-STANDORT, KONFIGURATION, dann auf SERVER und IHREN SERVER. Doppelklicken Sie dann auf PRIVATE INFORMATION STORE.
3. Öffnen Sie aus dem Menü DATEI den Eintrag EIGENSCHAFTEN. Notieren Sie sich dort die entsprechenden Werte.
4. Öffnen Sie dann auf dem Zielserver die SERVERVERWALTUNG aus dem Startmenü. Klicken Sie auf ERWEITERTE VERWALTUNG.
5. Doppelklicken Sie auf ORGANISATIONSNAME (EXCHANGE), ADMINISTRATIVE GRUPPEN, ERSTE ADMINISTRATIVE GRUPPE, dann auf SERVER und IHREN SERVER. Doppelklicken Sie dann auf ERSTE SPEICHERGRUPPE und wählen aus dem Kontextmenü von POSTFACHSPEICHER den Eintrag EIGENSCHAFTEN.
6. Öffnen Sie die Registerkarte GRENZWERTE und tragen die Werte des Quellservers für die maximale Postfachgröße sowie den Warnwert entsprechend ein.

Verschieben von Exchange-Postfächern

Die Postfächer des Exchange Server 5.5 werden mit Hilfe des *Exchange Server Migration Wizards* auf den Zielserver migriert. Zu diesem Zeitpunkt dürfen Sie sich an keinem der Clients anmelden und Outlook öffnen. Ansonsten wird das Outlook-Profil nicht migriert. Das Starten von Outlook ist erst nach Abschluss von Schritt 6 – Konfiguration der Clients – möglich.

Während der Migration des Exchange-Servers sollten auf diesem ebenfalls Echtzeit-Virenschutzprogramme sowie Disk Utilities beendet werden.

Um die Postfächer zu migrieren, führen Sie die folgenden Schritte aus:

1. Auf dem Zielserver öffnen Sie START/PROGRAMME/MICROSOFT EXCHANGE/BEREITSTELLUNG/ASSISTENT FÜR DIE MIGRATION. Geben Sie im Laufe des Migrationsassistenten die folgenden Informationen ein:

Seite des Migrationsassistenten	Vorzunehmender Eintrag
Migration	Wählen Sie hier MIGRATION VON MICROSOFT EXCHANGE.
Migration von Exchange Server	Sie müssen nun sicherstellen, dass LDAP (Lightweight Directory Access Protocol) aktiviert ist. Um dies zu prüfen, öffnen Sie auf dem Quellserver STARTMENÜ/PROGRAMME/MICROSOFT EXCHANGE/MICROSOFT EXCHANGE ADMINISTRATOR. Doppelklicken Sie EXCHANGE-STANDORT, KONFIGURATION, PROTOKOLLE UND LDAP (VERZEICHNIS) SITE DEFAULTS. Dieses Protokoll muss aktiviert sein.
Migrationsziel	Hier können Sie nur die Standardeinstellung MIGRATION AUF EINEN COMPUTER, DER EXCHANGE SERVER AUSFÜHRT akzeptieren.

Seite des Migrationsassistenten	Vorzunehmender Eintrag
Quell-Exchange Server	Geben Sie den Computernamen des Quellservers, das Administratorkonto sowie dessen Passwort an. Haben Sie das Exchange SA-Kennwort geändert, so dass es nicht mehr mit dem des vordefinierten Administratorkontos übereinstimmt, so müssen Sie das Exchange SA-Kennwort ändern. Weitere Hinweise finden Sie im Artikel 285297 der Microsoft Knowledge Base.
Migrationsinformationen	Bestätigen Sie die Standardeinstellung ERSTELLEN VON E-MAIL-KONTEN.
Kontenmigration	Wählen Sie hier sämtliche Konten aus, die Sie migrieren möchten. Mit Hilfe des Assistenten kann jedoch nicht das Postfach des Administrators migriert werden. Um dieses Konto zu exportieren, sichern Sie von einem Outlook-Client aus die Mails in eine pst-Datei und spielen diese später wieder zurück. Auch die Regeln für das Administrator-Postfach müssen exportiert werden. Die Migration der Postfächer für die Benutzerkonten kann erst durchgeführt werden, nachdem Sie die Benutzerkonten selbst mit Hilfe des ADMT auf das Zielsystem migriert haben.
Container for New Windows Account	Navigieren Sie hier zu DOMÄNENNAME\MYBUSINESS\USERS\SBSUSERS.

Tabelle 3.10: Der Microsoft Exchange Migrationsassistent

2. Folgen Sie den Anweisungen, um den Migrationsassistenten abzuschließen.

Verschieben der gemeinsam genutzten Benutzerordner

Die gemeinsam genutzten Benutzerordner verschieben Sie am einfachsten mit dem Befehl xcopy an der Kommandozeile. Alternativ können Sie auch das Programm Robo Copy benutzen. Dieses Programm ist Bestandteil der Windows Server 2003 Resource Kit-Tools und kann unter *http://go.microsoft.com/fwlink/?LinkId=20249* downgeloadet werden.

Stellen Sie vor dem Kopiervorgang sicher, dass die Benutzerordner nicht größer als 1 GB sind. Standardmäßig ist unter SBS 2003 das Kontingent für die Größe des Benutzerordners auf 1 GB festgelegt.

Zum Verschieben der Benutzerordner führen Sie folgende Schritte aus:

1. Öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgenden Befehl ein:

```
Xcopy \\Quellserver\Users \\Zielserver\Users /e /o /d /h /v /c >>c:\
Kopier.txt ↵
```

In dieser Befehlszeile haben die Parameter die folgende Bedeutung:

`/e`: Es werden alle Unterverzeichnisse kopiert, auch wenn diese ohne Inhalt sind.

`/o`: Es werden die Informationen der Discretionary Access Control List (DACL) sowie die Informationen über den Besitzer der Dateien kopiert.

`/d`: Es werden nur die Dateien kopiert, deren Quellzeit neuer ist als die Zielzeit. Sollen nur die Dateien kopiert werden, die nach einem bestimmten Zeitpunkt erstellt worden sind, so verwenden Sie die Option /d: m-t-j, wobei das Datum im Format Monat-Tag-Jahr angegeben werden muss.

`/h`: Es werden auch versteckte Dateien sowie Systemdateien kopiert.

`/v`: Jede neu geschriebene Datei wird überprüft.

`/c`: Sämtliche Fehler werden ignoriert.

`>>C:\Kopier.txt`: Die Ergebnisse der Kopieraktion werden in die Datei *Kopier.txt* auf Laufwerk C geschrieben. Prüfen Sie diese Datei nach Abschluss des Kopiervorgangs darauf, ob in ihr Fehlermeldungen verzeichnet sind. Zudem können Sie auch die Anzahl und Größe der Dateien in den Benutzerordnern auf dem Quell- und Zielserver miteinander vergleichen.

Da die vordefinierten Gruppen des Quellservers nicht auf den Zielserver migriert worden sind, müssen Sie die Berechtigungen für die Benutzerordner auf dem Zielserver anpassen. Führen Sie dazu die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü des Benutzerordners auf dem Zielserver den Eintrag EIGENSCHAFTEN.
2. Wählen Sie die Registerkarte SICHERHEIT. Entfernen Sie hier alle Benutzernamen und Gruppennamen, die als unbekanntes Konto aufgeführt sind. Klicken Sie dann auf ERWEITERT.
3. Deaktivieren Sie hier die Checkbox BERECHTIGUNGEN ÜBERGEORDNETER OBJEKTE AUF UNTERGEORDNETE OBJEKTE, SOFERN ANWENDBAR, VERERBEN. Diese mit den hier definierten Einträgen mit einbeziehen. Klicken Sie dann auf HINZUFÜGEN und fügen die Benutzergruppen mit den Berechtigungen gemäß der folgenden Tabelle ein:

Benutzergruppe	Berechtigung
Domänenadministratoren	Vollzugriff. Aktivieren Sie die Checkbox BERECHTIGUNGEN NUR FÜR OBJEKTE UND/ODER CONTAINER IN DIESEM CONTAINER ÜBERNEHMEN.
Ordneroperatoren	Vollzugriff. Aktivieren Sie die Checkbox BERECHTIGUNGEN NUR FÜR OBJEKTE UND/ODER CONTAINER IN DIESEM CONTAINER ÜBERNEHMEN.
SYSTEM	Vollzugriff. AKTIVIEREN SIE DIE CHECKBOX BERECHTIGUNGEN NUR FÜR OBJEKTE UND/ODER CONTAINER IN DIESEM CONTAINER ÜBERNEHMEN.

Benutzergruppe	Berechtigung
Domänenbenutzer	Ordner durchsuchen/Datei ausführen, Ordner auflisten/Daten lesen, Attribute lesen, Erweiterte Attribute lesen, Ordner erstellen/Daten anhängen sowie Berechtigungen lesen. Deaktivieren Sie die Checkbox BERECHTIGUNGEN NUR FÜR OBJEKTE UND/ODER CONTAINER IN DIESEM CONTAINER ÜBERNEHMEN.

Tabelle 3.11: Festlegen der Berechtigungen für vordefinierte Gruppenkonten

4. Führen Sie diese Schritte für jeden Benutzerordner durch.

Benutzerdefinierte Login-Skripte

Haben Sie auf dem Quellsystem benutzerdefinierte Login-Skripte verwendet, so kopieren Sie diese vom Ordner NETLOGON des Quellservers in den Ordner NETLOGON des Zielservers. Wird in den Skripten auf weitere Dateien verwiesen, so müssen Sie diese selbstverständlich auch auf den Zielserver kopieren.

Verschieben weiterer gemeinsam genutzter Ordner

Erstellen Sie auf dem Zielserver für jeden zu verschiebenden Ordner eine gleichnamige Freigabe, und vergeben Sie an diese dieselben Berechtigungen wie auf dem Quellserver. Danach verschieben Sie die Inhalte der Ordner, wie unter „Verschieben gemeinsam genutzter Benutzerordner“ weiter oben in diesem Kapitel beschrieben.

Bedenken Sie beim Erstellen der Freigaben auf dem Zielserver, sofern Sie diese auf derselben Partition erstellen wie die Benutzerordner, dass die für die Benutzerordner gesetzten Kontingenteinstellungen auch für alle weiteren Ordner greifen, die auf dieser Partition erstellt werden.

Verschieben des Firmenordners an die Intranet-Webseite

Der unter SBS 4.5 verwendete Ordner COMPANY ist unter SBS 2003 in diesem Format nicht mehr vorhanden. Vielmehr werden die Inhalte an die interne Webseite geleitet, die von den SharePoint Services bereitgestellt wird. Führen Sie zum Verschieben des Ordners die folgenden Schritte aus:

1. Öffnen Sie auf dem Zielserver die SERVERVERWALTUNG und klicken auf INTERNE WEBSEITE.
2. In der Detailansicht klicken Sie auf DATEIEN IMPORTIEREN. Es erscheint ein Assistent.
3. Auf der Seite DATEI- UND DOKUMENTBIBLIOTHEKSPFAD geben Sie unter DATEIEN KOPIEREN VON den Pfad *Quellserver**Company* ein. Unter DATEIEN KOPIEREN NACH können Sie entweder die Standardeinstellung HTTP://COMPANYWEB/GENERAL DOCUMENTS akzeptieren oder über DURCHSUCHEN eine andere Bibliothek bestimmen oder erstellen.

4. Beim Kopieren werden standardmäßig alle Dateien, die größer als 50 MB sind, nicht kopiert. Um diese Einstellung zu ändern, öffnen Sie ein Browserfenster und geben die Adresse *http://Zielserver:8081* ein. Klicken Sie hier auf KONFIGURIEREN DER VIRTUELLEN SERVEREINSTELLUNGEN, dann auf COMPANYWEB und danach auf GENERELLE EINSTELLUNGEN. Hier können Sie die Maximalgröße bestimmen.
5. Weiterhin werden standardmäßig auch keine Dateien mit bestimmten Dateiendungen wie z.B. *.exe* oder *.vbs* blockiert. Um diese Einstellungen zu ändern, geben Sie in einem Browserfenster ebenfalls die Adresse *http://Zielserver:8081* ein. Klicken Sie dann auf GESPERRTE DATEITYPEN VERWALTEN, um die Einstellungen zu modifizieren.

Generell werden nur Dateien kopiert, die auch Daten enthalten.

Verschieben weiterer Daten

Sollen noch weitere Daten verschoben werden, die sich nicht in den bisher beschriebenen Ordnern befinden, so müssen Sie diese ebenfalls kopieren. Dies gilt auch für Applikationsdaten. Spielen bei diesen Daten die Berechtigungen keine Rolle, so können Sie diese einfach kopieren. Sollen hingegen die Informationen über die Besitzer der Dateien sowie die Einträge der DACL beibehalten werden, so verwenden Sie das Programm *Xcopy* oder *Robo Copy.*

Verwenden Sie SQL-Datenbanken, die ebenfalls migriert werden müssen, so führen Sie die folgenden Schritte aus:

1. Geben Sie an der Eingabeaufforderung des Zielservers folgenden Befehl ein: \\Quellserver\Laufwerksbuchstabe$
2. Navigieren Sie auf diesem Laufwerk zum Speicherort der gewünschten Dateien, und kopieren Sie diese an den gewünschten Ort auf dem Zielserver. Wiederholen Sie diesen Vorgang für die Datenverzeichnisse sämtlicher Applikationen.

Haben Sie auf dem Quellserver eigene Webseiten unter dem IIS 4.0 (Internet Information Server) erstellt, so müssen Sie diese Dateien auf den Zielserver kopieren und danach die Webseiten unter IIS 6.0 neu erstellen. Für diesen Vorgang können Sie auch das IIS-Migrationstool benutzen. Dieses Programm befindet sich auf der Begleit-CD.

Zu diesem Zeitpunkt können Sie bereits alle erforderlichen Applikationen auf dem Zielserver installieren.

Verschieben von SQL-Datenbanken

Sofern Sie die Premium-Version des SBS 2003 verwenden und bestehende Datenbanken des SQL Servers migrieren wollen, führen Sie die folgenden Schritte aus:

Wenn auf dem Zielserver der SQL Server 2000 noch nicht installiert ist, führen Sie die Installation jetzt durch. Weitere Informationen zum Verschieben von SQL-Datenbanken zwischen SQL-Servern finden Sie im Microsoft KB-Artikel 314546 sowie zum Wiederherstellen von Datenbanken in Kapitel 7.6.4.

3.3.5 Schritt 5 – Konfiguration des Zielservers

In diesem Arbeitsschritt verbinden Sie die Benutzerkonten mit einer Benutzervorlage des SBS 2003 und verteilen Applikationen an die Clients, so dass diese bei der ersten Anmeldung bereits auf das SBS 2003-Netzwerk zugreifen können. Zusätzlich müssen auf dem Zielserver weitere Konfigurationseinstellungen vorgenommen werden. Ferner werden Exchange-Einstellungen vervollständigt, wie z.B. das Erstellen von Verteilerlisten oder die Konfiguration des Microsoft Connectors für POP3-Postfächer. Im Detail führen Sie die folgenden Schritte durch:

Berechtigungen für die migrierten Konten

Damit die Benutzer für den Zugriff auf die Ressourcen des SBS 2003-Netzwerks über die korrekten Berechtigungen verfügen, müssen Sie die Benutzerrechte auf dem Zielserver festlegen.

Im Zuge dieser Einstellungen legen Sie auch – sofern erforderlich – die Berechtigungen für Remote-Zugriff fest. Sie können auch das Connection Manager Configuration Package verteilen. Hiermit werden die erforderlichen Einstellungen für die Verbindung von mobilen und Remote-Clients konfiguriert.

Für das Festlegen der Benutzerrechte führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf dem Zielserver die SERVERVERWALTUNG. Klicken Sie dort auf BENUTZER und dann auf BENUTZERVERWALTUNG.
2. Auf der Seite der VORLAGENAUSWAHL wählen Sie für jedes migrierte Konto eine Kontenvorlage des SBS 2003 aus. Die Standardeinstellung zum Beibehalten der Benutzerrechte sollten Sie übernehmen.

Erscheint ein Benutzerkonto nicht auf der Seite der Benutzerauswahl, so stellen Sie sicher, dass dieses Konto nicht deaktiviert ist. Um dies zu prüfen, öffnen Sie die SERVERVERWALTUNG auf dem Zielserver, klicken auf BENUTZER, und in der Detailansicht wählen Sie aus dem Kontextmenü des deaktivierten Kontos den Eintrag AKTIVIEREN.

3. Folgen Sie dann den Anweisungen, um den Assistenten abzuschließen.

Haben Sie vor der Migration noch keinen Exchange-Server verwendet, so wird jetzt für jeden Benutzer automatisch ein Postfach angelegt.

Verteilen von Applikationen

Die Verteilung von Applikationen kann nur an Clients mit den Betriebssystemen Windows 2000 und XP Professional erfolgen. Für alle anderen Betriebssysteme muss die Installation manuell auf dem Client durchgeführt werden. Für Mitgliedserver unter Windows Server NT 4.0 finden Sie weitere Hinweise in der Serververwaltung unter SERVERCOMPUTER/WEITERE INFORMATIONEN/KONFIGURIEREN ZUSÄTZLICHER SERVER.

Bevor Sie die folgenden Schritte ausführen und über mehr als fünf Clients verfügen, müssen Sie zunächst zusätzliche Lizenzen hinzufügen. Im SBS 2003 sind lediglich fünf CALs inbegriffen.

1. Öffnen Sie auf dem Zielserver die SERVERVERWALTUNG und klicken auf CLIENTCOMPUTER.

2. In der rechten Fensterhälfte klicken Sie auf ZUWEISEN VON APPLIKATIONEN AN CLIENTCOMPUTER. Es erscheint ein Assistent, bei dem Sie die folgenden Informationen eingeben:

Seite des Assistenten	Vorzunehmender Eintrag
Clientcomputer	Wählen Sie hier sämtliche Clients aus, an die Sie Client-Applikationen verteilen möchten.
Client-Applikationen	Bestätigen Sie hier die Standardeinstellungen. Verwenden Sie auf dem Zielsystem den ISA-Server 2000, müssen Sie den Firewall-Client an alle Clients verteilen. Klicken Sie hierzu auf APPLIKATIONEN ÄNDERN. Auf der Seite VERFÜGBARE APPLIKATIONEN klicken Sie auf HINZUFÜGEN. Geben Sie dann den Applikationsnamen Firewall-Client ein oder navigieren über Durchsuchen zu \\ZIELSERVER\MSPCLNT\SETUP.EXE

Tabelle 3.12: Der Assistent zum Zuweisen von Client-Applikationen

3. Folgen Sie zum Abschluss den Anweisungen des Assistenten.

Die Aufgabenliste der Verwaltungsaufgaben abschließen

Sofern Sie diese Liste zwischendurch geschlossen haben, können Sie sie wieder öffnen, indem Sie in der SERVERVERWALTUNG die AUFGABENLISTE anklicken. Sie können jetzt die folgenden Verwaltungsaufgaben durchführen:

- Hinzufügen eines neuen Druckers: Hier können Sie sämtliche Drucker neu einrichten.
- Hinzufügen von Benutzern und Computern. Dieser Schritt ist nur notwendig, wenn Sie zu den migrierten Konten noch neue hinzufügen möchten.
- Faxkonfiguration: Verfügen Sie über ein Faxmodem, so können Sie dieses jetzt einrichten.
- Konfiguration der Überwachung: Hier können Sie Berichte über die Server-Performance sowie die Auslastung konfigurieren. Auch die Benachrichtigungen für Alarmoptionen werden hier bestimmt.
- Konfiguration des Backups: Hier können Sie die Optionen für das Windows Backup festlegen. Verwenden Sie das Backup-Programm eines Drittanbieters, so müssen Sie hier keine Einstellungen vornehmen.

Diese Aufgaben sind alle detailliert in Kapitel 2 beschrieben.

Übernahme benutzerdefinierter Einstellungen vom Quellserver

In diesem Schritt werden sämtliche benutzerdefinierten Konfigurationen wie z.B. DHCP-Bereichsoptionen, Einstellungen für Routing und RAS, Einstellungen an den Gruppenrichtlinien oder DNS-Einträgen auf dem Zielserver eingestellt. Kurz gesagt, in diesem Schritt werden sämtliche relevanten Einstellungen manuell auf den Zielserver übertragen, die durch keinerlei Assistenten migriert werden können.

E-Mail-Verteilerlisten und Empfangsrichtlinien

Auf dem Zielserver müssen Sie sämtliche benutzerdefinierten Empfangsrichtlinien wieder herstellen. Dasselbe gilt auch für migrierte Verteilergruppen, in denen sich vordefinierte Gruppen wie z.B. die Administratorengruppe als Mitglied befanden. Sie müssen nun die vordefinierten Gruppen des Zielservers wieder zur Verteilergruppe hinzufügen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die SERVERVERWALTUNG und dort den Eintrag VERTEILERGRUPPEN.
2. Klicken Sie in der rechten Fensterhälfte auf die gewünschte Verteilergruppe. Auf der Registerkarte MITGLIEDER können Sie die gewünschten vordefinierten Gruppenkonten wieder hinzufügen.

Microsoft Connector für POP3-Postfächer

Diese Konfiguration müssen Sie vornehmen, wenn Sie über POP3-Postfächer verfügen, die Sie auf den Exchange-Server downloaden möchten. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie in der SERVERVERWALTUNG den Eintrag INTERNET UND E-MAIL.
2. Klicken Sie in der rechten Fensterhälfte auf POP3-E-MAIL VERWALTEN. Klicken Sie dann auf POP3 CONNECTOR-MANAGER ÖFFNEN.
3. Die weitere Konfiguration von POP3-E-Mail entspricht den im Rahmen der Aufgabenliste in Kapitel 2 beschriebenen Schritten.

Aktualisieren benutzerdefinierter Login-Skripte

Nachdem Sie die benutzerdefinierten Login-Skripte bereits im Laufe der Migration in das Verzeichnis NETLOGON des Zielservers kopiert haben, müssen diese nun für die Benutzer nutzbar gemacht werden. Dazu müssen Sie jedes Benutzerkonto aktualisieren, so dass es auf das Login-Skript auf dem Zielserver referenziert. Zusätzlich müssen Sie im Login-Skript sämtliche Verweise auf den Quellserver mit den Verweisen auf den Zielserver aktualisieren.

3.3.6 Schritt 6 – Konfiguration der Clients

In diesem Schritt erhalten die Windows 2000- und XP Professional-Clients automatisch die Konfigurationseinstellungen für E-Mail und Proxy. Auf allen anderen Client-Betriebssystemen müssen Sie die Konfiguration manuell vornehmen. Weiterhin können Sie nun auch die öffentlichen Exchange-Ordner importieren, so dass die Clients vollständig für die Verbindung mit dem neuen Exchange-Server konfiguriert sind. Im Detail führen Sie die folgenden Schritte durch:

Konfiguration von Windows 2000-/XP-Clients

1. Melden Sie sich an jedem Clientcomputer mit dem jeweiligen Benutzerkonto an. Sie werden bei der Anmeldung aufgefordert, für das Konto ein neues Passwort festzulegen. Notieren Sie sich jeweils das vergebene Passwort. Achten Sie hierbei bereits auf die Passwortsicherheit, da Sie den Zielserver nach Abschluss der Migration mit dem Internet verbinden. Sofern Sie die alten Benutzerpasswörter nicht migriert haben,

sind die Passwörter standardmäßig alle in der Datei \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT gespeichert. Wie bereits erwähnt, besteht das Passwort aus den ersten 14 Zeichen des Benutzernamens.

2. Haben Sie den Client unter Schritt 5 (siehe Kapitel 3.3.5) für die Verteilung von Applikationen ausgewählt, so erscheint nach dem Start der Client-Installations-Wizard. Klicken Sie in diesem auf JETZT STARTEN.
3. Öffnen Sie dann die SYSTEMSTEUERUNG und klicken auf MAIL. Aktualisieren Sie dann die E-Mail-Eigenschaften gemäß dem Zielserver.

Verwenden Sie auch den ISA-Server, müssen Sie auch die Proxy-Einstellungen des Internet Explorer konfigurieren.

1. Öffnen Sie dazu den Internet Explorer. Im Menü EXTRAS klicken Sie auf INTERNETOPTIONEN.
2. Auf der Registerkarte VERBINDUNGEN klicken Sie unter LAN-EINSTELLUNGEN auf EINSTELLUNGEN.
3. Aktivieren Sie die Checkbox PROXY-SERVER FÜR LAN VERWENDEN und tragen unter ADRESSE den Namen des Zielservers und unter PORT 8080 ein.
4. Haben Sie lediglich auf dem Quellserver den Proxy-Server verwendet, jedoch nicht auf dem Zielserver, so stellen Sie sicher, dass die Proxy-Checkbox in den LAN-EINSTELLUNGEN sowie dort auch die Checkbox AUTOMATISCHE SUCHE DER EINSTELLUNGEN unter AUTOMATISCHE KONFIGURATION deaktiviert ist.

Danach können Sie auf dem Client wieder den Echtzeit-Virenschutz aktivieren. Fahren Sie dann im Abschnitt „Herstellung der Internetverbindung“ fort.

Konfiguration älterer Windows-Clients

Clientcomputer mit älteren Betriebssystemen als Windows 2000 müssen manuell für die Zieldomäne konfiguriert werden, danach werden manuell die Applikationen auf ihnen installiert.

1. Nachdem Sie diese beiden Vorbereitungen abgeschlossen haben, melden Sie sich an jedem Clientcomputer mit dem jeweiligen Benutzerkonto an. Sie werden bei der Anmeldung aufgefordert, für das Konto ein neues Passwort festzulegen.

Notieren Sie sich jeweils das vergebene Passwort. Achten Sie hierbei bereits auf die Passwortsicherheit, da Sie den Zielserver nach Abschluss der Migration mit dem Internet verbinden. Sofern Sie die alten Benutzerpasswörter nicht migriert haben, sind die Passwörter standardmäßig alle in der Datei \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT gespeichert. Wie bereits erwähnt, besteht das Passwort aus den ersten 14 Zeichen des Benutzernamens.

2. Öffnen Sie dann die SYSTEMSTEUERUNG und klicken auf MAIL. Aktualisieren Sie dann die E-Mail-Eigenschaften gemäß dem Zielserver.
3. Löschen Sie sämtliche Favoriten des Internet Explorers, die auf den Quellserver verweisen, da diese nicht länger gültig sind.
4. Löschen oder aktualisieren Sie sämtliche Desktop-Verknüpfungen mit den gemeinsam genutzten Benutzer- und Firmenordnern. Dies gilt auch für Verknüpfungen mit Netzlaufwerken und weiteren Verknüpfungen, die sich auf den Quellserver beziehen.

5. Sind hier Drucker und Faxgeräte konfiguriert, die auf den Quellserver verweisen, so löschen Sie diese. Aktualisierte Drucker und Faxgeräte wurden bereits in Schritt 5 – Konfiguration des Zielservers – eingerichtet.
6. Ist der Firewall-Client des ISA-Servers bereits installiert, müssen Sie den Namen des ISA-Servers gemäß dem des Zielservers auf den Clients anpassen. Doppelklicken Sie dazu das Firewall-Client-Icon im System-Tray. In den dann erscheinenden Optionen tragen Sie den neuen Servernamen ein.

Verwenden Sie auch den ISA-Server, müssen Sie auch die Proxy-Einstellungen des Internet Explorers konfigurieren.

1. Öffnen Sie dazu den Internet Explorer. Im Menü EXTRAS klicken Sie auf INTERNETOPTIONEN.
2. Auf der Registerkarte VERBINDUNGEN klicken Sie unter LAN-EINSTELLUNGEN auf EINSTELLUNGEN.
3. Aktivieren Sie die Checkbox PROXY-SERVER FÜR LAN VERWENDEN und tragen unter ADRESSE den Namen des Zielservers und unter PORT 8080 ein.
4. Haben Sie lediglich auf dem Quellserver den Proxy-Server verwendet, jedoch nicht auf dem Zielserver, so stellen Sie sicher, dass die Proxy-Checkbox in den LAN-EINSTELLUNGEN sowie dort auch die Checkbox AUTOMATISCHE SUCHE DER EINSTELLUNGEN unter AUTOMATISCHE KONFIGURATION deaktiviert ist.

Danach können Sie auf dem Client wieder den Echtzeit-Virenschutz aktivieren.

Überprüfen der Netzwerkverbindung

Abschließend müssen Sie prüfen, ob die migrierten Clients einen funktionierenden Netzwerkzugang haben. Um dies zu testen, trennen Sie den Quellserver vom Netzwerk und senden eine Test-E-Mail an die Benutzer. Erreicht die Mail ihre Empfänger, sind die Interneteinstellungen korrekt konfiguriert.

Zusätzlich müssen Sie auch testen, ob freigegebene Ordner, gemeinsam genutzte Applikationen sowie Netzwerkdrucker verfügbar sind und funktionieren.

Nach Abschluss dieser Schritte können Sie sich an einem Client als Administrator einloggen und das Postfach sowie Regeln für das Administratorkonto auf den Zielserver importieren.

Offline-Adressbücher stehen frühestens eine Stunde nach der Installation des SBS 2003 zur Verfügung. Versuchen Sie bereits früher einen Zugriff, so wird dieser fehlschlagen, da das Offline-Adressbuch zu diesem Zeitpunkt noch nicht generiert ist.

Import öffentlicher Ordner

Als Nächstes werden die in eine .pst-Datei exportierten öffentlichen Ordner des Quellservers wieder importiert. Führen Sie dazu die folgenden Schritte durch:

1. Melden Sie sich auf einem Client mit dem Administratorkonto an und starten *Outlook*.
2. Doppelklicken Sie ÖFFENTLICHE ORDNER und dann ALLE ÖFFENTLICHEN ORDNER.
3. Importieren Sie dann die .pst-Datei in den aktuell ausgewählten Ordner.

Waren für einen der öffentlichen Ordner spezielle Berechtigungen konfiguriert, so müssen Sie diese wieder herstellen.

1. ERWEITERTE VERWALTUNG, ADMINISTRATIVE GRUPPEN, ERSTE ADMINISTRATIVE GRUPPE, SERVER, IHR SERVER, ERSTE SPEICHERGRUPPE, INFORMATIONSSPEICHER FÜR ÖFFENTLICHE ORDNER, ÖFFENTLICHE ORDNER.
2. In der rechten Fensterhälfte wählen Sie aus dem Kontextmenü des gewünschten Ordners den Eintrag EIGENSCHAFTEN.
3. Auf der Registerkarte BERECHTIGUNGEN klicken Sie auf CLIENT-BERECHTIGUNGEN. Aktualisieren Sie dann die Felder NAME, ROLLE und BERECHTIGUNGEN mit den gewünschten Einträgen.

3.3.7 Schritt 7 – Abschluss der Migration

Nach Abschluss der Migration können Sie den Quellserver außer Betrieb setzen. Es ist jedoch sinnvoll, diesen für eine Übergangszeit noch bereitzuhalten, um so mögliche Konfigurationsprobleme des neuen Servers beheben zu können, sofern es sich dabei um Informationen handelt, die vom alten Server manuell übernommen werden können. Erst nach dieser Übergangszeit sollten Sie den alten Server ganz außer Betrieb nehmen und formatieren. Sie können dieses Gerät beispielsweise als zweiten Server einrichten.

Weiterhin wird das ADMT wieder vom Zielserver deinstalliert, und alle Prä-Windows 2000-Berechtigungen, die im Verlauf der Migration möglicherweise temporär heraufgesetzt wurden, müssen aus Sicherheitsgründen wieder auf die Ursprungswerte zurückgesetzt werden.

Zurücksetzen von Berechtigungen

Diesen Schritt müssen Sie nur ausführen, wenn Sie unter Schritt 4 – Beginn der Migration – auf dem Quellserver erweiterte Berechtigungen für den Prä-Windows 2000-kompatiblen Zugriff konfiguriert haben. Verwenden Sie Mitgliedserver unter Windows Server NT 4.0, so überspringen Sie diesen Schritt, damit für diese Server der Zugriff auf die neue Domäne gewährleistet ist.

1. Um die Berechtigungen zurückzusetzen, öffnen Sie auf dem Zielserver die Eingabeaufforderung und geben folgende Befehle ein:

   ```
   Net localgroup “pre-windows 2000 compatible access“ everyone /delete ↵
   Net localgroup “pre-windows 2000 compatible access“ “anonymous logon” /
   delete ↵
   ```

2. Starten Sie danach den Zielserver neu, und melden Sie sich unter dem Administratorkonto an.

Deinstallation des ADMT

Nach der Migration sämtlicher Konten sollten Sie ADMT vom Zielserver wieder deinstallieren. Erledigen Sie dies wie gewohnt über SYSTEMSTEUERUNG/SOFTWARE/PROGRAMME HINZUFÜGEN ODER ENTFERNEN.

Festlegen von Kennwortrichtlinien

Sofern Sie nicht die alten Benutzerpasswörter ebenfalls migriert haben, sollten Sie jetzt eine Kennwortrichtlinie festlegen, die alle Benutzer auffordert, bei der ersten Anmeldung ein neues Kennwort festzulegen.

1. Öffnen Sie dazu in der SERVERVERWALTUNG den Eintrag BENUTZER.
2. Klicken Sie in der rechten Fensterhälfte auf FESTLEGEN VON KENNWORT-RICHTLINIEN. Nach Möglichkeit sollten Sie alle drei angebotenen Optionen auswählen.
3. Klicken Sie dann auf KENNWORT-RICHTLINIEN KONFIGURIEREN, und klicken Sie dann auf SOFORT.

Sofern Sie Zugriff auf den Server über das Internet zulassen, sollten Sie in jedem Fall die Komplexität der Kennwörter aktivieren. Die Anforderungen für ein komplexeres Kennwort treten dabei erst nach drei Tagen in Kraft, so dass genügend Zeit verbleibt, um in Ruhe weitere Benutzerkonten einrichten zu können.

4. Zusätzlich sollten Sie die im Zuge der Kontenmigration angelegte Passwortdatei löschen. Dabei handelt es sich um die Datei \PROGRAM FILES\ACTIVE DIRECTORY MIGRATION TOOL\LOGS\PASSWORDS.TXT.

Ferner ist zu überlegen, ob Sie den Benutzern die Möglichkeit geben möchten, ihr Kennwort ändern zu können oder nicht. Für ein Zulassen des Änderns spricht eine höhere Sicherheit, dagegen möglicherweise, dass der Administrator ständig Kennwörter zurücksetzen muss, da die Benutzer diese vergessen. Im Einzelfall – auch abhängig von ihren Benutzern – müssen Sie entscheiden, für welche Option Sie sich entscheiden.

Um die Änderung von Kennwörtern zu aktivieren oder deaktivieren, öffnen Sie in der SERVERVERWALTUNG den Eintrag BENUTZER. Doppelklicken Sie auf das gewünschte Konto. Auf der Registerkarte KONTO können Sie die Checkbox BENUTZER KÖNNEN IHR KENNWORT NICHT ÄNDERN aktivieren oder deaktivieren.

Verbindung des Zielservers mit dem Internet

Verbinden Sie abschließend das Netzwerkgerät des Zielservers für die Internetverbindung wieder mit dem entsprechenden Kabel. Um die Verbindung ins Internet zu testen, öffnen Sie von einem beliebigen Client aus eine Webseite. Verschicken Sie auch eine Test-E-Mail an ein Mailkonto im Internet. Haben Sie auch die Faxdienste konfiguriert, so sollten Sie auch ein Testfax senden.

3.4 Update des Small Business Server 2000

Bei einem Update wird im Gegensatz zur Migration der SBS 2003 auf dem ursprünglichen System installiert. Ein Upgrade ist nur möglich, wenn bereits SBS 2000 oder aber Windows Server 2000 oder 2003 ausgeführt wird. Eine Update-Möglichkeit vom SBS 4.5 oder Windows Server NT 4.0 besteht nicht.

Im Laufe des Updates werden auf dem System die folgenden Schritte durchgeführt:

- Betriebssystemaktualisierung
- Konfiguration des Betriebssystems
- Aktualisierung bereits vorhandener SBS-Tools und Serveranwendungen
- Abarbeiten der Aufgabenliste nach Beendigung des Setups

1. Um einen SBS 2000 upzudaten, muss auf diesem das SBS 2000 Service Pack 1 installiert sein. Weiterhin müssen Sie überprüfen, ob die Hardwareanforderungen für SBS 2003 auf dem Server erfüllt sind. Zusätzlich sollten Sie auf sämtlichen Datenträgern die Datenträgerbereinigung sowie die Defragmentierung durchführen. Sie starten die Datenträgerbereinigung unter AUSFÜHREN über den Befehl cleanmgr.exe, die Defragmentierung über den Befehl dfrg.msc. Es müssen mindestens 2 GB freier Speicherplatz vorhanden sein. Dieser Speicherplatz wird temporär während des Setups verwendet. Auch die bisher verwendete Hardware und Software muss mit SBS 2003 kompatibel sein. Link von oben. Auf dem SBS 2000 sollten für sämtliche Hardwarekomponenten aktuelle Treiber installiert sein. Auch das BIOS sollte den neuesten Revisionsstand haben. Unmittelbar vor dem Update sollten Sie eine vollständige Virenprüfung des Systems durchführen.

Beachten Sie unbedingt, dass Sie während des Virenscans nicht das Exchange-Laufwerk M: mitscannen. Dies kann zu Schäden an der Exchange-Datenbank führen. Standardmäßig wird unter Exchange 2000 das IFS (Installable File System) auf das Laufwerk M: gemapt.

2. Danach führen Sie eine komplette Sicherung des Systems durch, so dass Sie dieses im Falle von Problemen während des Updates wieder zurückspielen können. Testen Sie die Sicherung, indem Sie einige Daten an einen alternativen Speicherplatz zurückspielen und mit dem Original vergleichen.

Beachten Sie unbedingt, dass Sie im Zuge des Exchange-Backups nicht das Exchange-Laufwerk M: sichern. Dies kann zu Schäden an der Exchange-Datenbank führen. Standardmäßig wird unter Exchange 2000 das IFS (Installable File System) auf das Laufwerk M: gemapt.

3. Sofern zu diesem Zeitpunkt noch Benutzer mit dem SBS-Netzwerk verbunden sind, fordern Sie diese auf, sich vom Netzwerk abzumelden. Verwenden Sie dazu beispielsweise folgenden net send-Befehl:

```
Net send * Bitte melden Sie sich innerhalb der nächsten 5 Minuten von der
Domäne ab. Es sind dann keine Netzwerk- und Internetverbindungen mehr ver-
fügbar. ↵
```

Dabei bedeutet das Symbol *, dass die Nachricht an alle Mitglieder der Domäne geschickt wird.

4. Wird auf dem Netzwerkgerät, das die Verbindung zum Internet herstellt, keine Firewall ausgeführt, sollten Sie dieses vom Internet trennen. Die Verbindung zum lokalen Netzwerk bleibt bestehen.
5. Auf dem SBS 2000 müssen Sie nun sämtliche Anwendungen beenden, die das lokale Systemkonto benutzen. Sind diese Anwendungen während des Updates aktiv, können sie möglicherweise Dateien des Betriebssystems sperren, so dass diese nicht aktualisiert werden können. Um zu ermitteln, welche Anwendungen das lokale Systemkonto benutzen, geben Sie unter AUSFÜHREN den Befehl services.msc ein. Prüfen Sie, für welche Applikationen in der Spalte ANMELDEN ALS der Eintrag LOKALES SYSTEM angezeigt wird. Notieren Sie sich den jeweiligen Starttyp dieser Dienste, und beenden Sie sie.
6. Zum Schluss beenden Sie Echtzeit-Virenschutzprogramme und andere Festplatten-Tools wie z.B. Sicherungssoftware.

3.4.1 Schritt 1 – Installation

Mit der Installation des SBS 2003 wird das Betriebssystem des bestehenden SBS 2000 aktualisiert. Der Ablauf der Installation entspricht dabei dem in Kapitel beschriebenen Verlauf. Nachdem die Update-Installation abgeschlossen worden ist, dürfen auf dem SBS 2003 noch keine Einstellungen am Server geändert werden, solange nicht die nach der Installation erscheinende Aufgabenliste abgearbeitet ist.

Für die Update-Installation werden auf einem Server mit den minimalen Hardwareanforderungen ca. 45 Minuten benötigt.

3.4.2 Schritt 2 – Konfiguration von Windows

Nach der Installation des Betriebssystems erfolgt nun die Konfiguration von Windows durch den SBS 2003. Genauer gesagt erhalten Sie auch beim Update die Aufgabenliste, die bereits ausführlich in Kapitel xx beschrieben worden ist.

Hier werden jetzt nur kurz die einzelnen Aufgaben vorgestellt. Für das Fertigstellen der Aufgabenliste ist ca. eine halbe Stunde erforderlich. Sie müssen sich mit dem Administratorkonto am System anmelden. Über die entsprechende Verknüpfung auf dem Desktop gelangen Sie zur Seite MICROSOFT WINDOWS SMALL BUSINESS SERVER SETUP WEITERFÜHREN. Hier klicken Sie auf WEITER.

Nacheinander geben Sie die folgenden Konfigurationsinformationen ein:

- Firmeninformationen: Hier prüfen Sie die vorhandenen Informationen zu Ihrer Firma.
- Anmeldeinformationen: Wählen Sie die Option AUTOMATISCH ANMELDEN aus, so dass Sie während der Installation und Konfiguration nach den Neustarts nicht jedes Mal das Benutzerkonto und Kennwort angeben müssen.
- Windows-Konfiguration: Hier sehen Sie die Windows-Komponenten, die zunächst installiert werden müssen, ehe Sie mit weiteren Schritten fortfahren können. Klicken Sie hier auf WEITER.

Danach erhalten Sie das Fenster KOMPONENTENSTATUS, das Sie über den Installations- und Konfigurationsstatus informiert. Zwischendurch wird der Server neu gestartet. Diese Installations- und Konfigurationsphase dauert ca. 20 Minuten. Wird das Fenster KOMPONENTENAUSWAHL angezeigt, ist die Installation der Komponenten abgeschlossen, und Sie können die Serveranwendungen des SBS 2003 installieren.

3.4.3 Schritt 3 – Installation der Serveranwendungen

Nun erfolgt die Aktualisierung der bisherigen Serveranwendungen wie z.B. Exchange und der Systemwerkzeuge. Bei einer Standardinstallation ist dieser Schritt mit ca. 1,5 Stunden zu veranschlagen.

Wird auf dem SBS 2003 der SQL Server 2000 ausgeführt, so wird im Zuge der Installation SharePoint Services dennoch eine Instanz der Microsoft Data Engine (MSDE) installiert. Diese hat jedoch keinen Einfluss auf den SQL Server 2000.

Im Fenster KOMPONENTENAUSWAHL werden alle für die Installation erforderlichen Komponenten aufgelistet.

Das Fenster DATENORDNER dient zur Angabe eines alternativen Speicherorts für Internet-Dateien. Zusätzlich müssen Sie hier einen Speicherort für die Applikationen bestimmen, die unter SBS 2000 noch nicht installiert waren.

Die eben vorgenommenen Einstellungen können Sie im Fenster KOMPONENTENZUSAMMENFASSUNG ansehen und bei Bedarf noch ändern.

Sie erhalten dann wie bereits vorhin das Fenster KOMPONENTENSTATUS, das Sie über den Status der Installation informiert. Die Installation dauert ca. eine Stunde. Wenn während der Installation Probleme und Fehler auftreten, erhalten Sie das Fenster KOMPONENTENNACHRICHT. Hier wird eine Fehlermeldung oder Nachricht angezeigt.

Sie erhalten dann das Fenster FERTIGSTELLEN DER INSTALLATION. Klicken Sie auf FERTIG STELLEN und dann auf OK. Danach erfolgt ein Neustart des Systems.

3.4.4 Schritt 4 – die Aufgabenliste

Zum Fertigstellen der Installation müssen Sie die abschließende Aufgabenliste abarbeiten. Hierbei ist es empfohlen, die dort angezeigte Reihenfolge beizubehalten. Für diesen Schritt müssen Sie ca. eine halbe Stunde Arbeitszeit einplanen.

Um mit der Abarbeitung zu beginnen, klicken Sie auf START. Sobald Sie eine Aufgabe der Liste abgeschlossen haben, können Sie die entsprechende Checkbox markieren, um die Aufgabe als erledigt zu kennzeichnen.

Die Aufgabenliste besteht aus den Bereichen Netzwerkaufgaben und Verwaltungsaufgaben. Nähere Informationen zu jeder Aufgabe erhalten Sie, wenn Sie auf WEITERE INFORMATIONEN klicken. Detailliert wurden die Optionen für die verschiedenen Aufgaben bereits in Kapitel 2 beschrieben.

Netzwerkaufgaben

Innerhalb der Netzwerkaufgaben sind die folgenden Punkte zu erledigen:

- Bewährte Sicherheitsmethoden anzeigen: Für die Sicherheit des Netzwerks sollten Sie die hier vorgeschlagenen Methoden und Verfahren umsetzen.
- Verbindung mit dem Internet herstellen: Bevor Sie hiermit beginnen, müssen Sie den Server wieder mit dem Internet verbinden. Hiermit starten Sie den Assistenten E-Mail und Internetverbindung konfigurieren. Sie können dabei die Netzwerkeinstellungen, E-Mail-Einstellungen, Firewall sowie die sichere Webseite des Servers konfigurieren. Bei der Konfiguration der Kennwortrichtlinien sollten Sie, sofern auf den Server vom Internet aus zugegriffen werden soll, auf jeden Fall komplexe Kennwörter verwenden.
- RAS konfigurieren: Diese Konfiguration ist erforderlich, wenn Sie Clients gestatten wollen, per VPN oder Wählverbindung eine Verbindung zum SBS 2003-Netzwerk herzustellen. Für die Konfiguration wird der RAS-Assistent gestartet. Alle Benutzer, die momentan bereits über die Berechtigung verfügen, von außerhalb auf das Netzwerk zuzugreifen, müssen zur Sicherheitsgruppe Mobil Users hinzugefügt werden. Dies geschieht über die Aufgabe Benutzer migrieren der Verwaltungsaufgaben. Der SBS 2003 bietet zudem das Verbindungsmanager-Konfigurationspaket. Mit Hilfe dieses Pakets werden die Konfigurationseinstellungen für mobile und Remote-Clients vorgenommen. Klicken Sie dazu auf die Aufgabe BENUTZER UND COMPUTER HINZUFÜGEN in der Aufgabenliste.
- Server aktivieren: Für den SBS 2003 ist eine Aktivierung erforderlich. Am komfortabelsten geschieht diese via Internetverbindung. Folgen Sie den Anweisungen des Aktivierungsassistenten.
- Clientlizenzen hinzufügen: Sofern Sie mehr als fünf Clients einsetzen, müssen Sie die zusätzlich zu den fünf enthaltenen CALs weitere Lizenzen hinzufügen. Hierzu muss der Server aktiviert sein.

Verwaltungsaufgaben

Innerhalb der Verwaltungsaufgaben sind die folgenden Punkte zu erledigen:

- Benutzer migrieren: In diesem Schritt werden die Benutzervorlagen des SBS 2000 auf die des SBS 2003 aktualisiert. Aktualisieren Sie die Benutzervorlagen nicht, so sind für die Benutzer die neuen Features nicht verfügbar.
- Clientcomputer aktualisieren: In diesem Schritt erhalten die Clients die Einstellungen für SBS 2003. Wenn Sie die Clientcomputer nicht aktualisieren, stehen die neuen Features nicht zur Verfügung.
- Fax konfigurieren: Hier können Sie ein Faxmodem zum Senden und Empfangen von Faxen konfigurieren.
- Überwachung konfigurieren: Hier werden sowohl Benachrichtigungen über verschiedene Alarme als auch Berichte über die Leistung und Ausnutzung des Servers konfiguriert.
- Sicherung konfigurieren: Konfigurieren Sie die Sicherungsoptionen der Windows-eigenen Sicherung.

Nachdem Sie diese Aufgaben alle abgearbeitet haben, ist das Update des SBS 2000 abgeschlossen. Für noch weitere Verwaltungsaufgaben können Sie nun die Serververwaltungskonsole benutzen. Sie finden diese ebenfalls in der Aufgabenliste.

Abschließend müssen Sie die Dienste, die Sie vor Beginn des Updates beendet haben, wieder starten und den vorher gesetzten Starttyp wieder einstellen.

3.5 Update des Windows Server 2000/2003

Das Update eines Windows Server 2000 oder 2003 verläuft nahezu analog zu dem im letzten Kapitel beschriebenen Update-Prozess des SBS 2000. Zur Vorbereitung der Installation führen Sie alle in Kapitel 3.4 aufgeführten Aufgaben durch.

Allerdings müssen Sie bei dem Update eines Windows 2000-/2003-Servers darauf achten, welche Rolle dieser im Netzwerk spielt, da der SBS 2003 nur eine Domäne bilden kann, die zudem die Root-Domäne bilden muss. Handelt es sich bei dem upzudatenden Server beispielsweise um einen Domänencontroller einer untergeordneten Domäne, so können Sie diesen zwar für eine neue Domäne konfigurieren, jedoch können mit der SBS-Domäne keine Vertrauensstellungen zu weiteren Domänen hergestellt werden.

3.5.1 Schritt 1 – Installation

Der in Kapitel 3.4.1 beschriebene Schritt 1 – Installation – verläuft hier genauso.

3.5.2 Schritt 2 – Konfiguration von Windows

Im zweiten Schritt erhalten Sie nach dem Fenster der Firmeninformationen zusätzlich das Fenster INTERNE DOMÄNENINFORMATIONEN. Hier wird für die Domäne der DNS- und NetBIOS-Name bestimmt. Nach Möglichkeit sollten Sie die vorgeschlagenen Standardwerte übernehmen.

Bedenken Sie, dass Sie nach der Installation des SBS 2003 den Computernamen, DNS-Namen sowie NetBIOS-Namen standardmäßig nicht mehr ändern können. Sie müssten für eine Änderung auf das Active Directory-Supporttool *Domainrename* (*RENDOM*) zurückgreifen.

Weiterhin erhalten Sie das Fenster INFORMATIONEN ZU LOKALEN NETZWERKADAPTERN, sofern der Server über mehrere Netzwerkkarten verfügt. Wählen Sie hier die Karte für den internen Netzwerkzugriff aus. Diese Netzwerkkarte wird konfiguriert, während die anderen vom Setup-Programm automatisch deaktiviert werden. Die Einstellungen dieser Karten bleiben dabei erhalten.

Das Fenster ANMELDEINFORMATIONEN erhalten Sie nur, wenn der Server kein Domänencontroller ist. Sie haben die Möglichkeit, bis zum Abschluss der Installation die Anmeldungen automatisch durchzuführen.

Das Fenster DATENORDNER wird angezeigt, wenn der Speicherort für das Active Directory nicht gültig ist. Sie müssen dann ein anderes Verzeichnis auswählen.

Danach erfolgt die Installation der Komponenten. Der Installationsstatus wird angezeigt.

3.5.3 Schritt 3 – Installation der Serveranwendungen

Die Installation der Serveranwendungen verläuft genauso wie beim Update des SBS 2000. Dieser Vorgang ist in Kapitel 3.4.3 beschrieben.

3.5.4 Schritt 4 – die Aufgabenliste

Auch bei dem Update eines Windows Server 2000/2003 erhalten Sie am Ende die Aufgabenliste. Die in ihr enthaltenen Netzwerkaufgaben und Verwaltungsaufgaben werden wie bereits im Kapitel 3.4.4 für das Update des SBS 2000 beschrieben.

4 Der Exchange Server 2003 und die Faxdienste

In diesem Kapitel werden Ihnen der Exchange Server 2003 sowie die Faxdienste des SBS und deren Verwaltung und Konfiguration vorgestellt. Die beiden Komponenten sind getrennt voneinander installierbar und ausführbar. Sie werden lediglich in einem Kapitel abgehandelt, da beide Dienste zum Bereich der Kommunikation gehören.

Die im Lieferumfang des SBS 2003 enthaltene Version des Exchange Servers 2003 unterscheidet sich im Funktionsumfang nicht von einem einzeln erwerbbaren Exchange Server 2003 in der Standardedition.

4.1 Aufbau des Exchange Servers 2003

Zunächst einmal erfolgt eine kurze Einführung in den Aufbau der Datenbank des Exchange Servers.

4.1.1 Die Datenbank des Exchange Servers

Wie schon unter Exchange 2000 verwendet auch Exchange 2003 eine ESE-Datenbank (Extensible Storage Engine). Dabei handelt es sich um eine Weiterentwicklung der bereits unter Exchange 5.5 verwendeten ESE97-Datenbank. In dieser Datenbank befinden sich die privaten Postfächer der Benutzer im Postfachspeicher und die öffentlichen Ordner im öffentlichen Speicher. Beim Anlegen der Datenbank wird vom Administrator entschieden, welche Funktion von Speicher die Datenbank enthält. Dieses kann später nicht mehr geändert werden.

Jeder Speicher besteht aus einer Reihe von einzelnen Dateien. In einer *.edb-Datei* befinden sich sämtliche E-Mails, Termine usw., die der Benutzer unter Outlook erstellt. Diese Datei ist für den schnellen Zugriff auf die darin enthaltenen Informationen optimiert. Sie wird im Exchange-internen EDBF-Format gespeichert.

Neben der edb-Datei enthält der Speicher auch eine *.stm-Datei*. Dabei handelt es sich um eine Stream-Datei. In ihr werden die Informationen gespeichert, die über eines der unterstützten Internetprotokolle im Speicher abgelegt werden. Um auf die Informationen der stm-Datei zugreifen zu können, wird der jeweilige Nachrichtenkopf zusätzlich in der edb-Datei gespeichert.

4.1.2 Das Speichern einer E-Mail in der Datenbank

Wenn ein Benutzer eine E-Mail über das Internet empfängt, wird der Inhalt zunächst in der stm-Datei gespeichert. Gleichzeitig wird der Nachrichtenkopf auch in der edb-Datei gespeichert. Sobald der Benutzer mit seinem Outlook auf die E-Mail zugreift, wird sie bei

der Übertragung an den Benutzer konvertiert. In der stm-Datei hingegen bleibt die E-Mail als ursprünglicher Inhalt erhalten. Sobald der Benutzer die E-Mail unter Outlook speichert oder in irgendeiner Form verändert, wird die stm-Datei gelöscht und eine Kopie im EDBF-Format in der EDB-Datei gespeichert.

4.2 Verwalten des Exchange Servers

Dieses Kapitel gibt Ihnen einen Überblick über die Grundlagen der Verwaltung sowie der Verwaltungsprogramme des Exchange Servers 2003.

4.2.1 Verwaltungspunkte

Die Konfigurationseinstellungen für den Exchange Server 2003 werden an zwei verschiedenen Stellen vorgenommen. Zum einen können Sie über den System-Manager Zugriff auf sämtliche Komponenten des Exchange Servers erlangen. In dieser Managementkonsole (siehe Abbildung 4.1) werden hierarchisch geordnet sämtliche Exchange-Organisationen angezeigt und können verwaltet werden.

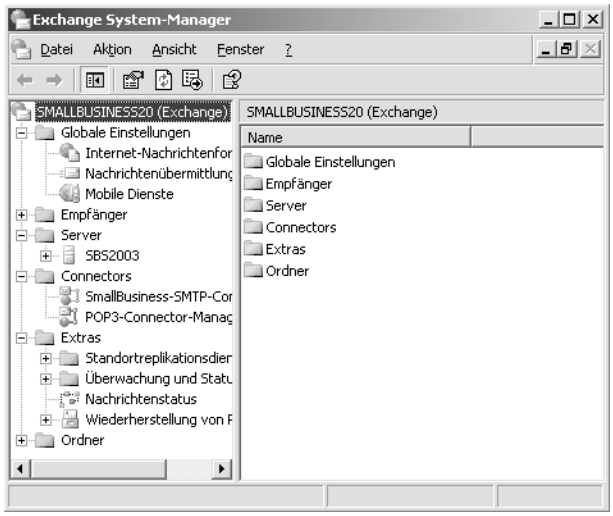


Abbildung 4.1: Der System-Manager des Exchange Server 2003

Sie starten den System-Manager, indem Sie in der SBS-Verwaltungskonsole den Eintrag ERWEITERTE VERWALTUNG/ERSTE ORGANISATION (EXCHANGE) wählen oder den Eintrag STARTMENÜ/ALLE PROGRAMME/MICROSOFT EXCHANGE/SYSTEM-MANAGER. Diese mmc ist in der Datei *Exchange System Manager.msc* gespeichert.

Sollen hingegen für die Benutzer Postfächer konfiguriert werden, so benutzen Sie dafür die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Auch diese können Sie über die entsprechende Option in der SBS-Verwaltung öffnen.

Nach der Installation von Exchange 2003 sind standardmäßig administrative Gruppen und Routing-Gruppen deaktiviert. Dies bietet in kleinen und mittleren Unternehmen den Vorteil einer vereinfachten Benutzeroberfläche, da dort diese Gruppen in aller Regel nicht benötigt werden.

4.2.2 Administrative Gruppen

Administrative Gruppen werden angelegt, um bestimmten Benutzern die Berechtigungen für Verwaltungsaufgaben zu übertragen. Im Gegensatz zu Exchange 2000 ist unter Exchange 2003 auf dem SBS 2003 standardmäßig keine administrative Gruppe vorhanden. Dies liegt darin begründet, dass administrative Gruppen in aller Regel eher in größeren Umgebungen verwendet werden. Um hier bezüglich der Übersichtlichkeit keine Verwirrung zu stiften, sind die administrativen Gruppen zunächst deaktiviert.

Um eine administrative Gruppe anzulegen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den System-Manager und wählen aus dem Kontextmenü der EXCHANGE-ORGANISATION den Eintrag EIGENSCHAFTEN.
2. Markieren Sie dort die Checkbox ADMINISTRATIVE GRUPPEN ANZEIGEN. Danach müssen Sie den System-Manager neu starten.
3. Im neuen Container ADMINISTRATIVE GRUPPEN befindet sich nun der Eintrag ERSTE ADMINISTRATIVE GRUPPE. Um eine neue Gruppe zu erstellen, klicken Sie im Kontextmenü des Containers auf NEU.
4. Geben Sie der neuen Gruppe einen Namen und klicken auf OK.
5. Um der Gruppe Berechtigungen zuzuweisen, klicken Sie im Kontextmenü der neuen Gruppe auf OBJEKTVERWALTUNG ZUWEISEN. Es wird ein Assistent gestartet.
6. Auf der Seite BENUTZER UND GRUPPEN wählen Sie die Personen aus, an die Sie Teile der Verwaltung delegieren möchten. Für bereits in der Liste vorhandene Benutzer und Gruppen können Sie über die Schaltfläche BEARBEITEN die Berechtigungen modifizieren. Allerdings dürfen die Benutzer dazu nicht das Attribut GEERBT tragen. Eigenschaften für die administrative Gruppe werden geerbt, wenn dem Benutzer oder der Gruppe bereits für die übergeordnete Exchange-Organisation eine Berechtigung zur Verwaltung zugewiesen worden ist. Sie können deshalb auch keinen Benutzer hinzufügen, der Mitglied in einer der Gruppen ist, die das Prädikat GEERBT tragen.

   Nachdem Sie über HINZUFÜGEN einen Benutzer ausgewählt haben, können Sie diesem eine der drei folgenden Berechtigungen zuweisen:

   - EXCHANGE-ADMINISTRATOR – VOLLSTÄNDIG: Es ist eine vollständige Administration der Exchange-Systeminformationen sowie von Änderungen der Berechtigungen möglich.
   - EXCHANGE-ADMINISTRATOR: Es ist eine vollständige Administration der Exchange-Systeminformationen möglich.
   - EXCHANGE-ADMINISTRATOR – NUR ANSICHT: Es können nur die Exchange-Konfigurationsinformationen angezeigt werden.
7. Klicken Sie dann auf OK und FERTIG STELLEN, um den Assistenten zu beenden.

4.3 Sicherheitsimplementierung unter Exchange

Dieses Kapitel gibt Ihnen grundlegende Hinweise für die Implementierung und Konfiguration der sicherheitsrelevanten Einstellungen. Sie sollten die in diesem Kapitel beschriebenen Verfahren durchführen, bevor Sie weitere Verwaltungsaufgaben unter Exchange vornehmen.

4.3.1 Berechtigungen unter Exchange

Für das Setzen von Berechtigungen für die Exchange-Objekte sollten Sie den Assistenten für die Zuweisung von Verwaltungsberechtigungen benutzen. Für die Exchange-Objekte Adresslisten, Nachrichtendatenbanken (MDBs) sowie die Strukturen der öffentlichen Ordner können die Berechtigungen einzeln bestimmt werden. Sie können hier sowohl standardmäßige Active Directory-Berechtigungen wie Lesen oder Schreiben als auch erweiterte Exchange-Berechtigungen wie z.B. ÖFFENTLICHE ORDNER ERSTELLEN zuweisen.

Um den Assistenten zu verwenden, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den System-Manager und wählen aus dem Kontextmenü der Organisation oder administrativen Gruppe, die eine Verwaltungsberechtigung erhalten soll, den Eintrag OBJEKTVERWALTUNG ZUWEISEN.
2. Klicken Sie im Assistenten zunächst auf WEITER und klicken unter BENUTZER UND GRUPPEN auf HINZUFÜGEN. Wählen Sie über Durchsuchen den gewünschten Benutzer oder die Gruppe aus.
3. Im Fenster OBJEKTVERWALTUNG ZUWEISEN (siehe Abbildung 4.2) wählen Sie unter FUNKTION eine der folgenden drei Optionen aus:

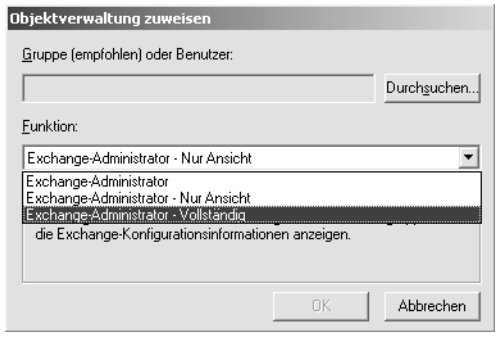


Abbildung 4.2: Zuweisen der Funktion für die Objektverwaltung

- EXCHANGE-ADMINISTRATOR – VOLLSTÄNDIG: Es ist eine vollständige Administration der Exchange-Systeminformationen sowie von Änderungen der Berechtigungen möglich.

- EXCHANGE-ADMINISTRATOR: Es ist eine vollständige Administration der Exchange-Systeminformationen möglich.
- EXCHANGE-ADMINISTRATOR – NUR ANSICHT: Es können nur die Exchange-Konfigurationsinformationen angezeigt werden.

4. Sollen bestehende Berechtigungen für einen Benutzer oder eine Gruppe modifiziert werden, so klicken Sie auf BEARBEITEN. Ebenso können Sie Benutzer und Gruppen über ENTFERNEN aus der Liste löschen.

Um für einzelne Exchange-Objekte die Berechtigungen zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den SYSTEM-MANAGER und wählen aus dem Kontextmenü des zu verwaltenden Objekts den Eintrag EIGENSCHAFTEN.
2. Öffnen Sie die Registerkarte SICHERHEIT und weisen dort dem Benutzer die entsprechenden Berechtigungen zu. Sie finden im oberen Bereich die standardmäßigen Active Directory-Berechtigungen und weiter unten die speziellen Exchange-Berechtigungen. Wählen Sie für jede Berechtigung den Eintrag ZULASSEN oder VERWEIGERN, sofern sich die Einstellung ändern lässt. Über ERWEITERT können Sie die speziellen Berechtigungen konfigurieren.

4.3.2 Authentifizierung am virtuellen Server

Ein virtueller Server unter Exchange ist eine Sammlung von Diensten, die vom Client als ein virtueller Server angesehen werden. Es handelt sich dabei um eine Instanz eines bestimmten Protokolls wie z.B. SMTP oder POP3, die eine definierte Menge von IP-Adressen/Anschlusskombinationen enthält sowie eine Sammlung von Konfigurationseigenschaften. Der virtuelle Server beinhaltet somit sämtliche Ressourcen wie Netzwerkname, IP-Adresse usw., die zum Ausführen einer Anwendung erforderlich sind.

Um zu ermitteln, ob der Benutzer sich unter Exchange 2003 anmelden darf, verwendet der virtuelle Server vier verschiedene Authentifizierungsmethoden. Diese sind:

- Anonymer Zugriff: Ohne Eingabe von Benutzername und Kennwort darf jeder Benutzer auf den virtuellen SMTP- und NNTP-Server zugreifen.
- Standardauthentifizierung: Der Benutzer muss einen Windows-Anmeldenamen und ein Kennwort angeben. Diese Informationen werden unverschlüsselt gesendet. Zur Verschlüsselung auf virtuellen NNTP-, HTTP-, IMAP4- sowie POP3-Servern sollten Sie mit der Standardauthentifizierung SSL (Secure Sockets Layer)/TSL (Transport Layer Security) verwenden.
- Integrierte Windows-Authentifizierung: Diese Authentifizierungsmethode ist für SMTP und NNTP verfügbar. Dabei gibt der Benutzer seinen Windows-Anmeldenamen an. Diese Information wird an den Server weitergegeben, so dass der Benutzer kein Kennwort angeben muss und auch keine unverschlüsselten Daten über das Netzwerk gesendet werden.
- Einfache Authentifizierung und Sicherheitsstufe: Der Benutzername und das Kennwort werden über das NTLM-Sicherheitspaket (NT LAN-Manager) verschlüsselt. Es erfolgt jedoch keine Verschlüsselung der Nachrichtendaten.

Um die Authentifizierung zu konfigurieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den System-Manager und navigieren zu SERVER/SERVERNAME/PROTOKOLLE. Doppelklicken Sie das gewünschte Protokoll und wählen aus dem Kontextmenü von VIRTUELLER STANDARDSERVER den Eintrag EIGENSCHAFTEN.
2. Öffnen Sie die Registerkarte ZUGRIFF und klicken auf AUTHENTIFIZIERUNG (siehe Abbildung 4.3).

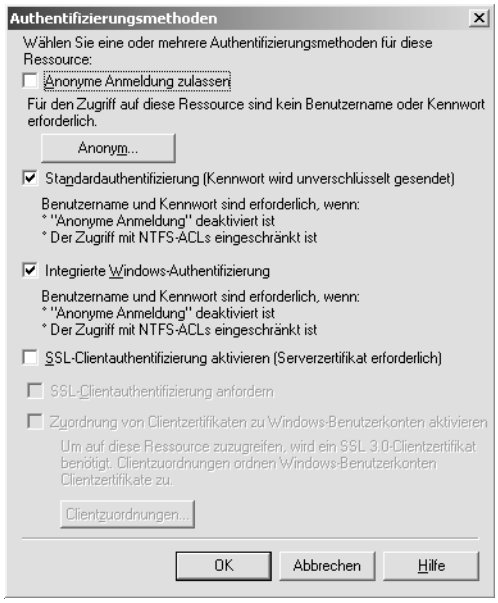


Abbildung 4.3: Die Authentifizierungsmethoden für einen virtuellen Server

Wählen Sie dort die für den jeweiligen virtuellen Server verfügbaren Authentifizierungsmethoden aus. Um die Standardauthentifizierung abzusichern, sollten Sie die Checkbox SSL/TLS-VERSCHLÜSSELUNG ERFORDERLICH aktivieren. Klicken Sie dann auf OK.

Authentifizierung am virtuellen HTTP-Server

Die Authentifizierung am virtuellen HTTP-Server wird nicht wie eben beschrieben über den System-Manager vorgenommen, sondern erfolgt über die mmc Internetinformationsdienste (IIS). Der virtuelle HTTP-Server von Exchange stellt die Standardwebsite des IIS dar. In der IIS-mmc wird dieser virtuelle Server als Standardwebsite angezeigt. Um für diesen virtuellen Server die Authentifizierung einzurichten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der Verwaltung den INTERNETINFORMATIONSDIENSTE-MANAGER. Navigieren Sie dort zu SERVERNAME/WEBSITES/STANDARDWEBSITE.
2. Öffnen Sie die EIGENSCHAFTEN und wechseln auf die Registerkarte VERZEICHNISSICHERHEIT. Klicken Sie unter AUTHENTIFIZIERUNG UND ZUGRIFFSSTEUERUNG auf BEARBEITEN (siehe Abbildung 4.4).

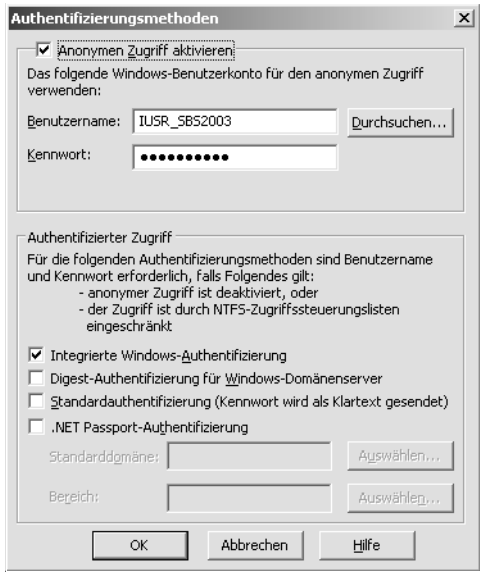


Abbildung 4.4: Die Authentifizierungsmethoden am virtuellen HTTP-Server

3. Markieren Sie unter AUTHENTIFIZIERTER ZUGRIFF die gewünschten Checkboxen der Authentifizierungsmethoden. Neben den beiden bereits beschriebenen Methoden INTEGRIERTE WINDOWS-AUTHENTIFIZIERUNG und STANDARDAUTHENTIFIZIERUNG können Sie auch die Optionen DIGEST-AUTHENTIFIZIERUNG FÜR WINDOWS-DOMÄNENSERVER sowie .NET PASSPORT-AUTHENTIFIZIERUNG wählen.
   - Digest-Authentifizierung für Windows-Domänenserver: Diese Methode entspricht der Standardauthentifizierung, jedoch wird dabei ein Herausforderungs-/Rückmeldemechanismus für die Benutzerauthentifizierung am Server benutzt. Das Kennwort wird nicht an den Server gesendet.
   - .NET Passport-Authentifizierung: Die Authentifizierung erfolgt mit Hilfe eines .NET Passport-Kontos.

   Um den anonymen Zugriff zuzulassen, markieren Sie die Checkbox ANONYMEN ZUGRIFF AKTIVIEREN und wählen ein Benutzerkonto für den Zugriff aus.

4.3.3 Verbindungen mit virtuellen Servern überwachen

Zusätzlich zur Wahl der Authentifizierung können Sie zur Erhöhung der Sicherheit auch bestimmten Computern, Subnetzbereichen oder Domänen den Zugriff auf einen bestimmten virtuellen Server gestatten oder verweigern. Standardmäßig ist der Zugriff für jeden Computer gestattet. Um dies zu ändern, führen Sie die folgenden Schritte durch:

1. Öffnen Sie im System-Manager den gewünschten virtuellen Server. Öffnen Sie dessen EIGENSCHAFTEN und wechseln auf die Registerkarte ZUGRIFF.
2. Klicken Sie im Bereich VERBINDUNGSKONTROLLE auf VERBINDUNG (siehe Abbildung 4.5).

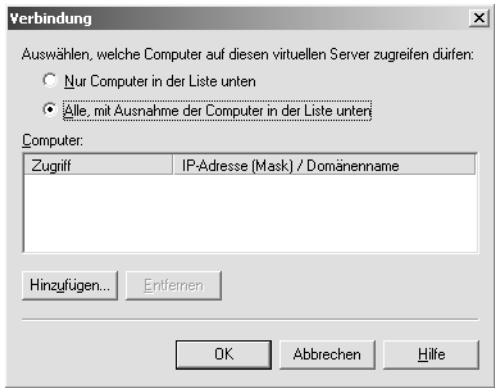


Abbildung 4.5: Die Verbindungsüberwachung zum virtuellen Server

Sie können entweder die Option NUR COMPUTER IN DER LISTE UNTEN wählen. Hierzu müssen Sie über HINZUFÜGEN die gewünschten Computer auswählen. Oder aber Sie wählen die Option ALLE, MT AUSNAHME DER COMPUTER IN DER LISTE UNTEN. Auch in diesem Fall können Sie über HINZUFÜGEN eine Auswahl vornehmen. Beim Hinzufügen können Sie wählen EINZELNER COMPUTER und dessen IP-Adresse angeben, GRUPPE VON COMPUTERN und das Subnetz angeben oder DOMÄNE und deren Namen eintragen. Möchten Sie einen Computer hinzufügen, dessen Namen, nicht aber IP-Adresse Sie kennen, so klicken Sie auf DNS-LOOKUP. Klicken Sie dann auf OK.

Verbindung des virtuellen HTTP-Servers überwachen

Wie bereits im letzten Kapitel beschrieben, wird auch die Verbindungsüberwachung des virtuellen HTTP-Servers über die Konsole Internetinformationsdienste-Manager realisiert.

1. Öffnen Sie in der Verwaltung den INTERNETINFORMATIONSDIENSTE-MANAGER. Navigieren Sie dort zu SERVERNAME/WEBSITES/STANDARDWEBSITE.
2. Öffnen Sie die EIGENSCHAFTEN und wechseln auf die Registerkarte VERZEICHNISSICHERHEIT. Klicken Sie unter BESCHRÄNKUNGEN FÜR IP-ADRESSEN UND DOMÄNENNAMEN auf BEARBEITEN.
3. Wählen Sie dort die Option ZUGRIFF GEWÄHRT oder ZUGRIFF VERWEIGERT und tragen über HINZUFÜGEN die einen einzelnen Computer, eine Gruppe von Computern oder einen Domänennamen ein. Klicken Sie dann auf OK.

4.3.4 Protokollierung für das SMTP-, NNTP- und HTTP-Protokoll aktivieren

Für die Internetprotokolle SMTP, NNTP sowie HTTP können Sie sämtliche Befehle protokollieren, die der jeweilige virtuelle Server erhält. Es werden dabei die folgenden Inhalte protokolliert: IP-Adresse und Name des Clients, Datum und Uhrzeit der E-Mail sowie die Größe der gesendeten Bytes. Diese Einträge finden Sie nach Aktivieren der Protokollierung im Ereignisprotokoll. Aus Sicherheitsgründen sollten Sie die Protokollierung aktivieren.

1. Öffnen Sie den System-Manager und navigieren zum virtuellen Server SMTP oder NNTP. Öffnen Sie die EIGENSCHAFTEN und danach die Registerkarte ALLGEMEIN.
2. Markieren Sie dort die Checkbox PROTOKOLLIERUNG AKTIVIEREN. Für SMTP ist das standardmäßige Protokollformat W3C-ERWEITERT, für NNTP MICROSOFT IIS (siehe Abbildung 4.6).

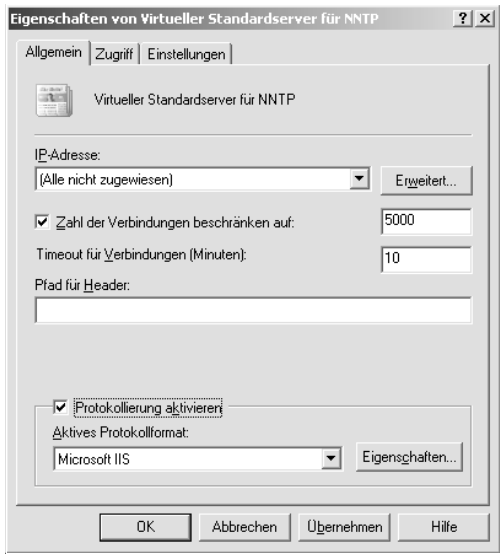


Abbildung 4.6: Die Protokollierungsfunktion für den virtuellen NNTP-Server

Über ERWEITERT können Sie im Fenster PROTOKOLLIERUNGSEIGENSCHAFTEN das Verzeichnis für die Protokolldatei sowie den Protokollzeitplan auswählen. Auf der Registerkarte ERWEITERT können Sie die zu protokollierenden Optionen auswählen wie z.B. Server-IP-Adresse, Protokollversion oder Cookies. Klicken Sie dann auf OK.

Die Protokollierung für das HTTP-Protokoll wird wiederum über die IIS-mmc vorgenommen.

1. Öffnen Sie wie weiter oben beschrieben die EIGENSCHAFTEN der STANDARDWEBSITE und wechseln auf die Registerkarte WEBSITE.
2. Markieren Sie dort die Checkbox PROTOKOLLIERUNG AKTIVIEREN und wählen ein Protokollformat. Die Protokolloptionen werden wie bei dem SMTP- und NNTP-Protokoll eingestellt.

4.4 Konfiguration des Exchange Servers

Um den Exchange Server zu konfigurieren, navigieren Sie im System-Manager zum Container SERVER und öffnen über das Kontextmenü des Servers dessen EIGENSCHAFTEN.

Auf der Registerkarte ALLGEMEIN sehen Sie zunächst die Version des Servers (siehe Abbildung 4.7). Die Version 6.5 steht dabei für Exchange 2003. Die Build-Nummer gibt den Patch-Level, also das installierte Service Pack des Servers an.

Noch ein kurzes Wort zum Service Pack für den Exchange Server: Für den „herkömmlichen" Exchange Server 2003 wurde bereits das Service Pack 1 veröffentlicht. Dieses lässt sich theoretisch auch für den Exchange Server des SBS installieren, es kann dabei jedoch später zu Problemen kommen. Trotz widersprüchlicher Angaben und Aussagen zur Funktionsweise des Service Packs sei an dieser Stelle von der Installation abgeraten.

4.4.1 Protokollierung

Die beiden Checkboxen NACHRICHTENBETREFF PROTOKOLLIEREN UND ANZEIGEN sowie NACHRICHTENTRACKING AKTIVIEREN stehen für die Funktion des Exchange Servers, innerhalb der Exchange-Organisation den Weg der Nachrichten nachzuvollziehen (siehe Abbildung 4.7). Besonders sinnvoll ist diese Option, um herauszufinden, an welchen Stellen es zu Problemen bei der E-Mail-Übertragung kommt.

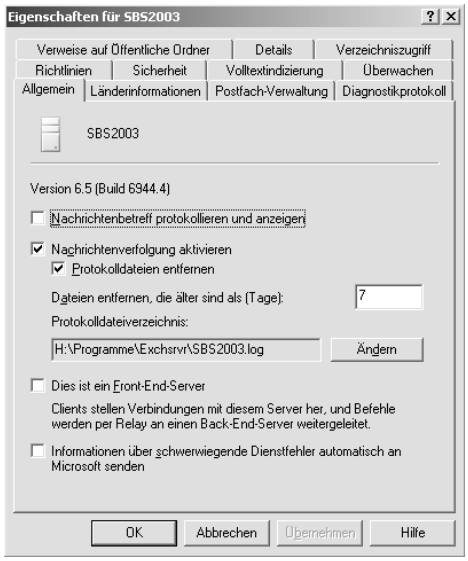


Abbildung 4.7: Die Protokollierung der E-Mail-Übertragung

Aktivieren Sie zunächst die Checkbox NACHRICHTENTRACKING AKTIVIEREN, um die Protokollierung generell zu aktivieren. Möchten Sie noch weitere Informationen sammeln, so aktivieren Sie zusätzlich noch die Checkbox NACHRICHTENBETREFF PROTOKOLLIEREN UND ANZEIGEN.

Bedenken Sie jedoch, dass die auf dem Exchange Server aktivierte Protokollierung zu Lasten der Performance des Servers geht. Besonders im Umfeld des SBS 2003 kann sich dies sehr negativ auswirken, da ja der Exchange Server hier auf demselben Server installiert sein muss wie das Betriebssystem und die weiteren SBS 2003-Serverkomponenten. Aktivieren Sie die Protokollierung also nur, wenn Sie ein bestimmtes Problem analysieren möchten.

Da auch der Umfang des Protokolls schnell auf einige Megabyte anwachsen kann, sollten Sie die Checkbox PROTOKOLLDATEIEN ENTFERNEN markieren und einen Wert wählen, nach dessen Ablauf in Tagen die Protokolldateien automatisch gelöscht werden sollen. Unter PROTOKOLLDATEIVERZEICHNIS können Sie auch den SPEICHERORT für die Protokolldateien festlegen.

Die Checkbox DIES IST EIN FRONT-END-SERVER ist eher in größeren Umgebungen interessant. Ein Front-End-Server dient quasi als Proxy-Server und leitet sämtliche E-Mail-Anfragen an die jeweiligen Back-End-Server weiter. Der Front-End-Server selbst stellt keine Informationen mehr bereit, sondern leitet die Anfragen nur weiter. Für dieses Szenario müssten also mindestens zwei Exchange Server vorhanden sein.

Auf der Registerkarte DIAGNOSTIKPROTOKOLL können Sie festlegen, für welche Exchange-Dienste eine Protokollierung erfolgen soll. Wählen Sie dazu unter DIENSTE den gewünschten Dienst. Unter KATEGORIE können Sie für jede Kategorie des Dienstes einen Protokollierungsgrad von KEINE, MINIMUM, MITTEL oder MAXIMUM bestimmen.

4.4.2 Spracheinstellungen

Über die Registerkarte LÄNDERINFORMATIONEN wird die Sprachunterstützung für die Outlook-Clients konfiguriert. Damit ein Benutzer des Outlook-Clients alle Informationen gemäß seiner Outlook-Spracheinstellung erhält, müssen Sie die vorhandenen Sprachen auf dem Exchange Server hinzufügen. Standardmäßig ist nur die Länderinformation DEUTSCH (DEUTSCHLAND) vorhanden. Nachdem Sie neue Länderinformationen hinzugefügt haben, müssen die entsprechenden Codeseiten für die Unterstützung länderspezifischer Formate manuell auf dem Server installiert werden. Danach ist ein Neustart des Systems erforderlich.

4.4.3 Postfach-Verwaltung

Auf der Registerkarte POSTFACH-VERWALTUNG können Sie bestimmen, wann die Postfächer nach alten Daten durchsucht werden sollen, die gelöscht werden sollen.

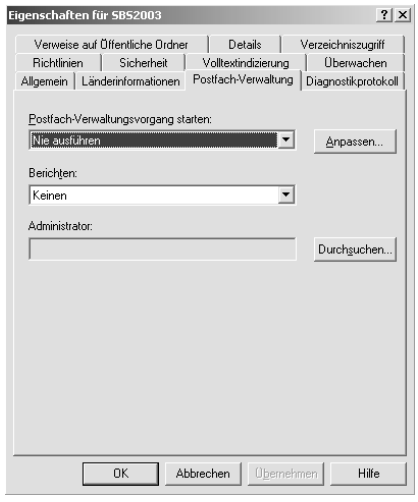


Abbildung 4.8: Die Postfach-Verwaltung

Unter POSTFACH-VERWALTUNGSVORGANG STARTEN können Sie entweder die Optionen FREITAGS UM MITTERNACHT AUSFÜHREN (bzw. Samstag oder Sonntag) oder einen benutzerdefinierten Zeitplan erstellen. Möchten Sie über den Verwaltungsvorgang nähere Details erhalten, so wählen Sie unter BERICHTEN die Option ZUSAMMENFASSUNGSBERICHT AN ADMINISTRATOR SENDEN oder DETAILBERICHT AN ADMINISTRATOR SENDEN. Unter ADMINISTRATOR können Sie den Benutzer auswählen, der die Berichte erhalten soll.

4.4.4 Volltextindizierung

Die Registerkarte VOLLTEXTINDIZIERUNG regelt die Ressourcenauslastung des Exchange Servers für das Durchsuchen des Informationsspeichers und das Erstellen von Indexdateien. Dadurch wird die Suche beschleunigt. Für die SYSTEMRESSOURCENAUSLASTUNG können Sie die Level MINIMUM, NIEDRIG, MITTEL oder MAXIMUM wählen. Bedenken Sie bei der Auswahl, dass der Server durch die Indizierung nicht so stark ausgelastet wird, dass er nicht mehr seinen herkömmlichen Aufgaben nachkommen kann.

4.4.5 Überwachung

Unter ÜBERWACHUNG können Sie festlegen, welche Dienste des Exchange Servers überwacht werden sollen. Standardmäßig sind nur die Exchange-Dienste eingetragen, wenn Sie unter NAME auf MICROSOFT EXCHANGE-STANDARDDIENSTE klicken. Weiterhin können Sie auch die Überwachung für einige Hardwarekomponenten sowie Connectoren aktivieren. Klicken Sie auf HINZUFÜGEN, um die folgenden Komponenten ebenfalls zu überwachen (siehe Abbildung 4.9):

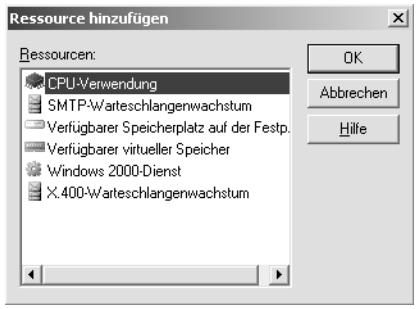


Abbildung 4.9: Auswahl der zu überwachenden Komponente

- CPU-VERWENDUNG: Eine wenig ausgelastete CPU garantiert schnelle Antwortzeiten.
- SMTP-WARTESCHLANGENWACHSTUM: Bei Netzwerkproblemen sollte es nicht zum Überlaufen der Warteschlange kommen.
- VERFÜGBARER SPEICHERPLATZ AUF DER FESTPLATTE: Für eine Auslagerung im Notfall sollte immer genügend Platz zur Verfügung stehen.

- VERFÜGBARER VIRTUELLER SPEICHER: Je mehr Speicher verfügbar ist, desto besser ist die Leistung des Servers.
- WINDOWS 2000-DIENST: Wählen Sie hier die zu überwachenden Dienste aus. Bedenken Sie aber, nur die Dienste zu wählen, deren Überwachung sinnvoll ist.
- X.400-WARTESCHLANGENWACHSTUM: Wie bei der SMTP-Warteschlange sollte auch hier ein Überlaufen unterbunden werden.

Neue Überwachungsrichtlinien erstellen

Um auf dem Exchange Server eine neue Überwachungsrichtlinie zu erstellen, klicken Sie auf der Registerkarte ÜBERWACHEN auf HINZUFÜGEN und wählen eine der eben genannten sechs verfügbaren Komponenten aus. Für jede Komponente erhalten Sie ein separates Fenster mit den individuellen Überwachungsoptionen.

Wählen Sie beispielsweise die CPU-VERWENDUNG aus (siehe Abbildung 4.10), können Sie zunächst unter DAUER die Anzahl der Minuten festlegen, für die der gewählte Zustand vorliegen muss. Unter WARNZUSTAND und KRITISCHER ZUSTAND bestimmen Sie in Prozent die Prozessorauslastung. Klicken Sie dann auf OK.

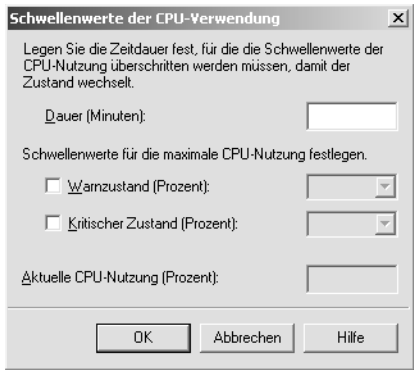


Abbildung 4.10: Konfiguration der CPU-Überwachung

Für die anderen Komponenten ist die Konfiguration der Werte entsprechend analog und selbsterklärend.

Um die konfigurierten Werte später zu ändern, markieren Sie die Komponente und klicken auf DETAILS. Weiterhin können überwachte Komponenten später über ENTFERNEN wieder gelöscht werden.

Klicken Sie auf MICROSOFT EXCHANGE-STANDARDDIENSTE (siehe Abbildung 4.11), so sehen Sie eine Liste der Exchange-Dienste.

Sobald einer dieser Dienste nicht mehr ausgeführt wird, wird der Zustand wahlweise auf WARNUNG oder KRITISCH gesetzt.

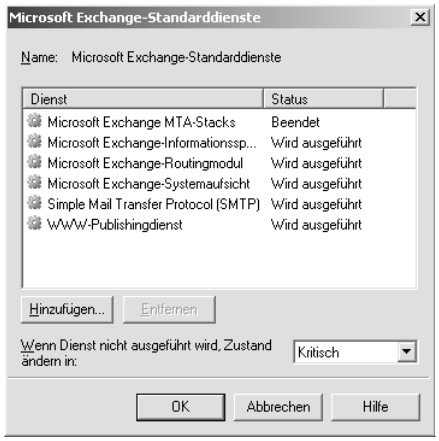


Abbildung 4.11: Status der Exchange-Standarddienste

Überwachungsbenachrichtigungen empfangen

Sobald auf dem Server eine Warnung oder ein kritischer Zustand auftritt, können Sie sich darüber informieren lassen. So sind Sie jedes Mal darüber informiert, wenn beispielsweise ein Dienst wiederholt abstürzt und dabei möglicherweise den Informationsspeicher beschädigen kann. Anderenfalls besteht die Gefahr, dass das wiederholte Abstürzen unbemerkt bleibt, wenn der Dienst wieder verfügbar ist, sobald ein Benutzer darauf zugreift.

Für die Konfiguration der Benachrichtigung führen Sie die folgenden Schritte aus:

1. Navigieren Sie im System-Manager zu EXTRAS/ÜBERWACHUNG UND STATUS/BENACHRICHTIGUNGEN und wählen aus dem Kontextmenü NEU/E-MAIL-BENACHRICHTIGUNG.

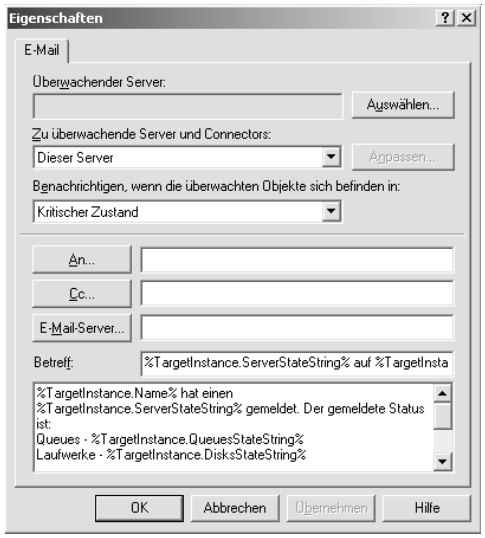


Abbildung 4.12: Konfiguration der E-Mail-Benachrichtigung

2. Im Feld ÜBERWACHENDER SERVER (siehe Abbildung 4.12) ist standardmäßig der Name des lokalen Mailservers eingetragen, von dem aus Sie den System-Manager starten. Sie können jedoch auch einen anderen Server auswählen. Unter ZU ÜBERWACHENDE SERVER UND CONNECTORS können Sie wählen, welche Server und/oder Connectoren in die Benachrichtigung mit einbezogen werden sollen. Weiterhin wählen Sie aus, ob die Benachrichtigung erfolgen soll, wenn sich die überwachten Objekte im WARNZUSTAND oder KRITISCHEN ZUSTAND befinden. Abschließend tragen Sie in die entsprechenden Felder die E-Mail-Adressen der Personen ein, welche die Warnungsbenachrichtigungen erhalten sollen.

   Neben der E-Mail-Benachrichtigung können Sie auch eine Skriptbenachrichtigung erstellen.

1. Öffnen Sie wie eben beschrieben den Pfad im System-Manager und wählen NEU/SKRIPTBENACHRICHTIGUNG.
2. Nehmen Sie dort wie eben beschrieben die Konfiguration vor.
3. Geben Sie unter PFAD FÜR PROGRAMMDATEI (siehe Abbildung 4.13) an, wo sich das auszuführende Skript befindet. Anstelle eines Skripts können Sie auch ein beliebiges Programm ausführen lassen. Optional können Sie unter BEFEHLSZEILENOPTIONEN noch Parameter für das Starten des Skripts oder Programms hinterlegen.

Abbildung 4.13: Konfiguration der Skriptbenachrichtigung

Beispielsweise können Sie beim Ausfall eines Dienstes via Skript den Neustart des Dienstes veranlassen und gleichzeitig dem Administrator eine Meldung schicken. Ein Beispielskript dazu kann folgendermaßen aussehen:

```
Net start pop3svc
If errorlevel 1
Net send Administrator Beim Starten des POP3-Servers ist ein Fehler
aufgetreten
```

Listing 4.1: Beispiel für eine Skriptbenachrichtigung

4.4.6 Serverrichtlinien unter Exchange

Der eigentliche Zweck für die Konfiguration von Serverrichtlinien ist die vereinfachte Steuerung von mehreren Exchange Servern. Im SBS 2003-Umfeld wird zwar in aller Regel nur ein Exchange Server eingesetzt werden, dennoch wird hier aber kurz auf die Richtlinien eingegangen.

Im Gegensatz zu den Gruppenrichtlinien des Active Directory wird durch das Anwenden einer Exchange-Serverrichtlinie die Eigenschaft eines Objekts endgültig überschrieben. Dies bedeutet, dass der ursprüngliche Wert der Eigenschaft auch dann nicht mehr wiederhergestellt werden kann, wenn die Serverrichtlinie wieder aufgehoben wird. Bei einer Gruppenrichtlinie des Active Directory hingegen wird die Eigenschaft nur so lange beeinflusst, wie die Richtlinie angewendet wird. Sobald die Gruppenrichtlinie wieder entfernt wird, gilt wieder der ursprüngliche Wert der Eigenschaft.

Um eine Exchange-Serverrichtlinie zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie im System-Manager zur EXCHANGE-ORGANISATION/ADMINISTRATIVE GRUPPEN. Aus dem Kontextmenü der gewünschten administrativen Gruppe wählen Sie den Eintrag NEU/SYSTEMRICHTLINIENCONTAINER.

Der Container ADMINISTRATIVE GRUPPEN ist standardmäßig nicht vorhanden. Das Anlegen einer neuen administrativen Gruppe wurde bereits in Kapitel Abbildung 4.2.2 abgehandelt.

2. Ein Name für den Container kann nicht gewählt werden, da immer der Name SYSTEMRICHTLINIEN gesetzt wird. Dieser Ordner kann auch später nicht umbenannt werden. Innerhalb einer administrativen Gruppe kann sich immer nur ein Ordner Systemrichtlinien befinden.
3. Zum Erstellen einer Serverrichtlinie wählen Sie aus dem Container SYSTEMRICHTLINIE den Eintrag NEU/SERVERRICHTLINIE.

4.4.7 Weitere Einstellungen

Auf der Registerkarte RICHTLINIEN erfahren Sie, welche Richtlinien auf den Server angewendet werden. Um die Richtlinien zu bearbeiten, müssen Sie jedoch die Richtlinien über die Sicherheitsrichtlinien und Gruppenrichtlinien in der Programmgruppe VERWALTUNG modifizieren.

Über die Registerkarte SICHERHEIT können Sie die für die einzelnen Benutzer und Gruppen konfigurierten Berechtigungen einsehen und ändern.

4.5 Die E-Mail-Verwaltung

Im Folgenden finden Sie eine Übersicht über die grundlegenden Verwaltungsaufgaben rund um den E-Mail-Verkehr. Dazu zählen das Erstellen von Verteilergruppen, eines Zeitplans für das Abrufen von E-Mails, Hinzufügen von Connectoren oder das Synchronisieren von E-Mails.

4.5.1 Das Einrichten von Postfächern

Ein Postfach für einen Benutzer wird automatisch im Active Directory erstellt, wenn Sie einen neuen Benutzer anlegen. Standardmäßig befinden sich sämtliche SBS-Benutzer in der Organisationseinheit (OU) MYBUSINESS/USERS/SBSUSERS der Domäne. Um dort oder in einer anderen OU einen neuen Benutzer anzulegen, wählen Sie aus dem Kontextmenü der OU NEU/BENUTZER. Zum Anlegen eines Postfachs führen Sie die folgenden Schritte durch:

1. Geben Sie für den Benutzer zunächst den Namen sowie Anmeldenamen an. Klicken Sie dann auf WEITER. Danach werden das Kennwort sowie die Kennwortoptionen für den Benutzer bestimmt. Klicken Sie abermals auf WEITER.
2. Im folgenden Fenster (siehe Abbildung 4.14) müssen Sie sicherstellen, dass die Checkbox EXCHANGE-POSTFACH ERSTELLEN markiert ist.

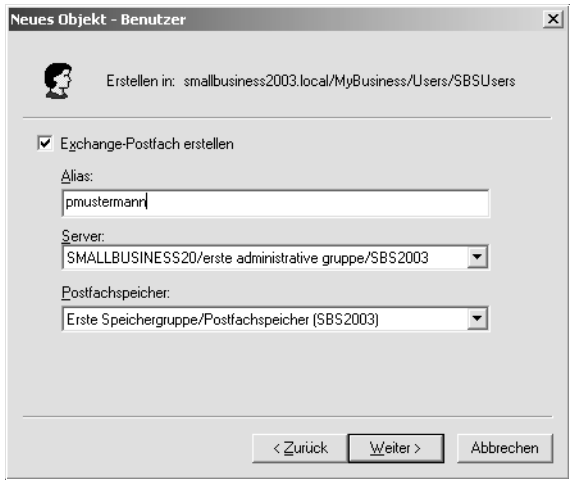


Abbildung 4.14: Das Exchange-Postfach für einen neuen Benutzer anlegen

Unter ALIAS wird das Mailalias des Benutzers eingetragen. Dieses wird für die Identifikation des Benutzers am Exchange Server benutzt. Idealerweise verwenden Sie als Alias den Benutzeranmeldenamen. Unter SERVER wird der Exchange Server eingetragen, auf dem das Benutzerpostfach gespeichert wird. Sofern mehrere Server verfügbar sind, können Sie einen aus der Drop-down-Liste auswählen. Der POSTFACHSPEICHER gibt den Speicherort auf dem gewählten Exchange Server an.

3. Klicken Sie dann auf WEITER und FERTIG STELLEN, um das Exchange-Postfach für den neuen Benutzer anzulegen.

4.5.2 Bearbeiten des Postfachs

Nachdem Sie einen Benutzer angelegt haben, können Sie dieses bearbeiten. Wählen Sie dazu aus dem Kontextmenü des Benutzers den Eintrag EXCHANGE-AUFGABEN. Es wird ein Assistent gestartet.

Auf der Seite VERFÜGBARE AUFGABEN (siehe Abbildung 4.15) können Sie vier verschiedene Aufgaben am Postfach durchführen. Markieren Sie jeweils die gewünschte Aufgabe und klicken auf WEITER.

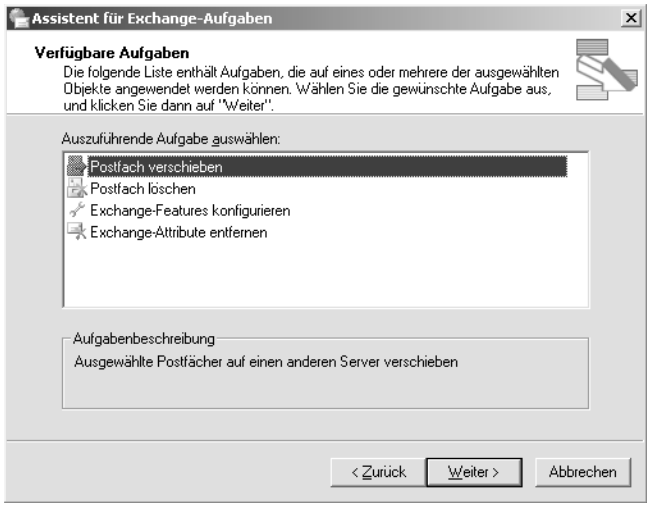


Abbildung 4.15: Bearbeiten der Postfach-Optionen

- POSTFACH VERSCHIEBEN: Das Postfach des Benutzers wird auf einen anderen Exchange Server verschoben. Im SBS-Umfeld wird dies in der Regel nicht der Fall sein.
- POSTFACH LÖSCHEN: Das Postfach des Benutzers wird gelöscht.
- EXCHANGE-FEATURES KONFIGURIEREN:
- EXCHANGE-ATTRIBUTE ENTFERNEN:

4.5.3 Erstellen von Verteilergruppen

Bei einer Verteilergruppe handelt es sich nicht um eine Benutzergruppe, der bestimmte Berechtigungen zugewiesen werden können, sondern um eine Gruppe, deren Mitglieder für den Empfang bestimmter E-Mails zusammengefasst werden. Einer Verteilergruppe können keine Benutzer- oder Dateirechte gegeben werden.

1. Um eine neue Verteilergruppe zu erstellen, öffnen Sie die Serververwaltung und wählen aus dem Kontextmenü von VERTEILERGRUPPEN den Eintrag VERTEILERGRUPPE HINZUFÜGEN.
2. Geben Sie der neuen Verteilergruppe einen NAMEN, eine BESCHREIBUNG sowie ein E-MAIL-ALIAS. Klicken Sie dann auf WEITER.
3. Im Fenster GRUPPENMITGLIEDSCHAFT wählen Sie die Benutzer und/oder Benutzergruppen aus, die Mitglied der neuen Verteilergruppe werden sollen. Klicken Sie dann auf WEITER.

4. Im Fenster GRUPPEN-MANAGER können Sie aus der Liste VORGESETZTE(R) einen Benutzer oder eine Gruppe auswählen. Dieser Benutzer hat später die Möglichkeit, weitere Mitglieder zu der Verteilergruppe hinzuzufügen. Dieses kann er später über Outlook 2003 ausführen. Bei dem Vorgesetzten muss es sich um eine Person oder Gruppe handeln, die Mitglied der Verteilerliste ist. Sie müssen jedoch keinen Vorgesetzten auswählen. In diesem Fall kann zu einem späteren Zeitpunkt lediglich ein Administrator die Gruppenmitgliedschaften bearbeiten. Klicken Sie dann auf WEITER.
5. Im Fenster GRUPPENOPTIONEN bestimmen Sie, ob die Verteilergruppe Internet-E-Mails empfangen darf und ob diese archiviert werden sollen. Um den Empfang von Internet-E-Mail zu gestatten, aktivieren Sie die Checkbox DIESER GRUPPE ERMÖGLICHEN, E-MAIL-NACHRICHTEN VON BENUTZERN AUSSERHALB DES NETZWERKS ZU EMPFANGEN. Deaktivieren Sie die Checkbox, wenn es sich um eine interne Verteilergruppe handelt. Dadurch wird das Risiko von Viren in den E-Mails sowie von unerwünschten E-Mails reduziert. Über die Checkbox ÖFFENTLICHEN ORDNER ZUM ARCHIVIEREN DER AN DIESE GRUPPE GESENDETEN E-MAIL-NACHRICHTEN ERSTELLEN bestimmen Sie, dass für die Gruppe ein Ordner mit dem Namen GRUPPENNAME-ARCHIV unter den öffentlichen Ordnern erstellt wird. In diesem Ordner werden Kopien aller an die Gruppe verschickten E-Mails gespeichert. Klicken Sie auf WEITER und beenden den Assistenten.

4.5.4 Verteilergruppen über Outlook 2003 erstellen

Sofern Sie unter Schritt 4 einen Personalvorgesetzten der Verteilergruppe bestimmt haben, kann dieser die Mitgliedschaftsliste der Verteilergruppe bearbeiten. Jedoch erfolgt dieser Vorgang nicht über die Serververwaltung, sondern über seine lokale Kopie von Outlook 2003. Weiterhin kann auch ein Administrator über Outlook 2003 neue Verteilergruppen erstellen.

1. Klicken Sie unter Outlook 2003 auf DATEI/NEU/VERTEILERLISTE. Geben Sie unter NAME einen Namen für die Gruppe ein.
2. Klicken Sie dann auf MITGLIEDER AUSWÄHLEN, um Benutzer aus einem Adressbuch hinzuzufügen. Im Fenster NAMEN AUS FOLGENDEM ADRESSBUCH ANZEIGEN können Sie zwischen verschiedenen Adressbüchern wählen. Über NEU HINZUFÜGEN können Sie auch Mitglieder zur Verteilergruppe hinzufügen, die nicht in einem Adressbuch vorhanden sind.
3. Um die Gruppe zu erstellen, klicken Sie auf SPEICHERN UND SCHLIESSEN. Die Verteilergruppe ist unter Outlook im Ordner KONTAKTE gespeichert.

Sie haben auch nach Erstellung der Verteilergruppe die Möglichkeit, der Gruppe einen Vorgesetzten zuzuweisen, der diese Gruppe verwalten darf.

1. Öffnen Sie in der Serververwaltung die EIGENSCHAFTEN der gewünschten Verteilergruppe und wechseln auf die Registerkarte VERWALTET VON.
2. Klicken Sie auf ÄNDERN und tragen den Benutzernamen ein. Dieser Benutzer kann nun die Verteilergruppe verwalten.

4.5.5 Zeitplan für die E-Mail-Zustellung

Sie können für den Exchange Server einen Zeitplan bestimmen, gemäß dem die E-Mails abgerufen und empfangen werden sollen. Dieser Zeitplan wird über den Assistenten VERBINDUNG MIT DEM INTERNET HERSTELLEN in der Aufgabenliste in der Serververwaltung erstellt und ist selbsterklärend.

4.5.6 Bearbeiten der Postfach-Größenbeschränkungen

Wenn bei einem Benutzer wiederholt das Problem auftritt, dass er keine E-Mails senden und empfangen kann, weil er die Größenbeschränkung für sein Postfach überschritten hat, sollten Sie für ihn dieses Limit heraufsetzen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die SERVERVERWALTUNG und dort den Eintrag BENUTZER.
2. Wählen Sie aus dem Kontextmenü des betreffenden Benutzerkontos den Eintrag EIGENSCHAFTEN.
3. Im Eigenschaftsfenster des Benutzers wechseln Sie auf die Registerkarte EXCHANGE – ALLGEMEIN und klicken auf SPEICHERGRENZWERTE. Sie erhalten das Fenster SPEICHERGRENZWERTE (siehe Abbildung 4.16).

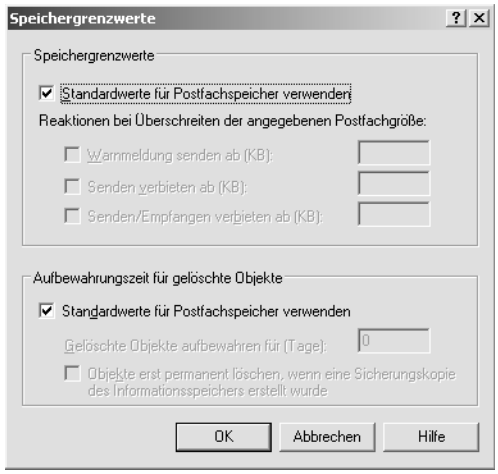


Abbildung 4.16: Die Grenzwerte für den Postfachspeicher festlegen

4. Deaktivieren Sie dort die Checkbox STANDARDWERTE FÜR POSTFACHSPEICHER VERWENDEN. Danach können Sie einige oder alle Werte für die Einträge WARNMELDUNGEN SENDEN AB (KB), SENDEN VERBIETEN AB (KB) sowie SENDEN/EMPFANGEN VERBIETEN AB (KB) festlegen. Bestätigen Sie mit OK.

4.6 Der POP3-Connector und SMTP-Connector

Bei der Installation des SBS werden standardmäßig der POP3-Connector und der SMTP-Connector installiert. Ein Connector hat die Aufgabe, zwischen zwei E-Mail-Systemen den Fluss der Nachrichten sicherzustellen. Der POP3-Connector ist dabei zuständig für den Nachrichtenaustausch von POP3-E-Mail-Systemen, der SMTP-Connector für den Austausch zwischen Exchange-Systemen. Der SMTP-Connector spielt im SBS 2003-Umfeld eher eine untergeordnete Rolle, da für dessen Einsatz mehrere Exchange Server innerhalb der Exchange-Organisation vorhanden sein müssten.

Wesentlich interessanter ist der POP3-Connector. Mit Hilfe des POP3-Connectors können Sie aus externen POP3-Postfächern die Nachrichten abrufen und diese dann an die Benutzerpostfächer unter Exchange verteilen. Dabei führt der Connector den Download der E-Mails vom POP3-Postfach durch und sendet diese neu an das Exchange-Postfach. Damit dieses funktioniert, muss der Benutzername des POP3-Postfachs entweder für ein einzelnes Exchange-Postfach oder für eine Verteilergruppe zugeordnet sein.

Zusätzlich zum Weiterleiten an ein Benutzerpostfach beherrscht der POP3-Connector auch das Weiterleiten an ein globales Postfach. Bei einem globalen Postfach wird dieses für den Empfang sämtlicher E-Mails verwendet, die an die Domäne gerichtet sind. So landen dort sämtliche E-Mails wie z.B. info@firma.de, pmustermann@firma.de oder webmaster@firma.de. Beim Download der E-Mails überprüft der POP3-Connector die Zeilen An sowie Cc und leitet die Nachrichten aufgrund dieser Informationen an die Benutzerpostfächer bzw. Verteilergruppen weiter.

Beachten Sie jedoch, dass bei einem globalen Postfach nicht die Empfänger der Zeile Bcc (Blind Carbon Copy) ausgelesen werden können. Die Original-Bcc-E-Mail wird an das Postfach gesendet, das sämtliche E-Mails empfängt, die für die Domäne nicht zugestellt werden können. Standardmäßig handelt es sich dabei um das Postfach des Administrators.

4.6.1 Konfiguration des POP3-Connectors

Um den POP3-Connector zu konfigurieren, klicken Sie in der Serververwaltung auf INTERNET UND E-MAIL und POP3-E-MAIL VERWALTEN. Dort klicken Sie auf POP3-CONNECTOR-MANAGER öffnen.

Um ein neues POP3-Konto zu erstellen, klicken Sie auf HINZUFÜGEN. Sie benötigen nun die folgenden Informationen: Benutzername und Kennwort für das Konto, Name des POP3-Servers und die Information, ob eine sichere Kennwortauthentifizierung (SPA) erforderlich ist. Dann bestimmen Sie, ob es sich um ein Benutzerpostfach oder ein globales Postfach handelt, und geben das Exchange-Postfach an, an das die E-Mails weitergeleitet werden sollen. Klicken Sie dann auf OK.

Weiterhin können Sie globale Optionen für den POP3-Connector festlegen. Auf der Registerkarte ZEITPLANERSTELLUNG legen Sie fest, in welchem Intervall die E-Mails von den POP3-Postfächern abgerufen werden sollen. Hierzu gibt es bereits vordefinierte Zeitpläne, Sie können jedoch auch selbst einen Plan erstellen. Zusätzlich können Sie über JETZT ABRUFEN auch das sofortige, außerplanmäßige Abrufen durchführen.

Auf der Registerkarte PROBLEMBEHANDLUNG sehen Sie eine Übersicht über den Dienststatus sowie die Anzahl der fehlgeschlagenen E-Mails. Unter DIENSTPROTOKOLLIERUNG können Sie festlegen, in welcher Detailstufe (Minimal, Mittel, Maximal, Keine) Einträge im Anwendungsprotokoll vorgenommen werden sollen. Schließlich können Sie unter UNZUSTELLBARE POP3-E-MAIL noch das Postfach angeben, an das sämtliche E-Mails gesendet werden sollen, die an kein gültiges Benutzerpostfach weitergeleitet werden können.

4.6.2 Hinzufügen weiterer Connectoren

Neben den beiden standardmäßig installierten Connectoren können Sie noch weitere nachträglich installieren. Führen Sie dazu die folgenden Schritte aus:

1. Legen Sie die CD 2 des SBS 2003 ein und klicken die Datei *Setup.exe* im Verzeichnis EXCHSRVR65\SETUP\I386 doppelt.
2. Im Installationsassistenten klicken Sie auf WEITER, stimmen dem Lizenzvertrag zu und geben die Lizenznummer ein. Im Fenster KOMPONENTENAUSWAHL klicken Sie in der Spalte MICROSOFT EXCHANGE unter AKTION auf den Pfeil und danach auf ÄNDERN.
3. Unter Microsoft Exchange-Dienste für Messaging und Collaboration können Sie die folgenden drei zusätzlichen Connectoren auswählen:
   - MICROSOFT EXCHANGE CONNECTOR FÜR LOTUS NOTES
   - MICROSOFT EXCHANGE CONNECTOR FÜR NOVELL GROUPWISE
   - MICROSOFT EXCHANGE KALENDER-CONNECTOR

   Zur Installation wählen Sie unter AKTION den entsprechenden Eintrag. Klicken Sie dann auf WEITER und folgen den Anweisungen des Assistenten.

4.7 Outlook-Web Access

Neben der Verwendung von Outlook an einem lokalen Rechner innerhalb des SBS-Netzwerks können Sie über Outlook Web Access (OWA) auf Ihre E-Mails auch von einem Remote-Arbeitsplatz aus zugreifen. OWA ist ein Bestandteil des Remote-Webarbeitsplatzes. Der Zugriff erfolgt dabei über einen Internetbrowser. Deshalb spielt das Client-Betriebssystem für OWA keine Rolle. Es kann sich um einen beliebigen Windows-, Macintosh- oder Linux-/Unix-Client handeln.

Um über das Internet per OWA auf die E-Mails zuzugreifen, geben Sie die folgende Adresse im Webbrowser ein: *https://Externer Name des SBS/Exchange/*. Dadurch wird eine spezielle, internetbasierte Version von Outlook geöffnet. Genau diese Version wird als OWA bezeichnet.

Auch mit Hilfe der Remote-Verbindungsdiskette können Sie eine OWA-Verbindung realisieren. Voraussetzung ist, dass Sie dazu den RAS-Assistenten in der Aufgabenliste der Serververwaltung abgeschlossen haben. Öffnen Sie dann in der Serververwaltung unter INTERNET UND E-MAIL den Link REMOTE-VERBINDUNGSDISKETTE ERSTELLEN. Folgen Sie dort den Anweisungen des Assistenten, um den Verbindungsmanager auf eine Diskette

zu kopieren. Diese Diskette legen Sie dann in die gewünschten Clients ein und führen zur Installation die Datei *setup.exe* aus. Damit wird der Verbindungsmanager auf dem Client installiert. Unter NETZWERKVERBINDUNGEN finden Sie nun den neuen Eintrag VERBINDUNG MIT SMALL BUSINESS SERVER HERSTELLEN. Sie können nun eine Remote-Verbindung zum SBS-Netzwerk erstellen.

Um OWA aufzurufen, geben Sie die folgende Adresse in den Internetbrowser ein: *https://Name des SBS/Exchange/*.

4.8 Spezielle Konfiguration für Exchange Server mit mehr als 1 GB RAM

Wird der Exchange Server 2003 auf einer Maschine betrieben, die über mehr als 1 GB RAM verfügt, und wenn auf diesem Server die Postfächer und/oder öffentlichen Ordner liegen, so müssen Sie die Datei *boot.ini* anpassen, damit eine optimale Nutzung des virtuellen Speichers gewährleistet ist. In diese Datei müssen zusätzliche Startparameter für das Betriebssystem hinzugefügt werden. Anderenfalls kann es vorkommen, dass Sie im Task Manager den Prozess *store.exe* finden, der nach dem Neustart des Systems ca. 20 MB belegt, im Laufe eines Tages aber bis zu 500 MB Speicher belegen kann, wodurch der gesamte Server erheblich verlangsamt wird. Es ist nicht möglich, diesen Speicher wieder freizugeben, sofern der Server nicht neu gestartet wird – was ja aber nicht im Sinne des Servers sein kann. Deshalb ist die Modifikation für den Start erforderlich.

Standardmäßig sind für jeden Prozess 2 GB des virtuellen Adressraums für den Benutzermodus aufgeteilt und weitere 2 GB für das Betriebssystem. Wenn Sie in der *boot.ini* den Parameter /3GB setzen, werden für den Benutzermodus 3 GB zugeteilt und nur 1 GB für das Betriebssystem. Dadurch, dass nur 1 GB an Speicher zugewiesen wird, reduziert sich die Gefahr der Speicherfragmentierung im virtuellen Adressraum der *store.exe*.

4.8.1 Anpassen der boot.ini

Um die Datei boot.ini anzupassen, werden in diese die beiden Parameter /3GB sowie /USERVA=3030 eingefügt. Für einen Small Business Server 2003 könnte der Eintrag danach folgendermaßen aussehen:

```
[boot loader]
Timeout=30 Default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[Operating Systems] multi(0)disk(0)rdisk(0)partition(1)
WINDOWS="Windows Server for Small Business Server" /fastdetect /3GB /
USERVA=3030
```

Listing 4.2: Anpassen der boot.ini für die optimale Speichernutzung durch den Exchange Server bei Computern mit mehr als 1 GB RAM

Der Windows Server 2003 – wie auch der SBS 2003 – reserviert 2 GB virtuellen Adressraum für den Kernel und lässt ebenso zu, dass auch Prozesse des Benutzermodus (wie den Exchange 2003 Informationsspeicher-Prozess store.exe) 2 GB des virtuellen Adressraums benutzen. Beim Start wird für einen Prozess eine bestimmte Menge an virtuellem

Speicher zugewiesen. Diese Menge kann sich jedoch im Betrieb erhöhen. Standardmäßig ist die Speichernutzung eines Prozesses viel geringer als der zugewiesene Adressraum für diesen Prozess. Auf einem Exchange Server 2003 mit mehr als 1 GB RAM erfolgt die Modifikation, so dass 3 GB an Speicher für die Prozesse des Benutzermodus zur Verfügung stehen.

Angenommen, ein Exchange Server 2003 verfügt über 2 GB RAM. Wird der Parameter /3GB nicht gesetzt, wird ein Speicherüberlauf erzeugt, wenn der virtuelle Adressraum der *store.exe* 2 GB erreicht. Der Task Manager zeigt in diesem Szenario zwar an, dass lediglich 1,5 GB Speicher in Benutzung sind. Jedoch ist diese Anzeige nicht korrekt, und der Server hat keinen freien Speicher mehr.

Der Parameter /USERVA ist ein neuer Parameter des Windows Server 2003. Über diesen ist es möglich, Speicherzuweisungen für den Benutzermodus und Kernelmodus besser aufzuteilen.

4.9 Die Faxdienste

Die Faxdienste bilden neben den E-Mail-Diensten des Exchange Servers die zweite Möglichkeit der Kommunikation. Über die Faxdienste wird es den SBS-Clients ermöglicht, Faxe zu senden und empfangen. Hierzu wird das auf dem SBS 2003 installierte Faxmodem verwendet. Bei diesem Modem muss es sich um ein Faxmodem der Klasse 1 handeln.

Die Installation der Faxdienste ist zwar auch möglich, wenn mit dem SBS 2003 kein Faxmodem verbunden ist. Eine Nutzung der Dienste ist so selbstverständlich *nicht* möglich.

4.9.1 Funktionsmodell der Faxdienste

Während der Installation der Faxdienste wird ein Standardfaxdrucker auf dem SBS 2003 eingerichtet. Dieser freigegebene Drucker wird für das Senden und Empfangen der Faxe benutzt. Sobald ein Benutzer ein Fax über den Faxdrucker senden möchte, gibt der Drucker an das Faxgerät den Befehl, das Dokument als Fax zu versenden.

Insgesamt bestehen die Faxdienste aus drei separaten Komponenten. Dabei handelt es sich um den Faxdienst, Fax (Lokal) sowie die Microsoft Faxkonsole.

- *Faxdienst*: Der Faxdienst ist die zentrale Komponente des Servers. Über diesen erfolgt die Steuerung des Dienstes. Der Faxdienst-Manager wird über START/PROGRAMME/ZUBEHÖR/KOMMUNIKATION/FAX/FAXDIENST-MANAGER aufgerufen.
- *Fax (Lokal):* Mit Hilfe von Fax (Lokal) können Sie sämtliche Verwaltungsaufgaben, Überwachungen und weitere Einstellungen am Faxdienst vornehmen. Diese Komponente rufen Sie über die Serververwaltung des SBS 2003 auf.
- *Faxclientkonsole*: Diese mmc dient ebenfalls der Verwaltung. Sie können hier die Fax-Warteschlange überwachen sowie Faxe senden und empfangen. Diese mmc rufen Sie über die SERVERVERWALTUNG/FAX (LOKAL) auf und klicken auf den Link FAXAUFTRÄGE VERWALTEN.

4.9.2 Die Verwaltung der Faxgeräte

Auch nach der Installation der Faxdienste können Sie auf dem SBS 2003 weitere Faxmodems hinzufügen. Optimal ist es, wenn Sie dort mindestens zwei Faxe installiert haben, von denen eines zum Senden, das andere zum Empfangen benutzt wird. Wenn Sie ein neues Faxmodem installieren, wird dieses automatisch vom SBS 2003 erkannt, sofern es Plug & Play-fähig ist. Anderenfalls fügen Sie das Gerät über SYSTEMSTEUERUNG/HARDWARE hinzu.

Alle vom Faxdienst erkannten Faxgeräte werden in der Serververwaltung unter GERÄTE UND ANBIETER/GERÄTE angezeigt. Um neu installierte Geräte dort ebenfalls zu sehen, müssen Sie den Faxdienst beenden und wieder neu starten. Ein Erkennen aller Geräte kann nur beim Start des Dienstes erfolgen.

Sobald Sie ein neues Gerät hinzufügen, ist dieses standardmäßig für das Senden von Faxen konfiguriert, nicht jedoch für den Empfang. Um für ein Faxgerät festzulegen, ob dieses Faxe senden und/oder empfangen soll, öffnen Sie die Eigenschaften des Geräts und konfigurieren auf der Registerkarte ALLGEMEIN die Einstellungen (siehe Abbildung 4.17).

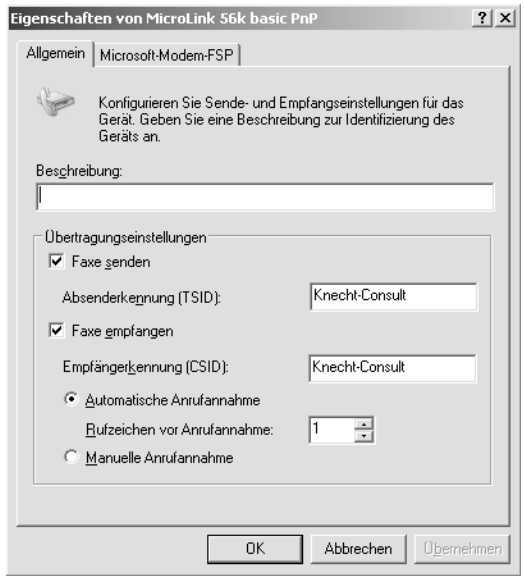


Abbildung 4.17: Die Übertragungseinstellungen für ein Faxgerät konfigurieren

Haben Sie die Option FAXE EMPFANGEN gewählt, müssen Sie für eine automatische Annahme die Anzahl der RUFZEICHEN VOR ANRUFANNAHME festlegen. Für den Faxempfang können Sie jedoch auch die MANUELLE ANRUFANNAHME auswählen.

Weiterhin müssen Sie für ein Fax, das zum Senden konfiguriert ist, die ABSENDERKENNUNG (TSID, Transmitting Subscriber Identification) festlegen. Für Faxe, die für den Empfang eingerichtet sind, wird die EMPFÄNGERKENNUNG (CSID, Called Subscriber Identification) bestimmt. Standardmäßig ist in beiden Fällen Ihr Firmenname dort eingetragen.

Den Zugriff auf den Faxdrucker regeln

Der Zugriff auf den Faxdrucker kann genauso geregelt werden wie der Zugriff auf einen herkömmlichen Drucker. Um bestimmten Benutzern oder Gruppen den Zugriff auf den Faxserver zu verwehren, öffnen Sie über die Serververwaltung die Eigenschaften von FAX (LOKAL) und dort die Registerkarte SICHERHEIT. Dort können Sie neue Benutzer und Gruppen hinzufügen bzw. entfernen und für diese die Berechtigungen einzeln konfigurieren. Es gibt die folgenden vier Standardberechtigungen für einen Faxdrucker:

- Fax
- Faxkonfiguration verwalten
- Faxdokumente verwalten
- Spezielle Berechtigungen

Um die speziellen Berechtigungen für den Faxdrucker zu konfigurieren, klicken Sie auf ERWEITERT und dann auf BEARBEITEN. Es gibt die folgenden speziellen Berechtigungen für einen Faxdrucker:

- Faxe niedriger Priorität einreichen
- Faxe normaler Priorität einreichen
- Faxe hoher Priorität einreichen
- Faxaufträge anzeigen
- Faxaufträge verwalten
- Dienstkonfiguration ansehen
- Dienstkonfiguration verwalten
- Archiv für eingehende Nachrichten anzeigen
- Archiv für eingehende Nachrichten verwalten
- Archiv für ausgehende Nachrichten anzeigen
- Archiv für ausgehende Nachrichten verwalten
- Berechtigungen lesen
- Berechtigungen ändern
- Besitz übernehmen

4.9.3 Eingehende Faxe

Dieses Kapitel zeigt Ihnen die Einstellungen, die Sie für eingehende Faxe vornehmen können. Besonders wichtig in diesem Zusammenhang ist die Konfiguration von Routing-Richtlinien für die eingehenden Faxe.

Beenden des Faxempfangs

Sie können jederzeit auf dem SBS den Empfang von Faxen beenden. Wählen Sie dazu die EIGENSCHAFTEN aus dem Kontextmenü von FAX (LOKAL) und wechseln auf die Registerkarte ALLGEMEIN. Markieren Sie dort die Checkbox ABSENDEN NEUER AUSGEHENDER FAXE DEAKTIVIEREN.

Routing-Richtlinien für eingehende Faxe

Unter Routing-Richtlinien versteht man die Verarbeitungsmethode für eingehende Faxe. Im SBS 2003 haben Sie die Möglichkeit, die Faxe zu drucken, per E-Mail weiterzuleiten, in einen Ordner zu speichern und in die Dokumentenbibliothek der SharePoint Services einzufügen.

Um für das Faxmodem die gewünschte Routing-Richtlinie zu bestimmen, öffnen Sie unter FAX (LOKAL) den Pfad GERÄTE UND ANBIETER/GERÄTE/GERÄTENAME/METHODEN FÜR EINGEHENDE FAXE. Um eine der Richtlinien zu konfigurieren, wählen Sie deren Eigenschaften und tragen die jeweils passenden Werte ein, wie z.B. die E-Mail-Adresse, an welche die Faxe gesendet werden sollen, oder den Ordner, in dem die Faxe gespeichert werden sollen. Nachdem Sie eine Methode konfiguriert haben, wählen Sie aus deren Kontextmenü den Eintrag AKTIVIEREN. Jede der Methoden kann auch wieder deaktiviert werden.

Da Sie auch mehrere der Methoden auswählen können, müssen Sie für diese Prioritäten festlegen. Hierzu öffnen Sie den Pfad ROUTING EINGEHENDER NACHRICHTEN/GLOBALE METHODEN unter FAX (LOKAL). Standardmäßig sind die folgenden Prioritäten gesetzt:

Priorität 1: Über E-Mail weiterleiten

Priorität 2: In Ordner speichern

Priorität 3: Drucken

Priorität 4: In einer Dokumentenbibliothek speichern

Über die Kontextmenüeinträge NACH OBEN und NACH UNTEN können Sie jedoch eine eigene Prioritätenliste erstellen.

Weitere Hinweise zur Konfiguration der Routing-Richtlinien finden Sie in Kapitel 2.

4.9.4 Ausgehende Faxe

In diesem Kapitel lernen Sie die Konfigurationseinstellungen für die ausgehenden Faxe näher kennen.

Möchten Sie für ein Faxmodem das Senden von Nachrichten verhindern, so wechseln Sie auf die Registerkarte ALLGEMEIN unter den EIGENSCHAFTEN von FAX (LOKAL). Markieren Sie dort die Checkbox ABSENDEN NEUER AUSGEHENDER FAXE DEAKTIVIEREN. Damit wird erreicht, dass die Benutzer keine neuen Faxe mehr an den Ordner AUSGEHEND schicken können. Es werden nur noch die Faxe verschickt, die sich bereits in dem Ordner befinden. Markieren Sie die Checkbox ÜBERTRAGEN AUSGEHENDER FAXE DEAKTIVIEREN, werden keine Faxe mehr gesendet, die sich bereits im Ordner AUSGEHEND befinden.

Weitere Einstellungen für ausgehende Faxe nehmen Sie auf der Registerkarte AUSGANGSFACH unter den Eigenschaften von FAX (LOKAL) vor (siehe Abbildung 4.18).

Haben Sie die Checkbox BANNER EINFÜGEN markiert, werden auf den Seitenrand der ausgehenden Faxe die Übertragungsinformationen gedruckt. Ist die Option PERSÖNLICHE DECKBLÄTTER ZULASSEN ausgewählt, können die Benutzer außer den Standarddeckblättern auch welche aus ihren persönlichen Ordnern benutzen. Weitere Hinweise zu Deckblättern finden Sie in Kapitel Abbildung 4.9.7. Ist die Checkbox ÄLTERE FAXE AUTOMA-

TISCH LÖSCHEN nach aktiviert, werden Faxe, die nach Ablauf der festgelegten Anzahl von Tagen nicht gesendet werden konnten, aus dem Ordner AUSGEHEND entfernt.

Abbildung 4.18: Die Konfiguration der Optionen für ausgehende Faxe

Unter FAXÜBERTRAGUNGEN legen Sie fest, wie oft versucht werden soll, ein fehlgeschlagenes Fax erneut zu versenden. Das Warteintervall für das erneute Senden bestimmen Sie unter WIEDERHOLUNG NACH. Unter GÜNSTIGER TARIF BEGINNT und GÜNSTIGER TARIF ENDET tragen Sie die Uhrzeiten an, während derer billige Tarife für das Senden von Faxen berücksichtigt werden sollen.

Wenn Sie einen Zeitraum für das Senden von Faxen festlegen, werden sämtliche Faxe nur noch in diesem angegebenen Zeitraum gesendet. Zu allen Zeiten außerhalb des günstigen Tarifs werden *keine* Faxe mehr gesendet. Dies kann insbesondere dann zu Problemen führen, wenn Faxe aufgrund von Auslastungen der Faxgeräte nicht innerhalb des Zeitraums gesendet werden konnten. Das erneute Senden wird erst durchgeführt, wenn der definierte Zeitraum am folgenden Tag wieder anbricht.

Beginnt eine Faxübertragung noch innerhalb des günstigen Zeitraums, aber überschreitet die Zeitgrenze, so wird die Übertragung dennoch fortgesetzt, allerdings fallen dann die nicht mehr vergünstigten Kosten an.

Sie sollten sich bei der Definition des Intervalls in jedem Fall überlegen, ob die Faxkapazitäten ausreichend sind, alle anstehenden Faxe innerhalb der vorgegebenen Zeit zu versenden. Ist dies nicht der Fall, sollten Sie entweder für weitere Faxkapazitäten sorgen oder aber die Zeitplanung deaktivieren. So werden zwar keine günstigen Tarife in Anspruch genommen, dafür können Sie jedoch sicher sein, dass sämtliche Faxe immer sofort gesendet werden.

Weiterhin können Sie auch die Empfangsbestätigungen für die ausgehenden Faxe konfigurieren. Diese Einstellungen werden auf der Registerkarte EMPFANGSBESTÄTIGUNGEN (siehe Abbildung 4.19) vorgenommen.

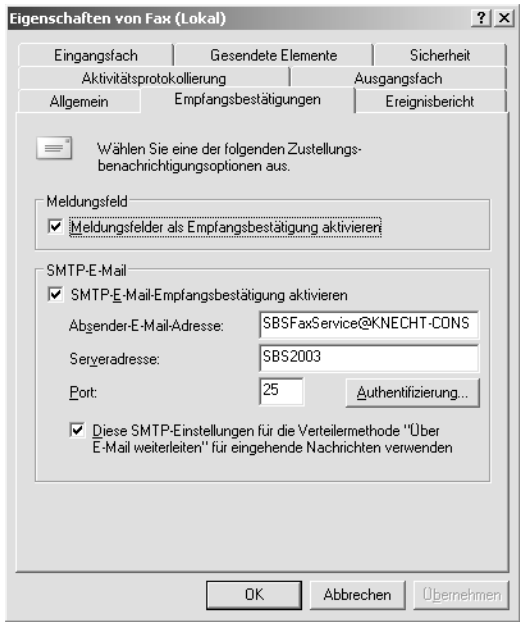


Abbildung 4.19: Konfiguration der Empfangsbestätigungen für gesendete Faxe

Ist die Checkbox MELDUNGSFELDER ALS EMPFANGSBESTÄTIGUNG AKTIVIEREN markiert, erhält der Benutzer ein Pop-up-Fenster, das ihn über das erfolgreiche Versenden des Fax informiert.

Möchten Sie hingegen eine Bestätigung per E-Mail, so markieren Sie die Checkbox SMTP-E-MAIL-EMPFANGSBESTÄTIGUNG AKTIVIEREN. Tragen Sie dann die Absenderadresse, die SMTP-Serveradresse sowie den Port in die entsprechenden Felder ein. Klicken Sie dann auf AUTHENTIFIZIERUNG, um die Authentifizierung für den SMTP-Server zu bestimmen. Sie können wählen zwischen ANONYMER ZUGRIFF, STANDARDAUTHENTIFIZIERUNG sowie INTEGRIERTE WINDOWS-AUTHENTIFIZIERUNG. In den beiden letzten Fällen geben Sie zusätzlich den Benutzernamen und das Kennwort an.

Schließlich können Sie noch festlegen, an wie viele Empfänger ein Fax gleichzeitig gesendet werden darf.

1. Öffnen Sie dazu den Faxdienst-Manager über START/PROGRAMME/ZUBEHÖR/KOMMUNIKATION/FAX. Beenden Sie dort den Faxdienst über das entsprechende Symbol.
2. Öffnen Sie mit dem Befehl regedit die Registry und navigieren zum Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fax\RecipientsLimit. Tragen Sie dort den Wert ein.
3. Starten Sie im Faxdienst-Manager den Faxdienst wieder neu.

Arbeiten mit mehreren Faxgeräten

Sind auf dem SBS 2003 mehrere Faxgeräte installiert, können Sie weitere Optionen für den Faxausgang konfigurieren. Es können dabei verschiedene Geräte zu Gruppen zusammengelegt werden, die dann bestimmte Regeln zur Verwendung befolgen.

Standardmäßig befinden sich sämtliche Faxgeräte in der Gruppe ALLE GERÄTE unter FAX (LOKAL)/VERTEILEN AUSGEHENDER NACHRICHTEN/GRUPPEN. Um eine neue Gruppe zu erstellen, klicken Sie im Kontextmenü von GRUPPEN auf NEU und geben der Gruppe einen Namen. Dieser Gruppe fügen Sie über NEU/GERÄTE die gewünschten Geräte hinzu. Innerhalb einer Gruppe können Sie die Reihenfolge der Geräte über die Kontextmenüs NACH OBEN und NACH UNTEN ändern. Auch das Löschen von Geräten einer Gruppe ist darüber möglich.

Unter (LOKAL)/VERTEILEN AUSGEHENDER NACHRICHTEN/REGELN bestimmen Sie, in welcher Weise die verschiedenen Geräte verwendet werden sollen. Um eine neue Regel zu erstellen, wählen Sie aus dem Kontextmenü von REGELN NEU/REGEL (siehe Abbildung 4.20).

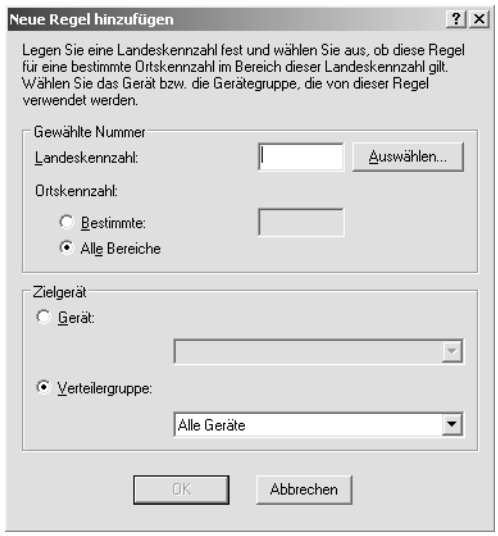


Abbildung 4.20: Festlegen der Regeln für ausgehende Faxe

Zunächst bestimmen Sie unter LANDESKENNZAHL die Länderkennzahl, für Deutschland wäre dies 49. Sofern Sie die Länderkennzahl nicht kennen, klicken Sie auf AUSWÄHLEN und selektieren den gewünschten Staat. Danach können Sie entweder eine bestimmte Ortskennzahl des Landes eintragen oder mit ALLE BEREICHE sämtliche Ortskennzahlen auswählen. Unter ZIELGERÄT bestimmen Sie entweder ein einzelnes Gerät oder eine der angelegten Gerätegruppen.

4.9.5 Überwachung der Faxdienste

Über die Faxclientkonsole können Sie die Faxdienste überwachen. Eine Überwachung kann für die Faxe in vier verschiedenen Stadien vorgenommen werden. Im Ordner EINGEHEND werden die Faxe angezeigt, die gerade empfangen werden. Das EINGANGSFACH zeigt die bereits empfangenen Faxe an. Unter AUSGANGSFACH sehen Sie die Faxe, die gerade versendet werden, und im Ordner GESENDETE ELEMENTE befinden sich die bereits gesendeten Faxe (siehe Abbildung 4.21).

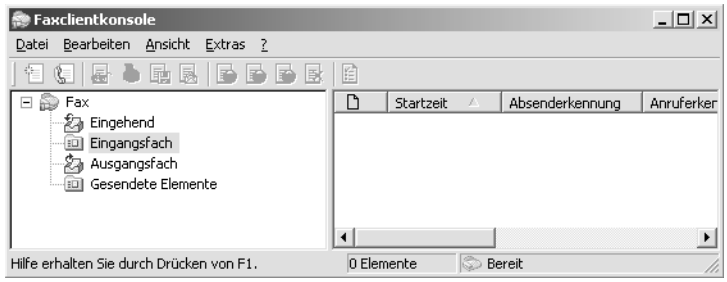


Abbildung 4.21: Übersicht über die Gesendeten Faxe sowie das Eingangs- und Ausgangsfach

In jedem der vier Ordner befindet sich die Spalte STATUS. In dieser Spalte kann eine der folgenden Statusmeldungen angezeigt werden:

- SENDEN: Das Fax wird gerade versendet. Der Sendevorgang besteht aus Wählen, Initialisieren und Übertragen. Dieses wird unter ERWEITERTER STATUS angezeigt.
- AUSSTEHEND: Das Fax befindet sich in der Warteschlange, bis es auf einem verfügbaren Faxmodem gesendet werden kann.
- ANGEHALTEN: Ein Fax innerhalb der Warteschlange wurde entweder vom Administrator oder vom Benutzer angehalten.
- WIRD WIEDERHOLT: Das Senden des Fax wird wiederholt, wenn die Telefonleitung des Empfängers besetzt ist.
- ANZAHL AN WIEDERHOLUNGEN ÜBERSCHRITTEN: Die maximale Anzahl der Sendeversuche wurde überschritten. Die maximale Anzahl wird auf der Registerkarte AUSGANGSFACH in den Eigenschaften von FAX (LOKAL) eingestellt.

4.9.6 Archivieren von Faxen

Für sämtliche eingehenden und ausgehenden Faxe können Sie die Archivierung aktivieren. Ist diese eingerichtet, werden die Faxe in bestimmten Ordnern archiviert.

Um die Archivierung für eingehende Faxe einzurichten, wählen Sie die EIGENSCHAFTEN von FAX (LOKAL) und wechseln auf die Registerkarte EINGANGSFACH. Dort markieren Sie die Checkbox ALLE EINGEHENDEN FAXE IN FOLGENDEM ORDNER ARCHIVIEREN und geben einen Ordner an. Um die gesendeten Faxe zu archivieren, wechseln Sie auf die Registerkarte GESENDETE ELEMENTE und markieren dort die Checkbox ALLE ERFOLGREICH GESENDETEN FAXE IN FOLGENDEM ORDNER ARCHIVIEREN. Um den Ordner zu wechseln, klicken Sie jeweils auf DURCHSUCHEN.

Zusätzlich können Sie festlegen, ob eine Anzeige im Ereignisprotokoll erfolgen soll, wenn der Inahlt eines Archivordners eine bestimmte Größe überschreitet.

Markieren Sie dazu auf den Registerkarten EINGANGSFACH sowie GESENDETE ELEMENTE die Checkbox WARNUNG IM EREIGNISPROTOKOLL GENERIEREN. Unter OBERE GRENZE FÜR KONTINGENT bestimmen Sie die Maximalgröße. Wird diese überschritten, erfolgt ein Eintrag in das Ereignisprotokoll. Unter UNTERE GRENZE FÜR KONTINGENT tragen Sie den Wert ein, der erricht werden muss, damit keine Ereigniswarnung mehr auftritt. Um ein stetiges Anwachsen des Archivordners zu verhindern, sollten Sie die Option ÄLTERE FAXE AUTOMATISCH LÖSCHEN NACH aktivieren. Geben Sie die Anzahl der Tage an, die ein empfangenes oder gesendetes Fax im Archivordner erhalten bleiben soll.

4.9.7 Die Fax-Deckblätter

Bei den Fax-Deckblättern handelt es sich um serverbasierte Deckblätter. Sobald ein Benutzer ein Fax versenden möchte, kann er eines der Deckblätter auswählen und dem zu sendenden Fax hinzufügen.

Standardmäßig finden Sie die vier bereits vorkonfigurierten Deckblätter für die Verwendungszwecke „Dringend“, „Info“, „Standard“ sowie „Vertraulich“ in der Serververwaltung unter DECKBLÄTTER. Sämtliche Deckblätter tragen die Dateiendung *.cov* (Cover). Die Vorlagen für die Deckblätter werden im Ordner \Dokumente und Einstellungen \All Users\Anwendungsdaten\Microsoft\Windows NT\MSFax\Common Coverpages gespeichert.

Um ein neues Deckblatt zu erstellen, wählen Sie aus dem Kontextmenü der Deckblätter den Eintrag NEU/DECKBLATT. Dadurch wird der Faxdeckblatt-Editor gestartet (siehe Abbildung 4.22). Möchten Sie ein vorhandenes Deckblatt ändern, so wählen Sie BEARBEITEN aus dem entsprechenden Kontextmenü.

Abbildung 4.22: Das Bearbeiten von Fax-Deckblättern

5 Die Windows SharePoint Services 2.0

Die Installation der SharePoint Services in der Version 2.0 erfolgt automatisch im Zuge der SBS 2003-Installation. Die Installationsdateien befinden sich auf der CD 3 der SBS 2003-Installationsmedien.

Da es bei Installationen, die nach dem 24.November 2003 ausgeführt worden sind, zu Problemen bei der Installation der SharePoint Services kommen kann, sollten Sie in jedem Fall die aktualisierte Version der SharePoint Services verwenden. Sie finden die aktualisierte Version auf der Begleit-CD. Außerdem besteht für die Kunden die Möglichkeit, eine fehlerfreie Version der Installations-CD 3 kostenfrei von Microsoft zu erhalten. Nutzen Sie dazu das Bestellformular unter *https://microsoft.order-4.com/sbsrtmcd/*. Weitere Hinweise zu den Installationsproblemen der SharePoint Services finden Sie in Kapitel 13.4.1

5.1 Aufgabe der SharePoint Services

Die Microsoft SharePoint Services stellen eine Neuerung des SBS 2003 gegenüber seinem Vorgänger dar. Diese Services bieten eine html-basierte zentrale Verwaltung sowie eine zentrale Zugriffsmöglichkeit auf Dokumente, Kalender, Projektdaten, Präsentationen und Listen für die gemeinsame Arbeit und Kommunikation an Projekten.

Die zentrale Seite für den Zugriff ist die Seite *http://companyweb*. Diese Seite wird automatisch bei der Installation der SharePoint Services angelegt und als Startseite für den Internet Explorer festgelegt. Sie enthält zunächst lediglich einige Beispieldaten. Nach der Installation sieht die Seite *companyweb* folgendermaßen aus (siehe Abbildung 5.1):

Um sämtliche Funktionalitäten der SharePoint Services nutzen zu können, müssen die Benutzer Microsoft Office XP oder Microsoft Office 2003 verwenden. Bei älteren Office-Versionen kann es zu Problemen kommen. Es können damit keine auf der Website hinterlegten Office-Dokumente bearbeitet und gespeichert werden. Nur die Betrachtung der Website sowie das Hinzufügen von Beiträgen ist möglich, da hierfür lediglich ein Webbrowser erforderlich ist.

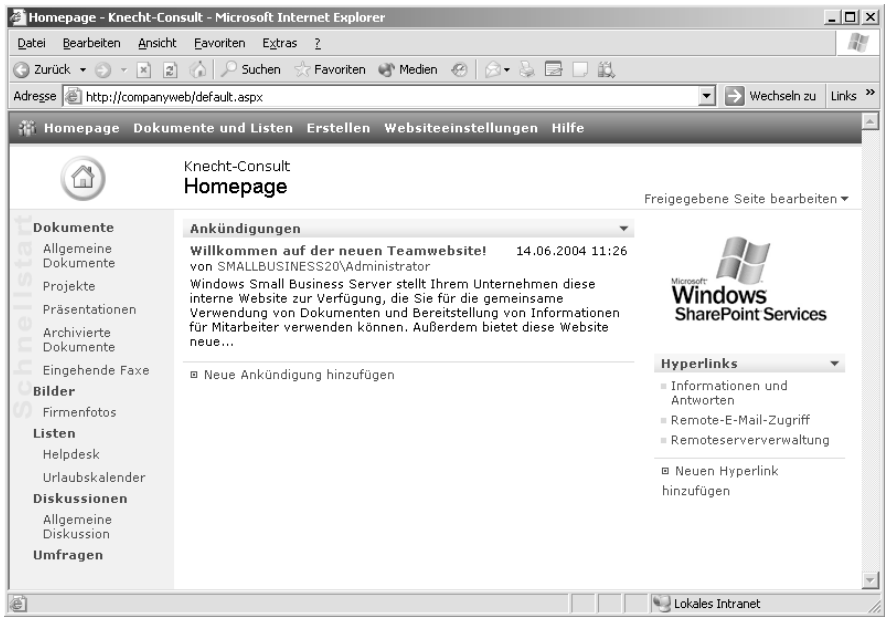


Abbildung 5.1: Die Website http://companyweb direkt nach der Installation

5.1.1 Features der SharePoint Services

Auf der SharePoint-Website können Sie die folgenden Informationen bereitstellen:

- Bereitstellen von Dokumenten für die gemeinsame Verwendung durch ein Team.
- Informationsbereitstellung über zu erledigende Aufgaben, wichtige Ereignisse oder projektbezogene Informationen.
- Veröffentlichen von Ansprechpartnern und deren Telefonnummern innerhalb des Projektes oder des Helpdesks.
- Diskussionen der Teammitglieder
- Umfragen für die Benutzer

Sobald beliebige der eben genannten Informationen vom Administrator oder von Benutzern zur Website hinzugefügt werden, werden automatisch neue Links auf der Website generiert, so dass stets die höchste Aktualität der Seite gegeben ist. Optional können auch Benachrichtigungen über sämtliche Änderungen an der Website an eine oder mehrere Personen ausgegeben werden.

Zudem ist für die Benutzer eine hohe Anpassbarkeit der Seite gegeben. So können sie sich die Informationen nach bestimmten Kriterien wie z.B. Datum, Autor oder Betreff sortieren. Zudem können nicht interessante Informationen ausgeblendet oder für bestimmte Benutzer vorgegebene Ansichten konfiguriert werden.

Auf der Website befinden sich standardmäßig die folgenden Inhaltsbereiche:

Inhaltsbereich	Beschreibung
Dokumente	ALLGEMEINE DOKUMENTE: Die hier enthaltenen Dateien werden mit ihren Eigenschaften wie z.B. Änderungsdatum und Person der letzten Bearbeitung sowie einem Hyperlink zu der Datei angezeigt. PROJEKTE: Hier können nach Projekten geordnet ebenfalls Dokumente abgelegt und bearbeitet werden. PRÄSENTATIONEN: In diesem Bereich können Firmenpräsentationen angelegt und bearbeitet werden. ARCHIVIERTE DOKUMENTE: In diesem Bereich werden archivierte Dokumente abgelegt, die momentan nicht benötigt werden. EINGEHENDE FAXE: Hier können Sie sämtliche eingehende Faxe sammeln. Allerdings muss dazu die entsprechende Option in der Aufgabenliste im Faxassistenten aktiviert sein.
Bilder	FIRMENFOTOS: Hier können Sie für die Benutzer Fotos bereitstellen, z.B. von einem Betriebsausflug, oder weitere Fotos, die für alle Benutzer verfügbar sein sollen.
Listen	HELPDESK: Hier können Sie die Daten der Person(en) des Helpdesk mit den dazugehörigen Informationen eintragen. URLAUBSKALENDER: Der Urlaubskalender gewährt einen schnellen Überblick über die Urlaubstage der Mitarbeiter und kann mit Outlook verknüpft werden.
Diskussionen	ALLGEMEINE DISKUSSIONEN: Die Teammitglieder können hier Diskussionen im Stil einer Newsgroup führen.
Umfragen	Standardmäßig sind keine Umfragen enthalten. Eine Umfrage an die Benutzer kann schnell mit Hilfe eines Assistenten erstellt werden.
Ankündigungen	Hier sind aktuelle Ankündigungen und Hinweise für das Team eingetragen.
Hyperlinks	Hier wird eine Reihe von Hyperlinks angezeigt, die für die Teammitglieder in ihrer Arbeit interessant und wichtig sein könnten.

Tabelle 5.1: Die Inhalte der SharePoint-basierten Website Companyweb

Der Inhalt der Website kann über einen Webbrowser modifiziert werden, indem Sie bestimmte Inhalte hinzufügen oder entfernen. Mit Hilfe des Webbrowsers können Sie auch verschiedene Ansichten für die Website wählen. Möchten Sie hingegen das Layout der Firmenwebsite ändern, benötigen Sie einen html-Editor wie z.B. das in der Premium-Edition enthaltene FrontPage 2003.

Im Rahmen der Sicherheit können Sie den Benutzern verschiedene Berechtigungsebenen für den Zugriff auf die Website zuweisen. So können einige Benutzer lediglich Lesezugriff erhalten, während andere Benutzer Dokumente hinzufügen oder sogar die Websitekonfiguration bearbeiten dürfen.

5.1.2 Die Struktur der SharePoint Services

Die bereits vorkonfigurierte Website *http://companyweb* basiert auf den Windows SharePoint Services. Diese Website benutzt die Internetinformationsdienste (IIS) sowie eine Datenbank, die von der MSDE (Microsoft SQL Database Engine) oder dem SQL Server bereitgestellt wird. In der MSDE werden die Inhalte der Website, d.h. die Dokumente, Listen, Einstellungen usw. gespeichert, während die Website selbst auf dem virtuellen Server COMPANYWEB des IIS gespeichert wird. Weitere Hinweise zu virtuellen Servern finden Sie in Kapitel Abbildung 5.6.

Dokumentenbibliotheken

Dokumentenbibliotheken sind der zentrale Speicherort für die Dokumente innerhalb der Website. Eine Dokumentenbibliothek kann durch Unterordner weiter gegliedert werden. Sobald ein Benutzer eine Bibliothek über die Website öffnet, werden die enthaltenen Dateien als Hyperlink angezeigt und können geöffnet und bearbeitet werden. Sobald der Mauszeiger auf den Link gesetzt wird, erhält der Benutzer weitere Informationen zu dem Dokument. Über die Änderungen an Dokumenten können auch E-Mail-Benachrichtigungen an die übrigen Benutzer eingerichtet werden. Eine Besonderheit stellt die Faxbibliothek dar, in der sämtliche eingehenden Faxe gespeichert werden können.

Eingliederung neuer Sites

Zur besseren Übersicht – besonders bei umfangreichen Konstrukten – kann es sinnvoll sein, neue Sites zur Website Companyweb hinzuzufügen. Diese können mit denselben oder unterschiedlichen Berechtigungen wie die Hauptseite konfiguriert werden.

5.1.3 Die Deinstallation der SharePoint Services

Für die Deinstallation der SharePoint Services haben Sie verschiedene Möglichkeiten. So können Sie die Services entweder direkt vom Server entfernen oder lediglich vom virtuellen Server.

Möchten Sie die SharePoint Services vom SBS 2003 entfernen, gehen Sie auf SYSTEMSTEUERUNG/SOFTWARE/WINDOWS SHAREPOINT SERVICES und klicken auf ENTFERNEN. Dabei wird nicht die dazugehörige Microsoft SQL Server Desktop Engine (MSDE) entfernt. Diese Komponente muss separat deinstalliert werden. Bei der Deinstallation der SharePoint Services wird jedoch nicht der Inhalt der Website gelöscht. Sie können dieses Verfahren auch wählen, wenn Sie eine Reparatur der SharePoint Services vornehmen möchten oder müssen.

Möchten Sie die SharePoint Services vom virtuellen Server entfernen, so können Sie dazu entweder die HTML-Administrationsseite oder die Kommandozeile verwenden.

Um die Deinstallation über die Administrationsseite vorzunehmen, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Verwaltung auf SHAREPOINT-ZENTRALADMINISTRATION.

2. Klicken Sie im Bereich VIRTUELLEN SERVER KONFIGURIEREN auf den Link EINSTELLUNGEN VIRTUELLER SERVER KONFIGURIEREN und klicken aus der Liste den gewünschten virtuellen Server an. Standardmäßig finden Sie dort die Einträge COMPANYWEB, MICROSOFT SHAREPOINT-ADMINISTRATION sowie STANDARDWEBSITE.
3. Im Fenster EINSTELLUNGEN VIRTUELLER SERVER klicken Sie im Bereich VERWALTUNG VIRTUELLER SERVER auf den Link WINDOWS SHAREPOINT SERVICES VOM VIRTUELLEN SERVER ENTFERNEN.
4. Sie erhalten das Fenster WINDOWS SHAREPOINT SERVICES VOM VIRTUELLEN SERVER ENTFERNEN. Wählen Sie dort die Option ENTFERNEN, OHNE DABEI INHALTSDATENBANKEN ZU LÖSCHEN, so werden lediglich die Ordner der SharePoint Services vom virtuellen Server gelöscht, während die Inhaltsdatenbank erhalten bleibt. Somit ist es möglich, später mit demselben oder einem anderen virtuellen Server wieder eine Verbindung zu der Datenbank herzustellen. Wählen Sie hingegen die Option ENTFERNEN UND DABEI INHALTSDATENBANKEN LÖSCHEN, so werden sowohl die Ordner der SharePoint Services als auch die Inhaltsdatenbank selbst vom virtuellen Server gelöscht. Die Websites können in diesem Fall nur über ein Backup wiederhergestellt werden. Treffen Sie Ihre Auswahl und klicken dann auf OK.

Möchten Sie die Deinstallation über die Kommandozeile über das Dienstprogramm *stsadm.exe* vornehmen, so führen Sie die folgenden Schritte aus:

1. Möchten Sie nur die Ordner der SharePoint Services löschen, die Datenbank aber beibehalten, verwenden Sie den Befehl

```
Stsadm.exe -o unextendvs -url http://Name des virtuellen Servers
```

2. Möchten Sie neben den Ordnern auch die Datenbank löschen, benutzen Sie den Befehl

```
Stsadm.exe -o unextendvs -url http://Name des virtuellen Servers -
deletecontent
```

Durch die Deinstallation der SharePoint Services auf eine der beiden eben beschriebenen Methoden können Sie sicherstellen, dass die Deinstallation sauber erfolgt und Sie den Server wieder für andere Websites oder Anwendungen benutzen können.

5.2 Verwalten der SharePoint Services

Dieses Kapitel beschreibt die wichtigsten Verwaltungsaufgaben, die Sie unter den SharePoint Services durchführen können.

5.2.1 Verwaltungspunkte der SharePoint Services

Für die Verwaltung der SharePoint Services steht Ihnen eine html-basierte Administration zur Verfügung. Die Administration kann sowohl über den lokalen als auch über einen Remote-Computer erfolgen. Sie müssen dazu in jedem Fall über die Berechtigung eines Administrators verfügen. Für die Verwaltung stehen die Zentraladministrationsseiten und die Websiteverwaltungsseiten zur Verfügung.

Zentraladministrationsseiten

Die zentrale Verwaltungsseite wird über die Serververwaltung unter INTERNE WEBSITE/ZENTRALVERWALTUNG aufgerufen. Auf diesen zentralen Seiten können Sie Einstellungen für den Webserver sowie die virtuellen Server vornehmen. Hier werden im Wesentlichen die Standardwerte des Servers bestimmt. Die hier festgelegten Werte werden beispielsweise an alle neu erstellten virtuellen Server weitergegeben. Abbildung 5.2 zeigt die Hauptseite der zentralen Verwaltung.

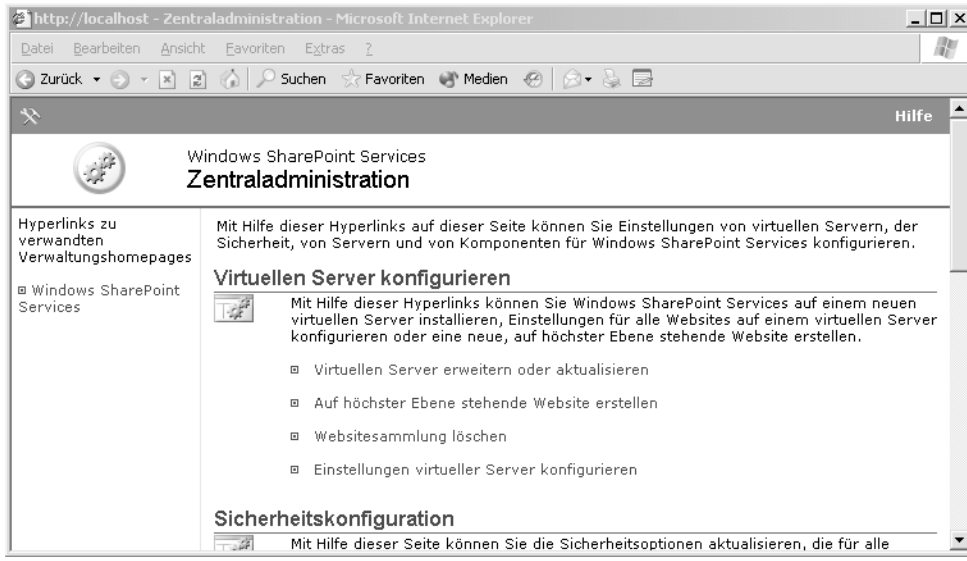


Abbildung 5.2: Die Hauptseite der Zentraladministration

Für die Ausführung dieser Seiten müssen Sie entweder zur Gruppe der lokalen Administratoren oder der SharePoint-Administratorengruppe gehören. Der Aufruf der zentralen Administrationsseiten erfolgt entweder über das Startmenü oder direkt über den Webbrowser.

Wenn Sie unter START/PROGRAMME/VERWALTUNG des SBS 2003 auf MICROSOFT SHAREPOINT-ADMINISTRATION klicken, erscheint nicht die Verwaltungsseite der Microsoft SharePoint Services, sondern fälschlicherweise die Verwaltungsseite der FrontPage Server Extensions 2002. Über den Eintrag in der Verwaltung ist ein Start der Verwaltungswebseite nicht möglich.

Öffnen Sie stattdessen unter START/PROGRAMME/VERWALTUNG den Eintrag SHAREPOINT-ZENTRALADMINISTRATION. Damit wird die korrekte Seite geöffnet.

Um die zentrale Administrationsseite über den Webbrowser zu öffnen, geben Sie die Adresse *http://Servername:Portnummer* oder *http://localhost:Portnummer* an. Die Portnummer wurde während der SharePoint-Installation festgelegt. Standardmäßig lautet der Port 8081.

Websiteverwaltungsseiten

Über die Websiteverwaltungsseiten werden die Einstellungen der einzelnen Websites vorgenommen (siehe Abbildung 5.3).

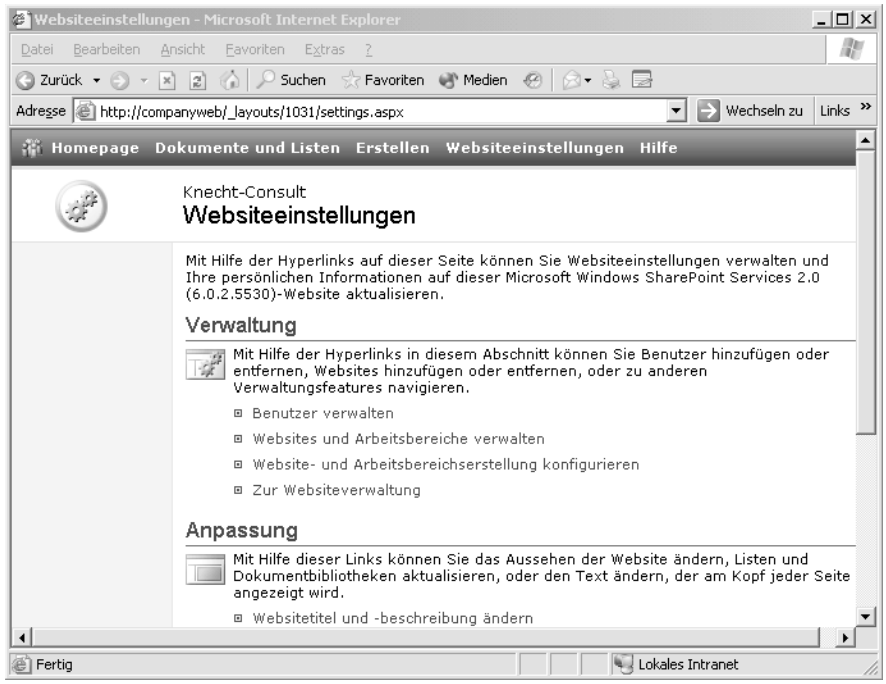


Abbildung 5.3: Die Konfigurationsseite für die Websiteeinstellungen

Sie erreichen diese auf der jeweiligen Website über das Menü WEBSITEEINSTELLUNGEN. Die hier vorgenommenen Konfigurationen beziehen sich immer nur auf die aktuelle Website. Beispielsweise können Sie hier den Titel, den Inhalt oder das Design der aktuellen Seite bearbeiten.

5.2.2 Websitegruppen

Für die Zuweisung und Verwaltung der Berechtigungen für die Website werden so genannte Websitegruppen benutzt. Damit ein Benutzer überhaupt Zugriff auf die Website erlangen kann, muss er Mitglied in mindestens einer der verschiedenen Websitegruppen sein. Insgesamt gibt es sechs verschiedene Websitegruppen mit unterschiedlichen Berechtigungsebenen. Die folgende Tabelle zeigt die Berechtigungen der einzelnen Websitegruppen.

Websitegruppe	Beschreibung
Gast	Ein Gast kann lesenden Zugriff auf bestimmte Seiten oder Listen erhalten, ohne dass er die komplette Website sehen kann. Diese Websitegruppe kann nicht gelöscht oder modifiziert werden. Sie können auch keinen Benutzer direkt zu dieser Gruppe hinzufügen. Es werden automatisch die Benutzer Mitglied der Websitegruppe Gast, denen Sie über Listenberechtigungen Zugriff auf bestimmte Dokumentenbibliotheken oder Listen erteilen.
Leser	Ein Mitglied dieser Gruppe darf Seiten und Einträge betrachten sowie übergeordnete Websites über das Feature Self-Service Site Creation erstellen. Jedoch können Sie keine Inhalte zu den Webseiten hinzufügen. Hat ein Leser eine Seite über die Self-Service Site Creation erstellt, so ist er für diese Website sowohl Besitzer als auch Mitglied der Websitegruppe Administrator.
Teilnehmer	Dieser besitzt zusätzlich zu den Berechtigungen eines Lesers noch die folgenden Berechtigungen: Hinzufügen, Löschen und Bearbeiten von Elementen, Hinzufügen, Entfernen und Aktualisieren persönlicher Webparts (siehe Kapitel), Verwalten persönlicher Ansichten, Durchsuchen von Verzeichnissen sowie Erstellen von websiteübergreifenden Gruppen. Diese Benutzer können jedoch keine Dokumentenbibliotheken oder Listen erstellen, wohl aber den Inhalt zu bereits vorhandenen Dokumentenbibliotheken oder Listen hinzufügen.
Webdesigner	Zusätzlich zu den Berechtigungen des Teilnehmers darf der Webdesigner die folgenden Aktionen ausführen: Verwalten von Listen, Hinzufügen und Anpassen von Seiten, Abbrechen des Auscheckens, Anwenden und Definieren von Stylesheets, Designs und Rändern. Sie dürfen die Struktur der Website ändern sowie Dokumentenbibliotheken oder Listen erstellen.
Administrator	Schließt die Berechtigungen der anderen Gruppen ein und kann zusätzlich Websitegruppen verwalten sowie neue SharePoint-Websites erstellen. Diese Websitegruppe kann nicht angepasst werden.

Tabelle 5.2: Die verschiedenen Websitegruppen und ihre Berechtigungen

Die Websitegruppen werden für jede einzelne SharePoint-Seite definiert. Um die Einstellungen für alle SharePoint-Websites oder den virtuellen Server zu ändern, muss der Benutzer Mitglied der Administratorengruppe des SBS 2003 selbst sein bzw. ein Mitglied der Gruppe SharePoint-Administratoren. Eine Mitgliedschaft der Websitegruppe Administrator ist für derartige Verwaltungsaufgaben nicht ausreichend.

Sie können die Berechtigungen einer Websitegruppe ändern oder neue Websitegruppen mit benutzerdefinierten Berechtigungen erstellen. Wenn Sie Websitegruppen bestimmte Berechtigungen entziehen, bedenken Sie, dass einige Berechtigungen voneinander abhängig sind. Löschen Sie eine Berechtigung, von der weitere abhängen, so werden auch die abhängigen Berechtigungen gelöscht. Fügen Sie eine Berechtigung hinzu, für die weitere Berechtigungen erforderlich sind, so werden diese automatisch hinzugefügt.

Die beiden Websitegruppen Gast und Administrator können nicht hinsichtlich der Berechtigungen bearbeitet werden.

Sofern ein Benutzer eine neue Website erstellt, ist er automatisch Mitglied der Websitegruppe Administrator. Er wird dadurch auch als Websitebesitzer angezeigt. Unter einigen Konfigurationen ist es notwendig, noch einen zweiten Benutzer anzugeben. Auch dieser wird dann automatisch Mitglied der Websitegruppe Administrator. Der Besitzer einer Website kann über die Zentraladministration auf der Seite WEBSITESAMMLUNGSBESITZER verwalten geändert werden. Weiterhin ist auch eine Änderung über das Kommandozeilenprogramm *Stsadm.exe* über den Parameter siteowner möglich.

Für die Benutzerauthentifizierung stehen Ihnen verschiedene Methoden zur Verfügung. Die Authentifizierungsmethode für die SharePoint Services basiert auf den Authentifizierungsmethoden des IIS. Die gewünschte Methode wird beim Einrichten des Webservers festgelegt. Es stehen die folgenden Methoden zur Wahl:

- Anonyme Authentifizierung
- Standardauthentifizierung
- Integrierte Windows-Authentifizierung
- Digest-Authentifizierung und erweiterte Digest-Authentifizierung
- Zertifikatsauthentifizierung (SSL)

5.3 Die Inhalte der Firmenwebsite bearbeiten

In diesem Kapitel sind diverse Aufgaben für die Anpassung der Firmenwebsite selbst sowie deren Inhalte beschrieben.

5.3.1 Daten zur Firmenwebsite hinzufügen

Die Firmenwebsite macht wenig Sinn, wenn sich in dieser keine Dokumente und Dateien zum Bearbeiten befinden. Um bereits vorhandene Dateien von beispielsweise einem Dateiserver in die Firmenwebsite zu bringen, steht Ihnen eine Importfunktion zur Verfügung.

1. Öffnen Sie in der Serververwaltung den Eintrag INTERNE WEBSITE und darin den Link DATEIEN IMPORTIEREN. Es wird ein Assistent gestartet.
2. Im Fenster DATEI- UND DOKUMENTBIBLIOTHEKSPFAD wählen Sie über DURCHSUCHEN die Datenquelle. Unter DATEIEN KOPIEREN NACH ist standardmäßig der Pfad COMPANYWEB/GENERAL DOCUMENTS eingetragen. Auch dieser Zielpfad kann über DURCHSUCHEN geändert werden. Klicken Sie dann auf WEITER und stellen den Assistenten fertig. Danach werden die ausgewählten Dateien in die gewählte Dokumentenbibliothek kopiert.

5.3.2 Erstellen einer neuen Dokumentenbibliothek

Wie Sie eben beim Importieren der Daten bemerkt haben, können Sie dort als Zielverzeichnis nur eine bereits bestehende Dokumentenbibliothek auswählen. Um eine neue Dokumentenbibliothek anzulegen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Seite *http://companyweb* und klicken dort auf das Menü ERSTELLEN und wählen unter DOKUMENTBIBLIOTHEKEN den Eintrag DOKUMENTBIBLIOTHEK.
2. Im Fenster NEUE DOKUMENTBIBLIOTHEK (siehe Abbildung 5.4) geben Sie zunächst den Namen und eine Beschreibung der neuen Bibliothek ein.

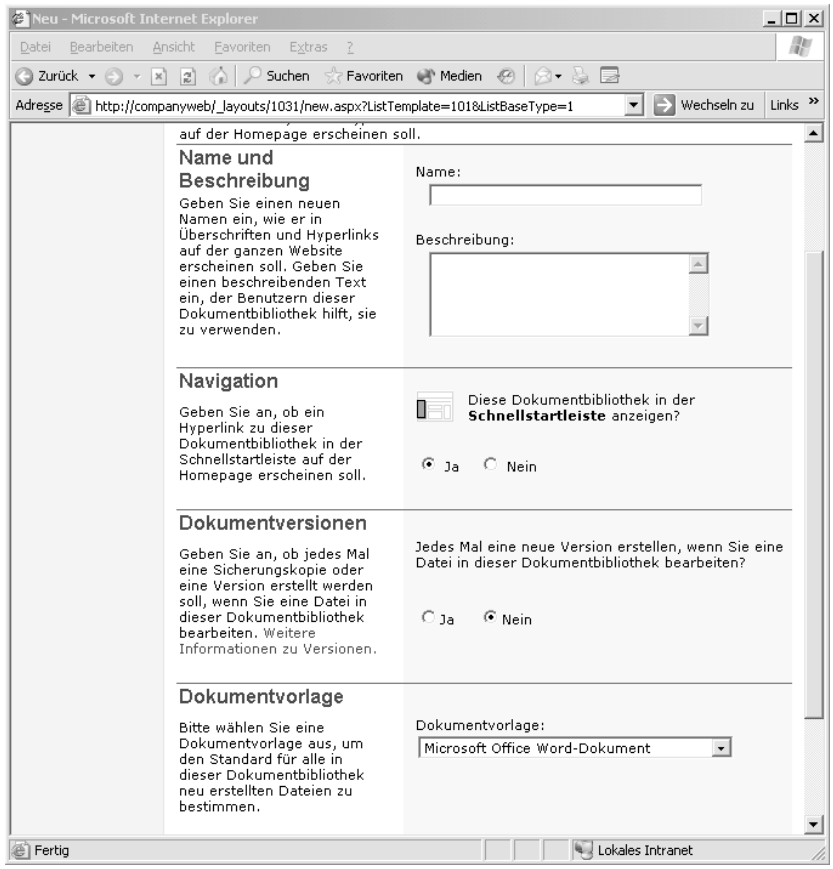


Abbildung 5.4: Das Anlegen einer neuen Dokumentenbibliothek

Unter NAVIGATION können Sie bestimmen, ob für die neue Bibliothek ein Link in der Schnellstartleiste, also im linken Bereich der Website, angelegt werden soll oder nicht.

Unter DOKUMENTVERSION bestimmen Sie, ob beim Bearbeiten des Dokuments eine neue Version oder eine Sicherungskopie der Datei erstellt werden soll. Weitere Hinweise zur Versionierung in den SharePoint Services finden Sie in Kapitel Abbildung 5.4.

Schließlich legen Sie unter DOKUMENTVORLAGE noch fest, ob eine Vorlage wie beispielsweise ein OFFICE WORD-DOKUMENT oder eine OFFICE EXCEL-KALKULATIONSTABELLE oder KEINE VORLAGE verwendet werden soll. Klicken Sie dann auf ERSTELLEN.

3. Nachdem Sie die neue Bibliothek erstellt haben, erhalten Sie das Fenster mit dem Namen der neu angelegten Bibliothek (siehe Abbildung 5.5). Hier werden der neuen Bibliothek die Dokumente zugewiesen.

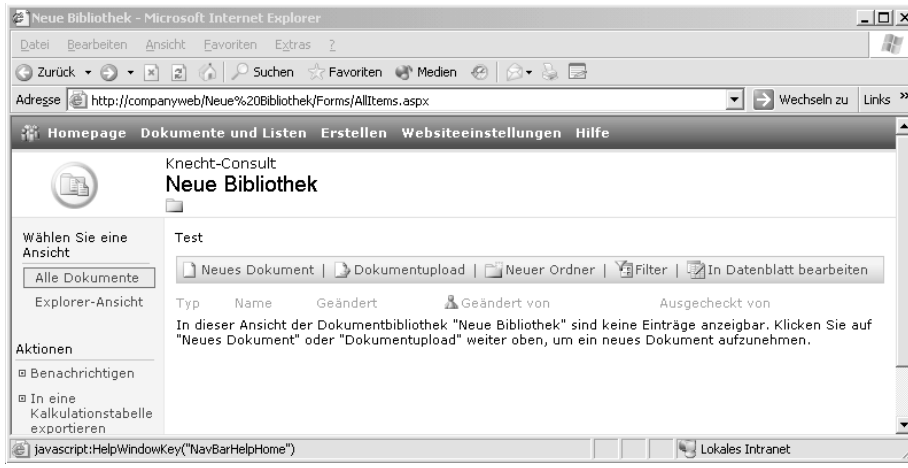


Abbildung 5.5: Das Zuweisen von Dokumenten zur neuen Dokumentenbibliothek

Zum Füllen der Bibliothek mit neuen Dokumenten können Sie entweder das Menü NEUES DOKUMENT oder DOKUMENT-UPLOAD benutzen. Im ersten Fall muss eine SharePoint-kompatible Applikation wie Office XP oder 2003 installiert sein. Beim Dokument-Upload geben Sie entweder den Namen für das gewünschte Dokument ein oder klicken auf DURCHSUCHEN. Soll eine gleichnamige bereits vorhandene Datei ersetzt werden, so markieren Sie die Checkbox VORHANDENE DATEI(EN) ÜBERSCHREIBEN. Um das Dokument hinzuzufügen, klicken Sie auf SPEICHERN UND SCHLIESSEN.

Weitere Bibliotheken

Analog zu einer Dokumentenbibliothek können Sie auch eine Formular-, Bild- und Faxbibliothek erstellen. In die Formularbibliothek können Sie XML-basierte Dokumente hinzufügen. Voraussetzung ist ein XML-kompatibler Editor wie beispielsweise Office InfoPath. In eine Bildbibliothek werden gemeinsam genutzte Bilder eingepflegt. Für diese können Sie zusätzliche Optionen wie Download-Optionen oder Miniaturansichten konfigurieren. In einer Faxbibliothek werden sämtliche eingehenden Faxe gesammelt. Weitere Hinweise zur Faxbibliothek finden Sie in Kapitel Abbildung 5.3.6.

5.3.3 Erstellen einer neuen Site

1. Um eine neue Website zu erstellen, klicken Sie auf der Website auf ERSTELLEN und dort unter WEBSEITEN auf WEBSITES UND ARBEITSBEREICHE.
2. Wie bei einer neuen Dokumentenbibliothek geben Sie auch hier einen Namen und eine Beschreibung der neuen Site an. Danach geben Sie die URL der neuen Site an. Der Pfad *http://companyweb/* ist dabei bereits vorgegeben. Als Drittes werden noch die Berechtigungen für die neue Site festgelegt. Sie können entweder die Berechtigungen der übergeordneten Site übernehmen oder EIGENE BERECHTIGUNGEN VERWENDEN. Werden die Berechtigungen von der übergeordneten Site geerbt, können die Benutzerberechtigungen später nur von einer Person mit Administratorberechtigung geändert werden. Klicken Sie dann auf ERSTELLEN.
3. Dann gelangen Sie auf die Seite VORLAGENAUSWAHL. Hier wählen Sie eine Vorlage wie beispielsweise TEAMSITE oder LEERE WEBSITE. Klicken Sie dann auf OK. Danach wird die neue Site erstellt. Um von dieser aus wieder auf die übergeordnete Site zu gelangen, benutzen Sie den Link NACH OBEN ZU SEITENNAME in der oberen rechten Ecke.

5.3.4 Bearbeiten einer Site

Nachdem Sie eine Site erstellt haben, können Sie diese zu einem späteren Zeitpunkt wieder bearbeiten. Dies gilt auch für die Site Companyweb. Hierzu verwenden Sie das Menü WEBSITEEINSTELLUNGEN.

Unter VERWALTUNG können Sie die folgenden Einstellungen vornehmen:

- BENUTZER VERWALTEN: Hier können Sie Benutzer zu Websitegruppen hinzufügen, aus diesen entfernen und Benutzer, die zur aktuellen Website hinzugefügt sind, bearbeiten.
- WEBSITES UND ARBEITSBEREICHE VERWALTEN: Hier werden die vorhandenen Websites und Arbeitsbereiche angezeigt. Es können neue Sites und Bereiche erstellt sowie vorhandene bearbeitet werden.
- WEBSITE- UND ARBEITSBEREICHSERSTELLUNG ÄNDERN: Hier sehen Sie, welchen Websitegruppen das Erstellen von Websites und Arbeitsbereichen gestattet ist. Diese Einstellungen können hier auch bearbeitet werden.
- WEBSITEVERWALTUNG: Über diesen Link gelangen Sie zur Seite Verwaltung der auf höchster Ebene stehenden Website (siehe Abbildung 5.6). Die dort vorgenommenen Einstellungen werden an die untergeordneten Websites weitergegeben.

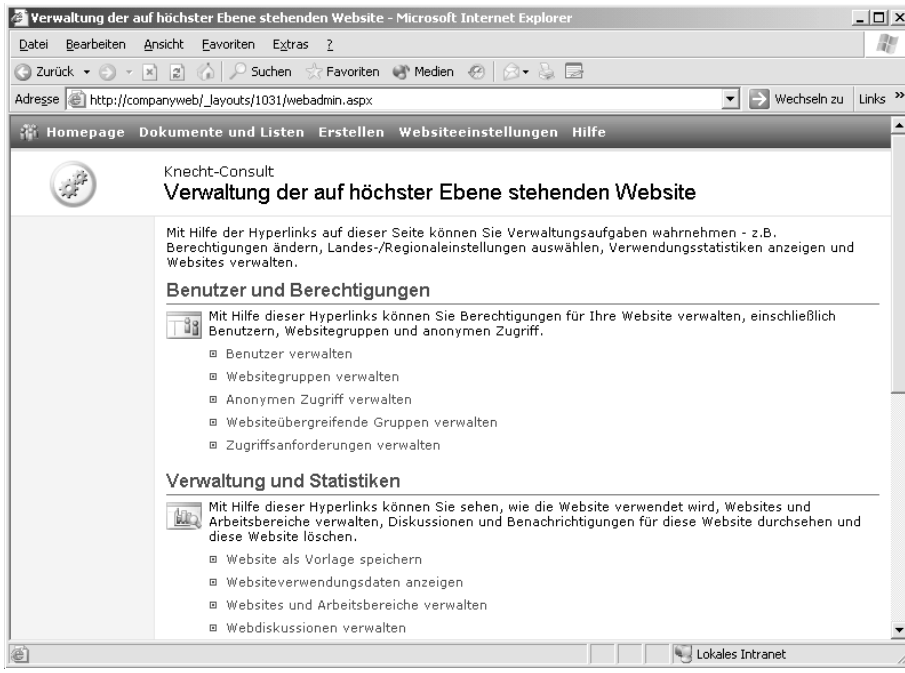


Abbildung 5.6: Die Verwaltung der auf höchster Ebene stehenden Website

Unter ANPASSUNG können Sie die folgenden Konfigurationen vornehmen:

- WEBSITETITEL UND -BESCHREIBUNG ÄNDERN: Hier können der Titel sowie die optionale Beschreibung der Site bearbeitet werden.
- DESIGN AUF WEBSITE ANWENDEN: Hier können Sie aus einer vordefinierten Liste von Designs eines für die Website auswählen und über die Vorschaufunktion betrachten.
- WEBSITEINHALT ÄNDERN: Hier können Sie die folgenden Bereiche der Website modifizieren: Dokumentenbibliothek, Liste, Diskussionsrunde und Umfrage. Dazu klicken Sie auf den gewünschten Link. Danach können Sie die allgemeinen Einstellungen des Elements ändern, es als Vorlage speichern, die Berechtigungen bearbeiten oder das Element löschen. Auch die Spalten sowie Ansichten des gewählten Elements können geändert werden.
- HOMEPAGE ANPASSEN: Über diesen Link können Sie die Webparts der Site bearbeiten (siehe Abbildung 5.7). Bei Webparts handelt es sich um die editierbaren Bereiche der Site wie z.B. ALLGEMEINE DOKUMENTE, ANKÜNDIGUNGEN, URLAUBSKALENDER usw. Sie können hier ausgewählte Webparts wahlweise dem rechten oder linken Websitebereich hinzufügen.

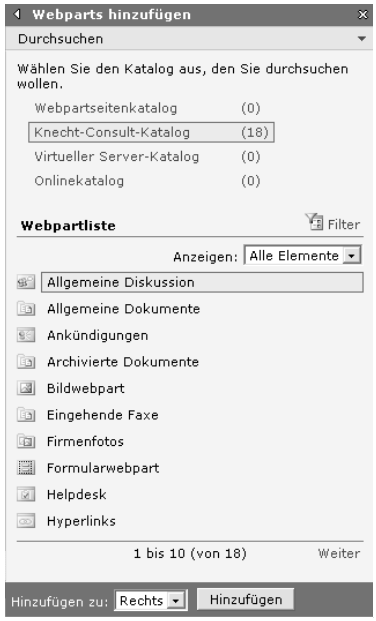


Abbildung 5.7: Das Hinzufügen von Webparts zu einer Site

Bearbeiten von Webparts

Webparts können bearbeitet werden, indem Sie auf der gewünschten Website auf das Pfeilsymbol in der Titelleiste des Webparts und darunter auf FREIGEGEBENES WEBPART BEARBEITEN klicken, beispielsweise unter ANKÜNDIGUNGEN (siehe Abbildung 5.8).

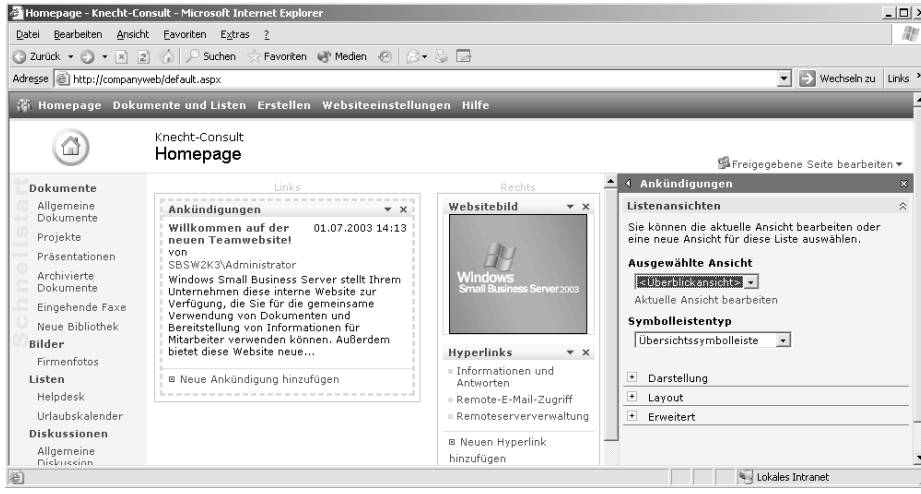


Abbildung 5.8: Das Bearbeiten von Webparts

5.3.5 Konfiguration der E-Mail-Benachrichtigung

Die E-Mail-Benachrichtigung wird eingesetzt, um Benutzer zu informieren, wenn Dokumente, Dokumentenbibliotheken oder Listen geändert oder neue Objekte hinzugefügt bzw. bestehende gelöscht worden sind. Um diese Benachrichtigung zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der Serververwaltung den Eintrag INTERNE WEBSITE/ZENTRALVERWALTUNG. Dort navigieren Sie zum Abschnitt SERVERKONFIGURATION und klicken auf STANDARDMÄSSIGE E-MAIL-SERVEREINSTELLUNGEN KONFIGURIEREN.
2. Dort konfigurieren Sie die Einstellungen für den SMTP-Server, die Von-Adresse sowie die Antwortadresse (siehe Abbildung 5.9). Als SMTP-Server ist standardmäßig der SBS 2003 selbst eingetragen. Klicken Sie dann auf OK.

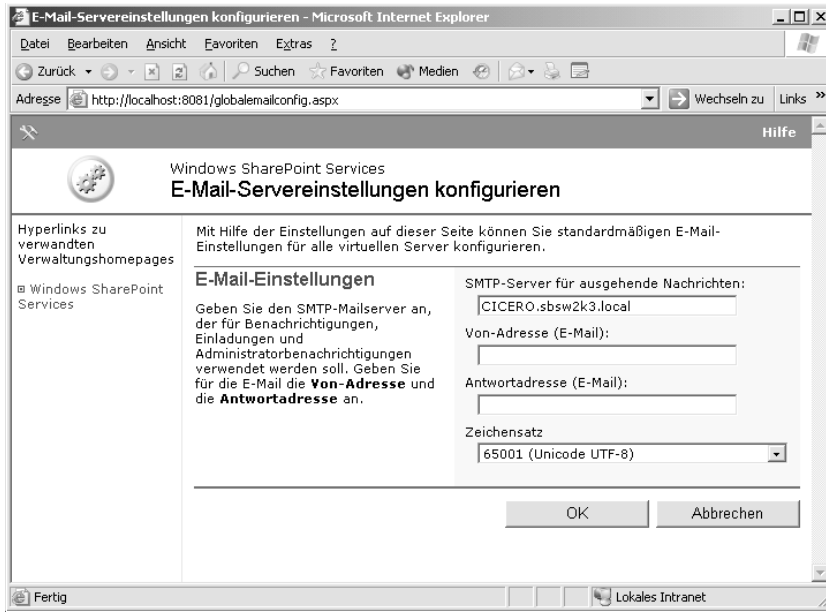


Abbildung 5.9: Die E-Mail-Konfiguration für die Benachrichtigungen

Auswahl der Benachrichtigungen

Damit ein Benutzer nicht zu viele oder unerwünschte Benachrichtigungen empfängt, kann eine Auswahl der gewünschten Nachrichten sowie deren Optionen getroffen werden. Klicken Sie dazu auf das gewünschte Element (z.B. ALLGEMEINE DOKUMENTE). Unter AKTIONEN klicken Sie auf BENACHRICHTIGUNGEN.

Hier können die folgenden Benachrichtigungsoptionen eingestellt werden:

- Die E-Mail-Adresse, an welche die Benachrichtigung geschickt werden soll.
- Der Typ der Änderungen, für welche die Benachrichtigung erfolgen soll. Mögliche Optionen sind beispielsweise ALLE ÄNDERUNGEN, HINZUGEFÜGTE EINTRÄGE, GEÄNDERTE EINTRÄGE, GELÖSCHTE EINTRÄGE oder WEBDISKUSSIONSÄNDERUNGEN.

- Die Benachrichtigungshäufigkeit. Hier können Sie wählen, ob die E-Mails sofort versendet werden sollen oder ob Sie tägliche oder nur wöchentliche Benachrichtigungen über die gewählten Änderungen erhalten möchten.

Anzeigen der Benachrichtigungen

Die Benachrichtigungen werden zum einen an die festgelegt E-Mail-Adresse gesendet, sie können aber auch auf der Website eingesehen werden. Klicken Sie dazu auf WEBSITE-EINSTELLUNGEN und dort im Bereich MEINE INFORMATIONEN VERWALTEN auf MEINE BENACHRICHTIGUNGEN AUF DIESER WEBSITE. Zusätzlich können dort neue Listen oder Bibliotheken ausgewählt werden, für die Sie Benachrichtigungen erhalten möchten. Vorhandene Benachrichtigungen können hier auch gelöscht werden.

5.3.6 Faxweiterleitung in die Dokumentenbibliothek

In der Dokumentenbibliothek EINGEHENDE FAXE werden sämtliche eingegangenen Faxe gespeichert. Zu jedem Fax finden Sie Informationen in verschiedenen Spalten wie Empfangsdatum, Seitenzahl oder Größe. Die Faxe werden jeweils als Hyperlink angezeigt und können nach den verschiedenen Spalten sortiert werden.

Voraussetzung für das Anzeigen der Faxe in der Dokumentenbibliothek ist, dass Sie in der Aufgabenliste für das Faxgerät als Ausgabeoption auch das Speichern in der Dokumentenbibliothek ausgewählt haben. Verwenden Sie mehrere Faxgeräte, so muss für jedes einzelne das Speichern in der Dokumentenbibliothek aktiviert werden.

5.4 Die Dateiversionierung der SharePoint Services

Wie bereits beim Anlegen einer neuen Dokumentenbibliothek beschrieben, können Sie bestimmen, ob Sie eine Sicherungskopie oder eine neue Version einer bearbeiteten Datei anlegen möchten. Um dies bestimmen zu können, erhalten Sie nun einen kurzen Einblick in die Dateiversionierungsmechanismen der SharePoint Services.

Haben Sie beim Erstellen der Dokumentenbibliothek die Option JEDES MAL EINE NEUE VERSION ERSTELLEN, WENN SIE EINE DATEI IN DIESER DOKUMENTBIBLIOTHEK BEARBEITEN aktiviert, wird zusätzlich der Eintrag VERSIONSVERLAUF hinzugefügt, wenn Sie auf den Pfeil neben dem Dokument bei einem Dokument klicken (siehe Abbildung 5.10). Damit besteht die Möglichkeit, gezielt eine ältere Version eines Dokuments auszuwählen und weiterzubearbeiten.

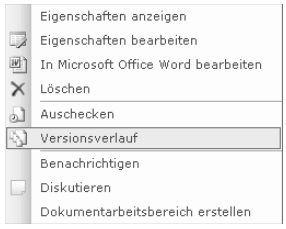


Abbildung 5.10: Der zusätzliche Menüeintrag Versionsverlauf nach dem Aktivieren der Versionierung

Sofern die Versionierung aktiviert ist, werden in den folgenden Fällen jeweils neue Versionen des Dokuments erstellt:

- Der Benutzer öffnet und editiert das Dokument und speichert es danach zum ersten Mal. Bei weiteren Speicherungen wird keine neue Version erstellt, sondern erst wieder, wenn der Benutzer die Applikation abermals geöffnet und darin die Datei neu gespeichert hat.
- Der Benutzer checkt eine Datei aus, editiert sie und checkt sie danach wieder ein.
- Der Benutzer stellt eine ältere Dateiversion wieder her und checkt diese nicht aus.
- Der Benutzer führt einen Upload einer bereits vorhandenen Datei durch. Die vorhandene Version wird somit zu einer älteren Version.

Sobald eine Datei aus der Dokumentenbibliothek gelöscht wird, werden automatisch auch alle vorhandenen Versionen dieser Datei entfernt.

5.5 Aktualisierung des Servers und der virtuellen Server

Sie können jederzeit einen Server auf den SharePoint Services aktualisieren. Durch diesen Vorgang werden sowohl der Server selbst als auch der virtuelle Standardserver aktualisiert. Um die Aktualisierungen durchzuführen, starten Sie von der Installations-CD des SBS 2003 die Datei *setupsts.exe* und folgen den Anweisungen des Assistenten.

Um weitere virtuelle Server zu aktualisieren, müssen Sie das Kommandozeilenprogramm *stsadm.exe* verwenden. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die Eingabeaufforderung und wechseln in dieser zum Ordner C:\Programme\Gemeinsame Dateien\Microsoft Shared\Web Server Extensions\60\Bin.
2. Geben Sie dann den folgenden Befehl ein, wobei URL für die URL des zu aktualisierenden virtuellen Servers steht:

   ```
   Stsadm.exe -o upgrade -url <URL> ↵
   ```

Möchten Sie einen virtuellen Server, auf dem die FrontPage 2002-Servererweiterungen ausgeführt werden, auf die SharePoint Services aktualisieren, müssen die FrontPage Servererweiterungen zunächst deinstalliert werden. Sollen die Inhalte der Website erhalten bleiben, migrieren Sie diese mit Hilfe des Tools *smigrate.exe* auf die SharePoint-Website. Sie finden dieses Programm im Verzeichnis Programme\Gemeinsame Dateien\Microsoft Shared\Web Server Extensions\60\Bin.

5.6 Die Verwaltung der virtuellen Server

Ein virtueller Server oder auch mehrere virtuelle Server befinden sich auf dem SBS 2003, der gleichzeitig ein http-Server ist. Außerhalb des SBS 2003-Umfeldes kann sich ein virtueller Server auch auf jedem anderen beliebigen Webserver befinden. Jeder virtuelle Server kann eigene Seiten beinhalten und eigene Programme ausführen. Weiterhin kann jeder der virtuellen Server eine eigene IP-Adresse und einen eigenen Domänennamen besitzen. Auf dem SBS 2003 befinden sich standardmäßig die virtuellen Server companyweb, Standardwebsite sowie Microsoft SharePoint-Administration.

Werden auf einen virtuellen Server die SharePoint Services angewendet, so spricht man vom Erweitern des virtuellen Servers. Eine Erweiterung ist die Grundlage, wenn eine SharePoint-basierte Website erstellt werden soll. Diese Erweiterung geschieht bei einer herkömmlichen Installation der SharePoint Services automatisch.

Die Inhalte der virtuellen Server werden in Datenbanken gespeichert. Beim Erweitern von Servern erfolgt ein Zugriff auf die Inhaltsdatenbank und die Konfigurationsdatenbank. In der Inhaltsdatenbank sind die Inhalte der verschiedenen Websites gespeichert. Dazu zählen auch Einstellungen der Benutzernamen, Berechtigungen oder die Dokumente und Listen der Dokumentenbibliotheken. Standardmäßig benötigt ein Server nur eine Inhaltsdatenbank. Betreiben Sie hingegen eine Serverfarm, so muss eine ausreichende Anzahl an Inhaltsdatenbanken bereitstehen. Die Konfigurationsdatenbank ist für die Verwaltung von Verbindungen zwischen den Servern und den Inhaltsdatenbanken verantwortlich. Ferner werden hier die Servereinstellungen gespeichert. Pro Server (und sogar pro Serverfarm) ist nur eine einzige Konfigurationsdatenbank erforderlich.

5.6.1 Erweitern virtueller Server

Eine Erweiterung kann dann sinnvoll werden, wenn Sie Platz für neue Benutzerwebsites bereitstellen möchten. Sie können entweder die neuen Inhalte zu einem neuen virtuellen Server hinzufügen oder auch Websitesammlungen oder weitere Inhaltsdatenbanken zu einem bestehenden virtuellen Server hinzufügen. Möchten Sie für eine größere Anzahl von möglichen Verbindungen zu einer Website oder für den Verweis mehrerer URLs auf dieselbe Website, stellen Sie zunächst eine Verbindung mit einer vorhandenen Inhaltsdatenbank her. Die Liste der vorhandenen Inhaltsdatenbanken wird automatisch durch die Konfigurationsdatenbank generiert. Die Inhaltsdatenbanken werden als virtuelle Server angezeigt.

Beim Erweitern eines virtuellen Servers müssen Sie die folgenden Informationen angeben:

- Konto und E-Mail-Adresse des Besitzers der übergeordneten Standardwebsite des virtuellen Servers
- Zu verwendender Anwendungspool
- Zu verwendende Inhaltsdatenbank

Optional können Sie noch die folgenden Informationen angeben:

- Abweichende URL, wenn die Standardwebsite nicht im Stammverzeichnis des virtuellen Servers erstellt werden soll
- Die anzuwendende Websitevorlage

- Die Sprache für die übergeordnete Standardwebsite. Es kann nur aus den Sprachen gewählt werden, die auf dem Server für die SharePoint Services installiert sind.
- Bei der Verwendung von Kontingenten können Sie die Kontingentvorlage angeben.

Beim Erweitern des virtuellen Servers können Sie auf zweierlei Arten vorgehen. Dies ist davon abhängig, ob Sie eine neue Inhaltsdatenbank erstellen oder eine vorhandene benutzen möchten. Beide Szenarien werden in den beiden nächsten Kapiteln vorgestellt.

5.6.2 Erstellen des virtuellen Servers im IIS

Bevor Sie einen virtuellen Server erweitern können, müssen Sie zunächst den Server im IIS anlegen. Dazu führen Sie die folgenden Schritte aus:

1. Öffnen Sie VERWALTUNG/INTERNETINFORMATIONSDIENSTE-MANAGER und erweitern dort den Server, zu dem Sie den neuen virtuellen Server hinzufügen möchten.
2. Aus dem Kontextmenü von WEBSITES wählen Sie NEU/WEBSITE.
3. Es erscheint ein Assistent. Klicken Sie zunächst auf WEITER und geben dann eine Beschreibung für die neue Website an.
4. Geben Sie dann die folgenden Informationen an:
   - Die IP-Adresse für diese Website, oder Sie verwenden dazu die Standardeinstellung KEINE ZUGEWIESEN.
   - Den TCP-Port (Standard ist Port 80)
   - Unter HOSTHEADER müssen Sie keinen Eintrag vornehmen, da das Hosting von den SharePoint Services gehandelt wird.
5. Als Nächstes geben Sie den Pfad zum Basisverzeichnis für die Seite an. Deaktivieren Sie hier die Checkbox ANONYMEN ZUGRIFF AUF DIESE WEBSITE ZULASSEN.
6. Legen Sie dann die Zugriffsberechtigungen für die Website fest. Sie sollten hier die beiden gewählten Einstellungen LESEN und SKRIPTE AUSFÜHREN (Z.B. ASP) beibehalten. Durch die SharePoint Services wird automatisch die Berechtigung AUSFÜHREN (Z.B. ISAPI-ANWENDUNGEN ODER CGI) zu den entsprechenden Ordnern hinzugefügt. Klicken Sie dann auf WEITER und FERTIG STELLEN.

5.6.3 Erweitern des virtuellen Servers und Erstellen einer Inhaltsdatenbank

Möchten Sie den virtuellen Server erweitern und dabei eine neue Inhaltsdatenbank erstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die SharePoint-Zentraladministration und klicken unter VIRTUELLEN SERVER KONFIGURIEREN auf VIRTUELLEN SERVER ERWEITERN ODER AKTUALISIEREN.
2. In der Liste der Server klicken Sie den gewünschten Server an. In dem folgenden Fenster klicken Sie unter EINRICHTUNGSOPTIONEN auf INHALTSDATENBANK ERWEITERN UND ERSTELLEN. Dort geben Sie die notwendigen Informationen wie Websitebesitzer, Sprache und zu verwendender Anwendungspool an. Klicken Sie dann auf OK.
3. Damit erfolgt die Erweiterung des virtuellen Servers. Die neue Seite wird im Stammverzeichnis des virtuellen Servers angelegt. Schließlich erhalten Sie noch das Fenster, um die Einstellungen für die übergeordnete Website zu konfigurieren.

5.6.4 Erweitern des virtuellen Servers und Verbinden mit einer vorhandenen Inhaltsdatenbank

Möchten Sie den virtuellen Server erweitern und dabei eine Verbindung zu einer bereits bestehenden Inhaltsdatenbank herstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die SharePoint-Zentraladministration und klicken unter VIRTUELLEN SERVER KONFIGURIEREN auf VIRTUELLEN SERVER ERWEITERN ODER AKTUALISIEREN.
2. Klicken Sie den gewünschten Server an und in dem dann folgenden Fenster auf ERWEITERN UND ZUORDNEN ZU EINEM ANDEREN VIRTUELLEN SERVER.
3. Sie erhalten das Fenster ERWEITERN UND ZUORDNEN ZU EINEM ANDEREN VIRTUELLEN SERVER. Dort wechseln Sie zum Abschnitt SERVERZUORDNUNG und geben den Namen des zu benutzenden virtuellen Servers bzw. Hosts im Feld HOSTNAME ODER VIRTUELLER SERVERNAME IN IIS an.
4. Im Abschnitt ANWENDUNGSPOOL entscheiden Sie, ob Sie einen bereits vorhandenen Anwendungspool verwenden oder einen neuen erstellen möchten. Für einen neuen Anwendungspool müssen Sie dessen Namen, den Benutzernamen sowie das Kennwort angeben. Klicken Sie dann auf ABSENDEN.

Nachdem der virtuelle Server auf diese Weise erweitert worden ist, stellt er die Inhalte derselben Datenbank bereit wie auch die anderen virtuellen Server, welche die Datenbank verwenden. Sofern Sie für den virtuellen Server eine neue übergeordnete Website erstellen, wird diese gleichzeitig auch von allen anderen virtuellen Servern gehostet, die dieselbe Inhaltsdatenbank verwenden.

6 Der Internet Security and Acceleration Server 2000 (ISA)

Der ISA-Server 2000 ist der Nachfolger des Microsoft Proxy-Servers 2.0. Zuweilen wird er auch als Proxy-Server 3.0 bezeichnet. Er besitzt gegenüber seinem Vorgänger neben der Proxy-Funktionalität eine wesentlich verbesserte Firewall-Funktion. Der ISA-Server kann sowohl nur als Proxy-Server oder Firewall als auch in Kombination der beiden Rollen eingesetzt werden. In seiner Firewall-Funktion verwendet der ISA-Server zur Verwaltung die Active Directory-Dienste des SBS 2003.

In diesem Kapitel erwartet Sie zunächst ein Überblick über die verschiedenen Konfigurations- und Einsatzszenarien des Servers. Danach werden die Installation und Grundkonfiguration besprochen. Darauf aufbauend geht es dann um Konfigurationsspezifikationen, das Zusammenspiel mit anderen Servern und Optionen für die Proxy-Funktion. Auch die Funktion, Installation und Konfiguration des Firewall-Clients des SBS 2003 wird besprochen.

Der ISA Server 2000 hat zwischenzeitlich seinen Nachfolger im ISA Server 2003 gefunden. Ob, inwieweit oder wann jedoch der ISA Server 2000 des SBS 2003 durch die neue Version des ISA Server 2004 ersetzt wird, ist bisher nicht bekannt gegeben worden.

Die Version des ISA-Servers im SBS 2003

Der im Lieferumfang des SBS 2003 enthaltene ISA-Server entspricht im Funktionsumfang dem herkömmlichen ISA Server 2000 mit Service Pack 1 in der Standardedition. Zusätzlich sind in diese Version auch alle Patches integriert, die zwischen dem Service Pack und dem Erscheinen des SBS 2003 herausgegeben worden sind. Gegenüber der herkömmlichen Version des ISA-Servers sind auch einige Setup-Dateien modifiziert worden.

6.1 Szenarien und Grundlagen für den ISA-Server

Die Installationsart des ISA-Servers ist davon abhängig, in welcher Form das Netzwerk abgesichert wird bzw. abgesichert werden soll. Die häufigsten Szenarien sind dabei der Einsatz einer Firewall, eine demilitarisierte Zone (DMZ) oder sogar eine DMZ mit zwei Firewalls.

6.1.1 Einsatz einer Firewall

Eine Firewall ist mit zwei Netzwerkkarten ausgestattet. Die eine stellt den Zugang zum Internet her, die andere die Verbindung zum lokalen Netzwerk. Damit sind zwei unterschiedliche physische Netzwerke etabliert. Die Firewall dient den Clients als Router und schützt über verschiedene Filtermechanismen das lokale Netzwerk vor unbefugten Zugriffen. Die Firewall des ISA-Server ist zwar in der Lage, auch auf Applikationsebene die Pakete zu überprüfen. Jedoch kann dennoch aufgrund von Sicherheitslücken ein modifiziertes Paket durch die Firewall gelangen und Schaden anrichten.

6.1.2 Aufbau einer DMZ

Dieses Verfahren ist sicherer als der Einsatz einer Firewall. In diesem Szenario verfügt die Firewall über drei Netzwerkkarten (im Falle einer DSL-Verbindung. Verfügen Sie über eine ISDN-Karte oder ein Analogmodem, so wird dieses anstelle der dritten Netzwerkkarte verwendet). Dabei wird die erste Netzwerkkarte für die Herstellung der Internetverbindung genutzt. Das Internet wird auch als öffentliches Netzwerk bezeichnet.

An die zweite Netzwerkkarte erfolgt der Anschluss der Computer, auf die direkt vom Internet aus zugegriffen werden darf. Dieser Bereich wird als Demilitarisierte Zone (DMZ) bezeichnet, da der Zugriff über die Firewall erfolgt und somit bereits ein Angriff erschwert wird.

An die dritte Netzwerkkarte werden sämtliche Clients und Server angeschlossen, auf die nicht aus dem Internet zugegriffen werden darf. Diese Computer sind ebenfalls durch die Firewall abgesichert. Man spricht hier auch vom privaten Netzwerk.

Damit die Sicherheit der DMZ auch umgesetzt wird, wird zwischen dem privaten Netzwerk und der DMZ sowie der DMZ und dem öffentlichen Netzwerk Routing durchgeführt. Sämtliche Clientanfragen werden über die DMZ weitergeleitet. Das direkte Routing zwischen dem privaten und öffentlichen Netzwerk ist nicht möglich. Der Internetzugriff der Benutzer kann nur über einen Proxy-Server erfolgen. Dieser kann entweder gemeinsam mit der Firewall installiert werden oder wird in der DMZ eingerichtet. Die IP-Adresse des Proxy-Servers muss in die Konfiguration des Internet Explorers der Clients eingetragen werden.

6.1.3 Eine DMZ mit zwei Firewalls

Dieses Szenario wird in Umgebungen angewendet, die sehr sicherheitskritisch sind. Hierbei wird die DMZ durch eine Firewall geschützt, die sich zwischen der DMZ und dem öffentlichen Netzwerk befindet, und durch eine zweite Firewall, die sich zwischen der DMZ und dem privaten Netzwerk befindet. Gegenüber der Lösung mit nur einer Firewall ist hier der Zugriff auf das private Netzwerk durch die zweite Firewall wesentlich erschwert. Im Szenario mit nur einer Firewall kann ein Angreifer auch in das private Netzwerk gelangen, sofern er die DMZ und die Firewall ausgehebelt hat.

6.1.4 Welche Gefahren können durch den ISA-Server erkannt werden?

Heutzutage gibt es eine Reihe von Gefahren, die im Internet lauern. Die meisten Angriffe sind darauf ausgerichtet, unberechtigt Informationen zu sammeln, Server oder deren Dienste zu blockieren oder bestimmte Daten zu modifizieren. Im Folgenden finden Sie eine Auflistung der häufigsten Gefahren.

Auslesen unverschlüsselter Daten

Ein sehr hoher Risiko stellt das Senden von unverschlüsselten Daten über das Internet dar, da diese jederzeit abgefangen und ausgelesen werden können. Zwischenzeitlich wurde dieses Problem minimiert, indem es für zahlreiche Protokolle Zusätze gibt, die auch eine verschlüsselte Übertragung der Daten ermöglichen. Bei einer verschlüsselten Kommunikation besteht jedoch das Problem, dass eine Firewall wegen der Verschlüsselung manipulierte IP-Pakete nicht mehr erkennen kann. Der ISA-Server ist jedoch in der Lage, die Verschlüsselung des Servers zu verwenden. Damit ist er in der Lage, auf der Firewall die Daten zu entschlüsseln, zu überprüfen und nach der Überprüfung wieder zu verschlüsseln und zu senden.

IP Half Scan

Bei dieser Form des Angriffs werden an den Server Pakete mit einem gefälschten Absender geschickt. Der Server versucht, diese Pakete zu bestätigen. Da er von dem gefälschten Absender keine Antwort erhält, versucht er dies immer wieder und gerät in eine Endlosschleife, da er gleichzeitig eine Reihe weiterer dieser gefälschten Pakete erhält. Auch diese Form des Angriffs kann mit Hilfe von IP-Paketfiltern erkannt werden.

Land

Bei einer Landattacke wird an den Server ein Paket gesendet, das als verfälschte Absenderadresse die Zieladresse angibt. Somit erhält der Server quasi sein eigenes Paket, das er bestätigt. Dabei ergibt sich eine Endlosschleife, die den Server auslastet. Auch diese Angriffsform kann über IP-Paketfilter erkannt werden.

WinNuke

Diese Form der Attacke wird auch als Windows out-of-band bezeichnet. Dabei werden veränderte TCP-Pakete vornehmlich an die NetBIOS-Schnittstelle des Servers gesendet, um einen Absturz des Servers zu provozieren. Diese Form des Angriffs kann über IP-Paketfilter leicht erkannt werden. Allerdings sollten Sie generell darüber nachdenken, ob in Ihrem Netzwerk das NetBIOS-Protokoll noch erforderlich ist. Im Rahmen des Active Directory wurde NetBIOS durch DNS abgelöst und ist dafür nicht mehr erforderlich. Prüfen Sie, ob bestimmte Anwendungen zwangsweise dieses Protokoll noch erfordern.

Ping of Death

Mit einer Denial of Service-Attacke (DoS-Attacke) wird ein Server so attackiert, dass er aufgrund von Überlastung nicht mehr reagieren kann. Hierbei handelt es sich um das so genannte *Ping of Death*. Dabei wird der herkömmliche Ping-Befehl so modifiziert, dass

IP-Pakete mit unzulässigen Größen gesendet werden. Abhilfe schafft hier einerseits die Einstellung, dass Server im internen Netzwerk keine Ping-Befehle mehr annehmen können. Allerdings können dennoch weitere DoS-Attacken auf die Ports erfolgen, die Sie für die Kommunikation der Server im Netzwerk benötigen. Der ISA-Server nutzt dagegen seine Filtermechanismen, um IP-Pakete gezielt herauszufiltern. Über das ISA-SDK (Software Development Kit) können zudem Anpassungen vorgenommen werden, um auf neue Paketeigenschaften reagieren zu können.

Portscans

Ein Portscan wird über so genannte Portscanner durchgeführt. Diese Scanner analysieren, welche Ports vom Server verwendet werden, um so in das System eindringen zu können. Besonders gern werden diese Portscanner eingesetzt, wenn die Server so konfiguriert sind, dass diese nicht mehr die Standardports verwenden. Der ISA-Server ist in der Lage, einerseits über Filter nur an bestimmte Ports und IP-Adressen das Senden von Daten zuzulassen. Andererseits ist der ISA-Server auch in der Lage, bei einem erkannten Portscan die Ausgangs-IP-Adresse zu ermitteln.

SMTP-Relaying

Bei dieser Form wird ein fremder SMTP-Server für das Senden von Massen-E-Mails benutzt. Über das SMTP-Relaying sendet eine Person an den SMTP-Server eine Nachricht, die an diverse Empfänger in anderen Domänen als der des SMTP-Servers versendet werden soll. Diese Massensendung wird dann über den missbrauchten SMTP-Server durchgeführt, so dass dieser als Absender erscheint und zudem auch die Kosten für den Massen-E-Mail-Versand nicht vom eigentlichen Absender zu zahlen sind. Hiergegen erfolgt ein Schutz, indem nur noch die E-Mails über den SMTP-Server versendet werden, die auch für diesen bestimmt sind. Lediglich die Benutzer der eigenen E-Mail-Domäne können noch E-Mails über das Internet versenden.

6.1.5 Betriebsmodus des ISA-Servers

Der ISA-Server kann in drei verschiedenen Betriebsmodi ausgeführt werden. Je nachdem, ob Sie den Server als Firewall oder Proxy einsetzen, ist ein Betriebsmodus definiert. Gerade in kleinen und mittleren Unternehmen wie im Umfeld des SBS 2003 werden Sie jedoch den dritten Betriebsmodus, den integrierten Modus, ausführen. Dabei werden der Proxy und die Firewall gemeinsam auf einem Computer installiert, in unserem Fall also auf dem Server des SBS-Netzwerks.

6.2 Die Installation des ISA Servers 2000

Dieses Kapitel beschreibt die Installation des ISA-Servers. Zum besseren Verständnis finden Sie vorweg eine Übersicht über die verschiedenen Komponenten des ISA Servers 2000.

6.2.1 Die Komponenten des ISA-Servers

Der ISA-Server besteht aus verschiedenen Services und Konfigurationstools. Die Kernkomponente des ISA-Servers sind die *ISA-Services*. Diese werden immer installiert, der Inhalt ist davon abhängig, ob Sie den ISA-Server als Firewall oder Proxy oder beides einsetzen. Eine weitere Komponente sind die *Add-in-Services*. Diese bestehen aus dem *H.323 Gatekeeper-Service* sowie dem *Message-Screener*. Der *Message-Screener* dient dem Filtern von Dateianhängen nach einem Dateinamen oder einem bestimmten Text innerhalb einer E-Mail. Mit Hilfe dieses Tools ist es möglich, bereits auf einen bestimmten Virus zu reagieren und com-Netzwerk fern zu halten, bevor eine Lösung vom Antiviren-Hersteller angeboten wird. Der *H.323 Gatekeeper-Service* wird bei Audio- und Videokonferenzen über NetMeeting verwendet. Die Installation dieser beiden Komponenten ist optional.

Außer den Services bietet der ISA-Server die *ISA-Management-Konsole* für die zentrale Verwaltung des Servers sowie das *H.323 Gatekeeper-Administration-Tool* für die Verwaltung des Gatekeeper-Services.

6.2.2 Die Installation des ISA-Servers

Nachdem Sie die Installation vorbereitet haben, kann diese nun durchgeführt werden.

1. Nach Einlegen der CD SBS 2003 Premium Technologies starten Sie die Installation des ISA-Servers über den entsprechenden Link.
2. Nach dem Hinweis, alle geöffneten Programme zu beenden, wird Ihnen die Microsoft Produkt-ID des ISA-Servers angezeigt. Diese Nummer sollten Sie sich aufschreiben, da Sie diese später zu möglichen Supportzwecken benötigen. Danach müssen Sie noch dem Lizenzvertrag zustimmen. Die Eingabe einer Lizenznummer ist nicht erforderlich. Danach wird geprüft, ob bereits eine Installation des ISA-Servers oder einiger seiner Komponenten vorhanden ist.
3. Danach bestimmen Sie, ob Sie eine Standardinstallation, vollständige oder benutzerdefinierte Installation durchführen möchten. Nur im letzten Fall können Sie selbst die zu installierenden Komponenten wählen. Standardmäßig erfolgt die Installation im Verzeichnis \PROGRAMME\MICROSOFT ISA SERVER. Sie können jedoch auch ein anderes Installationsverzeichnis wählen. Die Installation des ISA-Servers belegt nur circa 17 MB. Klicken Sie dann auf die Schaltfläche der gewünschten Installationsart.

Der Installationspfad bezieht sich nur auf die Programmdateien. Der Speicherort für den Cache des Proxys wird später (siehe Schritt 7.) bestimmt.

4. Haben Sie die benutzerdefinierte Installation gewählt, können Sie nun die gewünschten Komponenten auswählen. Um für ZUSÄTZLICHE DIENSTE und VERWALTUNGSPROGRAMME weitere Komponenten zu installieren, klicken Sie auf OPTION ÄNDERN. Haben Sie alle zu installierenden Komponenten ausgewählt, klicken Sie auf WEITER.

5. Als Nächstes wählen Sie den Betriebsmodus des ISA-Servers aus. Sie haben die Wahl zwischen FIREWALLMODUS, CACHEMODUS und INTEGRIERTER MODUS. In unserem Beispiel wird der Server im integrierten Modus installiert. Im weiteren Verlauf dieses Kapitels wird der integrierte Modus vorausgesetzt, da sich dieser in der SBS-Umgebung anbietet. Klicken Sie dann auf WEITER.
6. Sie erhalten dann das Informationsfenster, dass der IIS-Veröffentlichungsdienst (W3SVC) angehalten wurde. Nach Abschluss der ISA-Installation muss der IIS so konfiguriert werden, dass dieser nicht mehr die Standardports 80 und 8080 verwendet, da diese nun vom ISA-Server benutzt werden. Bestätigen Sie diese Meldung mit OK.
7. Danach bestimmen Sie den Speicherort für den Cache für den Proxy (siehe Abbildung 6.1).

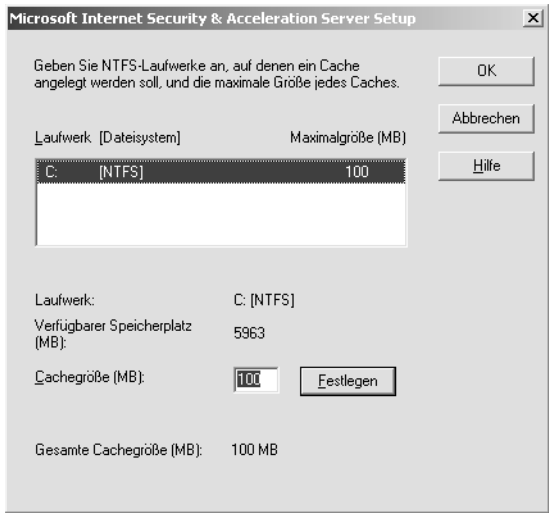


Abbildung 6.1: Den Speicherort für den Cache des Proxy-Servers festlegen

Dabei muss es sich um ein Laufwerk mit dem NTFS-Dateisystem handeln. Sie können den Cache auch auf mehrere Laufwerke verteilen. Dadurch wird die Leistung des ISA-Servers erhöht. Markieren Sie jeweils ein Laufwerk und tragen den maximalen Wert für die Cachegröße in das entsprechende Feld ein und klicken auf FESTLEGEN. Klicken Sie dann auf OK.

Um den Cache nachträglich verwalten zu können, benutzen Sie das Programm *Cachedir.exe*. Allerdings müssen Sie dieses nach Abschluss der Installation manuell aus dem Verzeichnis SUPPORT/TOOLS/TROUBLESHOOTING der CD in das Installationsverzeichnis des ISA-Servers kopieren.

8. Dann müssen Sie dem ISA-Server die IP-Bereiche des privaten und öffentlichen Netzwerks beibringen (siehe Abbildung 6.2).

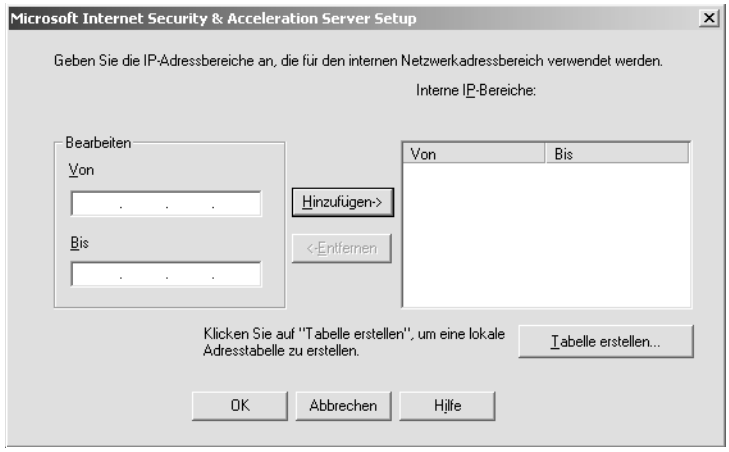


Abbildung 6.2: Das Bestimmen der privaten IP-Adressbereiche für den ISA-Server

Tragen Sie dazu den Adressbereich des privaten Netzwerks in die Felder VON und BIS ein und klicken dann auf HINZUFÜGEN. Auf diese Art können Sie auch mehrere private Netzwerke hinzufügen. Die hier von Ihnen eingegebenen Informationen werden auf dem ISA-Server in die *Local Address Table* (LAT) eingetragen. Alle IP-Adressen, die sich nicht in dieser Tabelle befinden, werden als öffentliche IP-Adressen angesehen. Um diese Tabelle zu erstellen, klicken Sie auf TABELLE ERSTELLEN. Sie erhalten dann das Fenster LOKALE ADRESSTABELLE.

9. In diesem Fenster können Sie zusätzliche Adressbereiche zur LAT hinzufügen (siehe Abbildung 6.3).

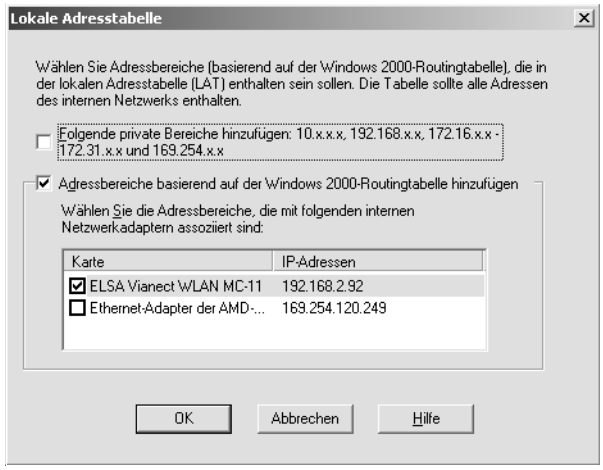


Abbildung 6.3: Die weiteren Konfigurationsmöglichkeiten der LAT

Über die obere Checkbox können Sie die Adressbereiche hinzufügen, die als private Netzwerkadressen reserviert sind. Dazu zählen die Bereiche 10.x.x.x, 192.168.x.x, 172.16.x.x bis 172.31.x.x sowie 169.254.x.x. Über die zweite Checkbox können Sie die Adressbereiche basierend auf der Windows-Routingtabelle hinzufügen. Achten Sie jedoch darauf, nur die Netzwerkkarten auszuwählen, die eine Verbindung zum privaten Netzwerk herstellen. Klicken Sie dann auf OK. Sie erhalten eine Meldung, dass die LAT nun erstellt wurde. Danach wird die Installation durchgeführt.

Der Assistent „Erste Schritte"

Nach Abschluss der Installation haben Sie die Möglichkeit, den Assistenten ERSTE SCHRITTE zu starten. Dieser Assistent unterstützt Sie beim Erstellen von Sicherheitsrichtlinien und Cachekonfigurationen für das Netzwerk. Dessen Konfigurationsoptionen werden in Kapitel Abbildung 6.3.1. beschrieben

Die Konfiguration des IIS ändern

Ist auf dem SBS 2003 vor der Installation des ISA-Servers bereits ein Webserver in Betrieb gewesen, so wird dieser wie schon erwähnt während der Installation des ISA-Servers angehalten. Dies liegt darin begründet, dass der ISA-Server die Ports des Webservers selbst benutzt. Um den Webserver wieder zu aktivieren, müssen Sie zunächst dem virtuellen www-Server einen anderen Port zuweisen und danach die IIS-Dienste neu starten. Bei einem Aufruf der auf dem Webserver liegenden Seiten nimmt nun der ISA-Server anstelle des Webservers die Anfragen entgegen und leitet diese dann an den Webserver weiter.

Installierte Dienste des ISA-Servers

Nach der Installation werden auf dem Server die folgenden neuen Dienste ausgeführt. Je nach Auswahl der Komponenten kann es zu Abweichungen kommen.

Dienstname	Beschreibung
Microsoft Firewall	Dies ist der Dienst für die Firewall-Komponente des ISA-Servers.
Microsoft H.323 Gatekeeper	Dienst für den Gatekeeper, der als Schnittstelle für Dienste mit dem H.323-Standard (z.B. NetMeeting) zwischen dem privaten und öffentlichen Netzwerk fungiert.
Microsoft ISA-Server Control	Hierbei handelt es sich um den zentralen Dienst des ISA-Servers, der die übrigen Dienste steuert.
Microsoft Scheduled Cache Content Download	Der Dienst ist für das Forward-Caching zuständig. Dabei werden die gecachten Dateien überprüft, ob sie noch aktuell sind, und dann bei Bedarf neu geladen.
Microsoft Web Proxy	Dieser Dienst ist für die Zwischenspeicherung der Daten zuständig, die via http oder FTP übertragen worden sind.

Tabelle 6.1: Die Dienste des ISA Servers 2000

6.3 Die Verwaltung des ISA-Servers

In diesem Kapitel werden Sie mit den umfangreichen Verwaltungsoptionen des ISA-Servers vertraut gemacht. Zur Grundkonfiguration sollten insbesondere Administratoren, die noch nicht mit dem ISA-Server vertraut sind, den Assistenten „Erste Schritte“ verwenden. Die weitere Konfiguration des Servers wird über die ISA-Verwaltungskonsole vorgenommen. Auch diese wird im folgenden Kapitel vorgestellt.

6.3.1 Der Assistent „Erste Schritte“ und die Grundkonfiguration

Dieser Assistent führt Sie durch grundlegende Einstellungsoptionen des ISA-Servers. Dazu werden sämtliche Schritte der Aufgabenliste zum Punkt VERBINDUNG MIT DEM INTERNET HERSTELLEN nochmals abgearbeitet. Die ausführliche Beschreibung dazu haben Sie bereits in Kapitel 2.7.2 gelesen.

Die Steuerung und Verwaltung des ISA-Servers erfolgt über die mmc ISA-VERWALTUNG unter PROGRAMME/MICROSOFT ISA SERVER (siehe Abbildung 6.4).

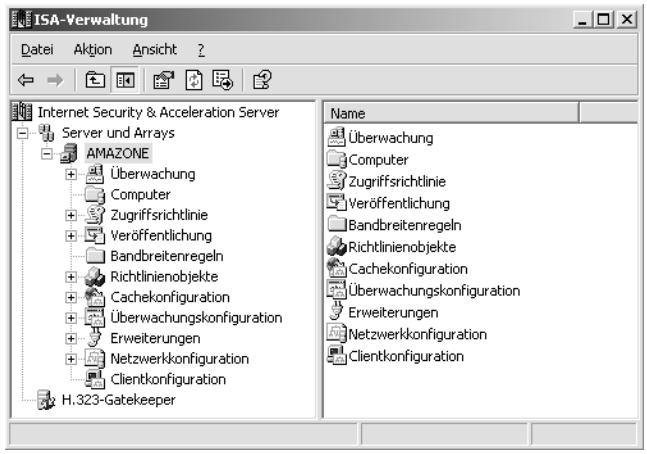


Abbildung 6.4: Die Verwaltungskonsole des ISA-Servers

Bevor Sie mit weiteren Arbeitsschritten beginnen, sollten Sie die Ansichtsoption dieser Konsole auf die erweiterte Ansicht umstellen. Wählen Sie dazu im Menü ANSICHT den entsprechenden Eintrag.

Nach der Installation müssen Sie einige grundlegende Verwaltungsschritte durchführen. Dazu zählen die Konfiguration des Routings sowie das Einrichten einer Wählverbindung (falls vorhanden).

Die Routing-Konfiguration

Standardmäßig ist aus Sicherheitsgründen das Weiterleiten von Paketen vom privaten Netzwerk ins Internet deaktiviert. Diese Routing-Funktion aktivieren Sie, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie die Eigenschaften von ZUGRIFFSRICHTLINIE/IP-PAKETFILTER und wechseln auf die Registerkarte ALLGEMEIN.
2. Dort aktivieren Sie die Checkbox PAKETFILTERUNG AKTIVIEREN sowie IP-ROUTING AKTIVIEREN.

Das Aktivieren der Routing-Funktion ist nur dann sinnvoll, wenn die Funktion auch benötigt wird. Wird der ISA-Server als Proxy-Server eingesetzt, ist dies nicht nötig, da die Clients die Anfragen an den Proxy-Server stellen und dieser die Anfrage an den Zielserver herstellt.

Haben Sie das Routing unter dem ISA-Server konfiguriert, darf die Routing-Funktion des SBS 2003 nicht mehr aktiviert sein. Die Routing-Funktion des SBS 2003 könnte ansonsten die Sicherheitsmechanismen des ISA-Servers außer Kraft setzen.

Überprüfen Sie deshalb in der mmc ROUTING UND RAS, ob dort noch Schnittstellen eingetragen sind.

Konfiguration einer Wahlverbindung

Sofern auf dem SBS eine Wahlverbindung eingerichtet ist, muss diese auch entsprechend für den ISA-Server eingetragen werden. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie RICHTLINIENOBJEKTE/DFÜ-EINTRÄGE und wählen aus dem Kontextmenü NEU/DFÜ-EINTRAG.
2. Auf der Seite NEUER DFÜ-EINTRAG (siehe Abbildung 6.5) geben Sie einen Namen und eine Beschreibung ein. Unter NETZWERK-DFÜ-VERBINDUNG wählen Sie die Verbindung aus. Unter NETZWERK-DFÜ-KONTO klicken Sie auf KONTO FESTLEGEN und geben den Benutzernamen und das Kennwort für das DFÜ-Konto an. Klicken Sie dann auf OK.

Abbildung 6.5: Festlegen des DFÜ-Eintrags in der ISA-Konfiguration

Routing und Wahlverbindung

Als Letztes müssen Sie noch das Routing für die Wahlverbindung einrichten. Dies ist auch notwendig, wenn die Wahlverbindung nur als Redundanz für eine temporär nicht verfügbare Standleitung dienen soll.

1. Öffnen Sie NETZWERKKONFIGURATION/ROUTING. Aus dem Kontextmenü von STANDARDREGEL wählen Sie den Eintrag EIGENSCHAFTEN.
2. Wechseln Sie auf die Registerkarte AKTION (siehe Abbildung 6.6). In aller Regel können Sie den Eintrag DIREKT VOM ANGEGEBENEN ZIEL ABRUFEN beibehalten. Die Einstellungen für den Upstream-Server sind nur dann notwendig, wenn der Internet-Provider einen Webproxy verwendet, da er nicht den Zugriff auf alle Internet-Server gestattet. Dies ist jedoch in der Regel nicht der Fall. Sollte dies doch zutreffen, müssen Sie den Webproxy des Internet-Providers als Upstream-Server eintragen.

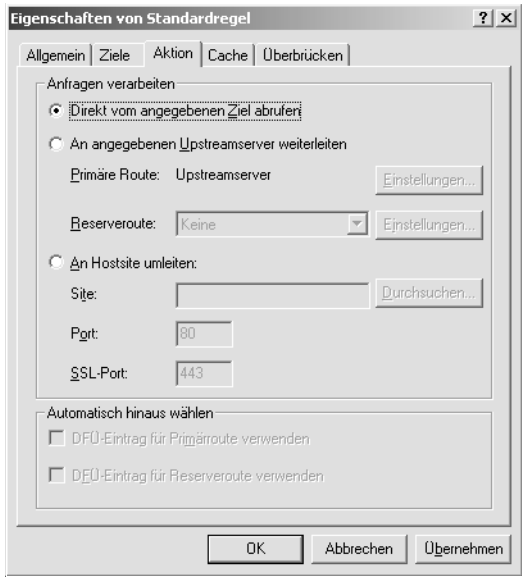


Abbildung 6.6: Konfiguration der Routing-Funktion

Schließlich legen Sie unter AUTOMATISCH HINAUS WÄHLEN noch fest, wann die Route verwendet werden soll. Ist die Route nur als Ausweichleitung konzipiert, markieren Sie die zweite Checkbox, dient Sie als Hauptroute, wählen Sie die obere Checkbox.

6.4 Die Filterfunktionen des ISA-Servers

Die wichtigste Funktion des ISA-Servers ist die Überwachung des Datenverkehrs zwischen dem lokalen Netzwerk und dem Internet. Für die Überwachungs- und Kontrollfunktionen werden verschiedene Filter und Regeln eingesetzt. Zunächst sind diese Filter bzw. Regeln so konfiguriert, dass sämtliche Verbindungen über den ISA-Server untersagt sind. Damit wird erreicht, dass ein Administrator alle erlaubten Verbindungen quasi

als Ausnahme konfigurieren muss. Wären zunächst alle Verbindungen gestattet und wäre es Aufgabe des Administrators, die nicht erlaubten Verbindungen einzurichten, so wäre die Gefahr zu groß, dass Sicherheitslücken verbleiben würden.

Die vorhandenen Filter- und Regelfunktionen sind Protokollregeln, Site- und Inhaltsregeln sowie IP-Paketfilter und Applikationsfilter.

6.4.1 Protokollregeln

Die Protokollregeln werden verwendet, wenn die Clients den Proxy-Client verwenden und der ISA-Server entsprechend als Proxy-Server konfiguriert ist. Dabei wird der Proxy-Server als Standard-Gateway für die Clients eingetragen. Eine Protokollregel legt fest, welche Protokolle der Client verwenden darf.

1. Wählen Sie aus dem Kontextmenü von ZUGRIFFSRICHTLINIE/PROTOKOLLREGELN den Eintrag NEU/REGEL und geben dieser einen Namen.
2. Dann legen Sie fest, ob die Antwort auf Clientanfragen mit dem Protokoll der Regel zugelassen oder verweigert werden soll. Klicken Sie dann auf WEITER.
3. Im Fenster PROTOKOLLE bestimmen Sie, für welche Protokolle die Regel angewendet werden soll. Haben Sie dort die Option AUSGEWÄHLTE PROTOKOLLE gewählt, können Sie aus der Liste die Protokolle auswählen (siehe Abbildung 6.7). Klicken Sie dann auf WEITER.

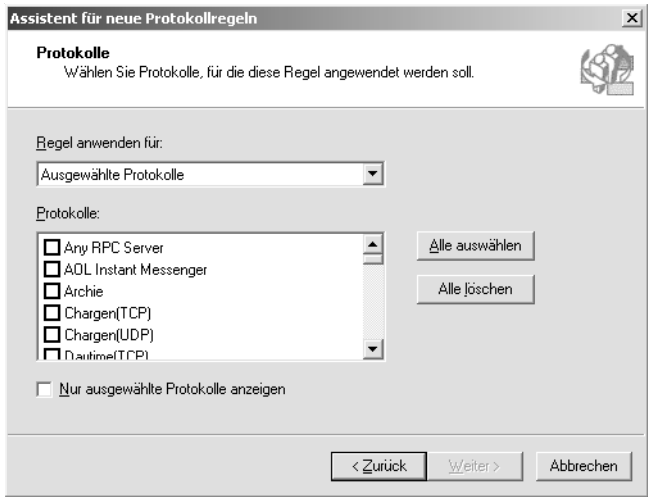


Abbildung 6.7: Auswahl der Protokolle, für welche die Protokollregel gelten soll

4. Als Nächstes entscheiden Sie, ob diese Regel immer angewendet werden soll (Standard) oder nach den Zeitplänen „Normale Arbeitszeit“ bzw. „Wochenende“. Eine genaue Einstellung der beiden Optionen ist jedoch nicht möglich. Klicken Sie dann auf WEITER.

5. Als Letztes bestimmen Sie noch, für welchen Clienttyp diese Regel gelten soll. Sie können entweder die Option JEDE ANFRAGE wählen oder bestimmte Computer bzw. Benutzer und Gruppen. Haben Sie die Option JEDE ANFRAGE gewählt, klicken Sie auf WEITER und stellen den Assistenten fertig. Anderenfalls wählen Sie die Computer bzw. Benutzer aus, auf welche die Regel angewendet werden soll, und schließen dann den Assistenten ab.

6.4.2 Site- und Inhaltsregeln

Diese Art von Regeln wird verwendet, um den Benutzer in seinen Zugriffsmöglichkeiten im Internet einzuschränken. Sie können damit den Zugriff auf bestimmte Seiten einschränken sowie den Download bestimmter Dateitypen untersagen. Für Letzteres müssen so genannte Inhaltsgruppen angelegt werden. Dieses Verfahren wird im übernächsten Unterkapitel beschrieben.

1. Wählen Sie aus dem Kontextmenü von ZUGRIFFSREGEL/SITE- UND INHALTSREGELN den Eintrag NEU/REGEL und geben dieser einen Namen.
2. Danach legen Sie fest, ob die Antwort auf die Clientanfrage zugelassen oder verweigert werden soll. Standardmäßig wird diese verweigert. Sie können zudem eine URL angeben, auf der Sie dem Benutzer beispielsweise (in netter Form) mitteilen, dass er auf die angeforderte Seite vom Firmennetzwerk aus nicht gehen darf. Klicken Sie dann auf WEITER.
3. Als Nächstes bestimmen Sie, ob die Regel basierend auf dem aufgerufenen Ziel, einem Zeitplan oder bestimmten Clients greifen soll. Auch eine benutzerdefinierte Regelung kann erfolgen. Dabei gibt es die folgenden Optionen:

   ZIEL:

   - ALLE ZIELE: Die Regel wird für alle Zielserver angewendet.
   - ALLE INTERNEN ZIELE: Die Regel wird für alle Server des internen Netzwerks angewendet. Die Zugehörigkeit der Server ergibt sich aus der LAT (siehe).
   - ALLE EXTERNEN ZIELE: Die Regel wird auf alle externen Server, d.h. alle außerhalb des lokalen Netzwerks, angewendet.
   - ANGEGEBENEN ZIELSATZ: Hierbei wird aus einem so genannten Zielsatz ausgewählt. In einem Zielsatz sind verschiedene IP-Adressen zu einer Gruppe zusammengefasst. Das Erstellen eines Zielsatzes wird im folgenden Unterkapitel beschrieben. Nach der Installation des SBS 2003 steht Ihnen beispielsweise der Zielsatz SMALL BUSINESS EXCHANGE OWA DESTINATION SET zur Verfügung.
   - ALLE ZIELE AUSSER DEM AUSGEWÄHLTEN SATZ: Dies ist die Umkehrung der vorherigen Option. Die Regel wird auf alle Server außer denen des gewählten Satzes angewendet.

   ZEIT: Als Zeitplan können Sie wieder „Immer“, „Normale Arbeitszeit“ sowie „Wochenende“ auswählen. Eine genauere Bestimmung der Zeitpläne ist nicht möglich.

   CLIENTS: Hier können Sie bestimmen, ob die Regel für alle Anfragen gelten soll oder ob sie nur für bestimmte Computer bzw. Benutzer und Gruppen gelten soll. Diese können nachfolgend ausgewählt werden.

Haben Sie im Fenster REGELKONFIGURATION BENUTZERDEFINIERT gewählt, können Sie nacheinander für Ziel, Zeit und Clients die Einstellungen vornehmen.

Anlegen von Zielsätzen

1. Um einen neuen Zielsatz zu erstellen, wählen Sie aus dem Kontextmenü von RICHTLINIENOBJEKTE/ZIELSÄTZE den Eintrag NEU/FESTLEGEN.
2. Im Fenster NEUER ZIELSATZ geben Sie einen Namen und eine optionale Beschreibung für den Zielsatz an. Über HINZUFÜGEN wählen Sie die Elemente des Zielsatzes aus (siehe Abbildung 6.8).

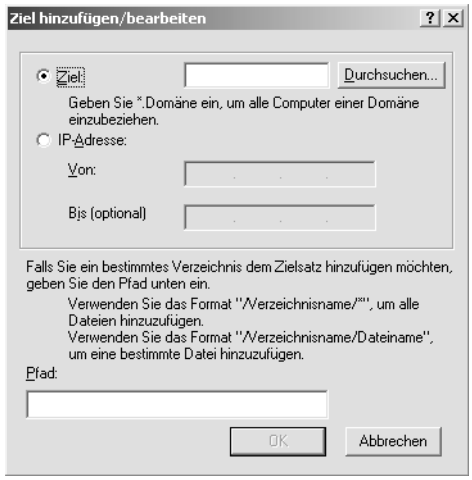


Abbildung 6.8: Hinzufügen von Computern oder IP-Adressen zu einem Zielsatz

Sie können entweder die Computer domänenbasiert oder IP-Adressen-basiert auswählen. Zudem können Sie auch ein Verzeichnis auswählen. Klicken Sie dann auf OK.

Zudem können vorhandene Zielsätze bearbeitet und entfernt werden.

Anlegen von Inhaltsgruppen

Mit Hilfe von Inhaltsgruppen können Sie Benutzer daran hindern, dass sie bestimmte Dateitypen downloaden. Um eine neue Inhaltsgruppe anzulegen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü von RICHTLINIENOBJEKTE/INHALTSGRUPPEN den Eintrag NEU/INHALTSGRUPPE und geben dieser zunächst einen Namen.
2. Aus der Liste VERFÜGBARE TYPEN (siehe Abbildung 6.9) wählen Sie dann die Dateitypen aus und klicken auf HINZUFÜGEN. Ist ein Dateityp nicht darin vorhanden, können Sie diesen auch manuell in das Textfeld eintragen.

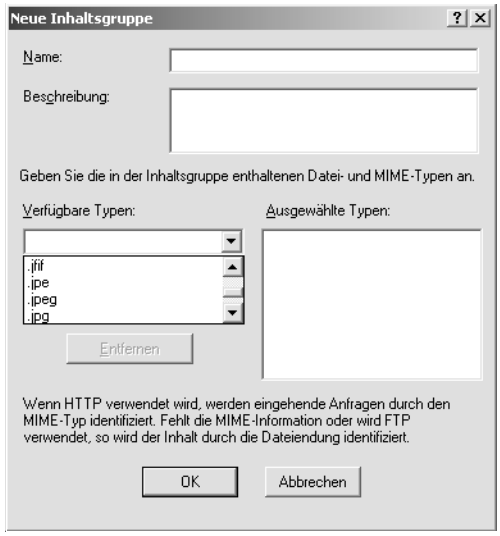


Abbildung 6.9: Auswahl der Datei- und MIME-Typen, die der Benutzer nicht downloaden darf

Außer Dateitypen können Sie auch bestimmte MIME-Typen auswählen. Dabei gibt beispielsweise der MIME-Typ *audio/midi* an, dass es sich um eine Audiodatei handelt. Und diese wird genauer durch den Typ midi spezifiziert.

Um bestimmte Typen aus der Liste wieder zu löschen, klicken Sie auf ENTFERNEN.

6.4.3 Die IP-Paketfilter

IP-Paketfilter werden eingesetzt, um Daten zu filtern, die an den ISA-Server gesendet, von diesem gesendet sowie über diesen geroutet werden. Um die IP-Paketfilterung zu aktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die EIGENSCHAFTEN von ZUGRIFFSRICHTLINIE/IP-PAKETFILTER und wechseln auf die Registerkarte PAKETFILTER.
2. Auf dieser Seite können Sie die Grundlagen der Filterung festlegen. Über FILTERN VON IP-FRAGMENTEN AKTIVIEREN stellen Sie sicher, dass auch die Pakete gefiltert werden, die zwar einzeln ungefährlich sind, jedoch aus den Fragmenten wieder zusammengesetzt ein bösartiges Datenpaket darstellen können. Markieren Sie FILTERN VON IP-OPTIONEN AKTIVIEREN, werden auch die IP-Header, die auch als IP-Optionen bezeichnet werden, gefiltert, so dass auch über diese keine schadenbringenden Pakete ins Netzwerk gelangen können. Mit PAKETE VON ZULASSUNGSFILTERN PROTOKOLLIEREN werden zusätzlich noch die Pakete kontrolliert, die laut Filtereinstellung den Filter passieren dürfen. Klicken Sie dann auf OK.

Wie Sie unter IP-Paketfilter sehen, sind bereits standardmäßig einige IP-Filter vom ISA Server angelegt worden. Den Status eines Filters erkennen Sie an dem jeweiligen Symbol. Ein deaktivierter Filter ist mit einem kleinen roten Pfeil versehen. Die vordefinierten Filter lassen DNS-Abfragen sowie ICMP (für Ping-Funktion) zu.

1. Möchten Sie einen neuen Filter erstellen, wählen Sie aus dem Kontextmenü von IP-PAKETFILTER den Eintrag NEU/FILTER.
2. Zunächst geben Sie dem Filter einen Namen. Danach bestimmen Sie, ob der Filter eine Übertragung der Daten zulassen oder sperren soll. Klicken Sie dann auf WEITER.
3. Auf der Seite FILTERTYP bestimmen Sie, ob Sie einen benutzerdefinierten oder einen vordefinierten Filter erstellen möchten. In der Liste der vordefinierten Filter finden Sie eine Auswahl der wichtigsten Verbindungen (siehe Abbildung 6.10).

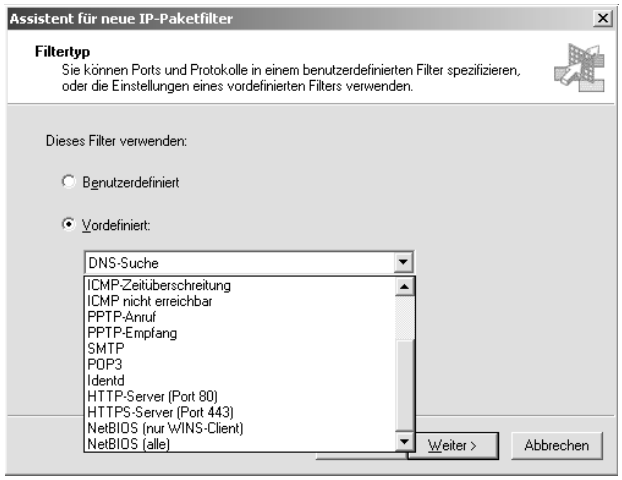


Abbildung 6.10: Auswahl der vordefinierten Verbindungen für den IP-Paketfilter

Möchten Sie hingegen einen benutzerdefinierten Filter erstellen, so müssen Sie dafür das Protokoll, die Nummer, die Richtung sowie den lokalen und Remoteport angeben (siehe Abbildung 6.11).

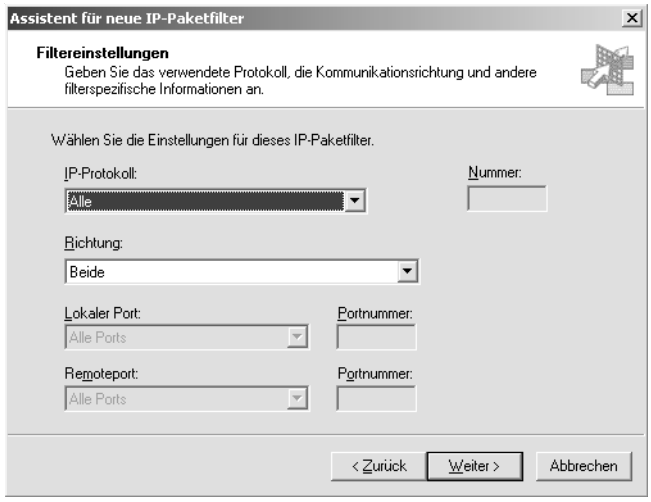


Abbildung 6.11: Erstellen eines benutzerdefinierten Protokolls für den IP-Filter

Da die Filterung auf IP-Adressen und Ports zurückgreift, finden Sie in der folgenden Tabelle als Hilfestellung eine Übersicht über die wichtigsten Protokolle und zugehörigen Nummern.

Nummer	Protokoll	Nummer	Protokoll	Nummer	Protokoll
0	HOPOPT	46	RSVP	95	MICP
1	ICMP	47	GRE	96	SCC-SP
2	IGMP	48	MHRP	97	ETHERIP
3	GGP	49	BNA	98	ENCAP
4	IP	50	ESP	100	GMTP
5	ST	51	AH	101	IFMP
6	TCP	52	I-NLSP	102	PNNI
7	CBT	53	SWIPE	103	PIM
8	EGP	54	NARP	104	ARIS
9	IGP	55	MOBILE	105	SCPS
10	BBN-RCC-MON	56	TLSP	106	QNX
11	NVP-II	57	SKIP	107	A/N
12	PUP	58	IPv6-ICMP	108	IPComp
13	ARGUS	59	IPv6-NoNxt	109	SNP
14	EMCON	60	IPv6-Opts	110	Compaq-Peer
15	XNET	62	CFTP	111	IPX-in-IP
16	CHAOS	64	SAT-EXPAK	112	VRRP
17	UDP	65	KRYPTOLAN	113	PGM
18	MUX	66	RVD	115	L2TP
19	DCN-MEAS	67	IPPC	116	DDX
20	HMP	69	SAT-MON	117	IATP
21	PRM	70	VISA	118	STP
22	XNS-IDP	71	IPCV	119	SRP
23	TRUNK-1	72	CPNX	120	UTI
24	TRUNK-2	73	CPHB	121	SMP
25	LEAF-1	74	WSN	122	SM
26	LEAF-2	75	PVP	123	PTP
27	RDP	76	BR-SAT-MON	124	ISIS
28	IRTP	77	SUN-ND	125	FIRE
29	ISO-TP4	78	WB-MON	126	CRTP
30	NETBLT	79	WB-EXPAK	127	CRUDP

Nummer	Protokoll	Nummer	Protokoll	Nummer	Protokoll
31	MFE-NSP	80	ISO-IP	128	SSCOPMCE
32	MERIT-INP	81	VMTP	130	SPS
33	SEP	82	SECURE-VMTP	131	PIPE
34	3PC	83	VINES	132	SCTP
35	IDPR	84	TTP	133	FC
36	XTP	85	NSFNET-IGP	255	Reserviert
37	DDP	86	DGP		
38	IDPR-CMTP	87	TCF		
39	TP++	88	EIGRP		
40	IL	89	OSPFIGP		
41	IPv6	90	Sprite-RPC		
42	SDRP	91	LARP		
43	IPv6-Route	92	MTP		
44	IPv6-Frag	93	AX.25		
45	IDRP	94	IPIP		

Tabelle 6.2: Übersicht über die verschiedenen Protokolltypen und Nummern

4. Nachdem Sie den Filter konfiguriert haben, müssen Sie bestimmen, für welche IP-Adressen er angewendet werden soll. Sie haben die Wahl, alle IP-Adressen der externen Serverschnittstellen zu wählen (Standard), nur eine externe IP-Adresse oder für einen bestimmten Computer des Netzwerks. Klicken Sie dann auf WEITER.
5. Danach wählen Sie aus, auf welche Remote-Computer der Filter angewendet werden soll. Standardmäßig lautet die Einstellung ALLE REMOTE-COMPUTER. Sie können jedoch auch nur einen bestimmten Remote-Computer angeben. Klicken Sie auf WEITER und stellen den Assistenten fertig.

Um über den IP-Paketfilter zu ermitteln, ob ein Angriff stattfindet, müssen Sie zunächst auf der Registerkarte ALLGEMEIN unter ZUGRIFFSRICHTLINIE/IP-PAKETFILTER die Checkbox ERKENNUNG VON EINDRINGVERSUCHEN AKTIVIEREN markieren.

Danach wechseln Sie auf die Registerkarte EINDRINGVERSUCHSERKENNUNG (siehe Abbildung 6.12) und markieren dort die Checkboxen der Angriffe, die über den ISA-Server erkannt werden sollen.

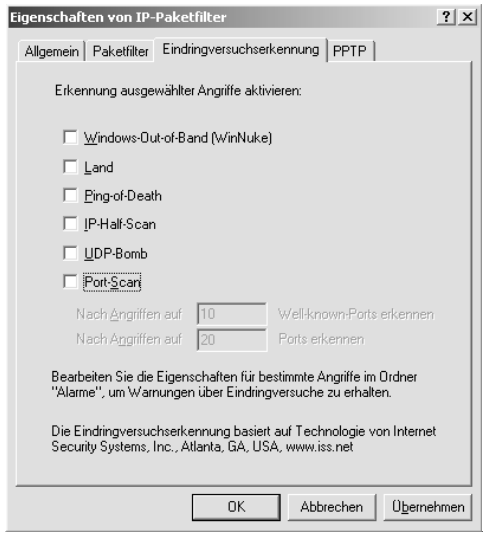


Abbildung 6.12: Die Auswahl der zu überwachenden Angriffsarten

Die verschiedenen Formen der Angriffe wurden bereits in Kapitel Abbildung 6.1.4 erläutert. An dieser Stelle nur noch einige Worte zur Einstellung des Portscans. Ist diese Option ausgewählt, können Sie die Anzahl der Angriffe einstellen, die als Attacke gewertet werden soll. Die Well-known-Ports stellen den Bereich von 1 bis 2048 dar. Dieses ist der Bereich, der am häufigsten von Serverdiensten verwendet wird. Deshalb ist hier standardmäßig auch ein kleinerer Wert gesetzt als für die restlichen Ports.

6.4.4 Applikationsfilter

Die Applikations- bzw. Anwendungsfilter werden eingesetzt, um die Dienste selbst zu schützen, die für die Übertragung bestimmter Pakete zuständig sind. Beispielsweise können so der http-, DNS- oder SMTP-Dienst geschützt werden. Der ISA-Server verfügt bereits über eine Reihe von Applikationsfiltern. Diese finden Sie unter ERWEITERUNGEN/ANWENDUNGSFILTER. Hier sehen Sie auch, ob ein Filter aktiviert ist oder nicht. Ist er deaktiviert, ist er mit dem Symbol eines roten Pfeils im weißen Kreis versehen. Über das Kontextmenü des Filters können Sie diese aktivieren und deaktivieren.

Zusätzliche Filter außer den hier vordefinierten können Sie von einigen Drittanbietern erhalten. Eine Übersicht über diese weiteren Applikationsfilter finden Sie unter *http://www.microsoft.com/isaserver/partners*.

Im Folgenden werden die Einstellmöglichkeiten der Applikationsfilter kurz beschrieben.

DNS Intrusion Detection Filter

Diese Form des Angriffs besteht darin, dass an einen DNS-Server so große Datenmengen gesendet werden, dass es zu einem Überlauf des DNS-Speichers kommt. Sofern hier seitens der Programmierung keine Speicherbegrenzung gesetzt ist, können weitere Speicherbereiche überschrieben werden, wodurch es zum Absturz des Servers kommt.

Dieser Filter ist in der Lage, die folgenden Angriffsversuche am DNS-Server zu erkennen:

- DNS-HOSTNAMENÜBERLAUF: Für die DNS-Anfragen werden gezielt zu lange Hostnamen angegeben.
- DNS-LÄNGENÜBERLAUF: Die standardmäßige Länge einer IP-Adresse beträgt vier Byte. Für den Angriff wird ein größerer Wert benutzt.
- DNS-ZONENÜBERTRAGUNG VON PRIVILEGIERTEN PORTS (1–1024): Bei einer Zonenübertragung wird die DNS-Datenbank von einem DNS-Server auf einen anderen übertragen und abgeglichen. Liegt der Port dabei im Bereich zwischen 1 und 1024 , stellt in der Regel ein regulärer DNS-Server diese Anfrage. Mit Hilfe des Filters kann dieses überprüft werden.
- DNS-ZONENÜBERTRAGUNG VON HOHEN PORTS (ÜBER 1024): Wird einer der hohen Ports benutzt, erfolgt die Anfrage in der Regel von einem Client aus. Der Filter kann auch dieses überprüfen.

FTP Access Filter

Dieser Filter ist wichtig für die reinen textbasierten FTP-Clients, bei denen keine Proxy-Einstellungen vorgenommen werden können. Der ISA-Server wird als so genannter *transparenter Proxy* eingesetzt. Wie auch für einen Webserver werden die FTP-Anfragen an Port 21 zunächst an den ISA-Server gesendet, der die Anfrage dann an den FTP-Server weiterleitet. Für diesen Filter sind keine weiteren Optionen verfügbar.

H.323-Filter

Dieser Filter ist in erster Linie für die Steuerung von Diensten wie Microsoft NetMeeting zuständig. Wenn Sie diese Dienste nicht verwenden, muss der Filter auch nicht aktiviert werden. Sofern zwischen zwei Netzwerken aufgrund einer Firewall keine routbare Verbindung besteht, müssen Sie den Gatekeeper verwenden. Dieser fungiert dann quasi als NetMeeting-Proxy. Wählen Sie dazu über DURCHSUCHEN den gewünschten Computer aus. Weiterhin können Sie festlegen, ob eingehende und/oder ausgehende Anrufe gestattet sind und welche Medien (Audio, Video) übertragen werden sollen.

http-Redirector-Filter

Über diesen Filter werden die Anfragen an den Webserver umgeleitet, da diese der ISA-Server entgegennimmt. Über die Optionen können Sie bestimmen, wie die Umleitung durchgeführt werden soll. Standardmäßig ist die Option AN LOKALEN WEBPROXY-DIENST UMLEITEN gesetzt. Über die entsprechende Checkbox können Sie festlegen, dass beim Ausfall des Proxy-Servers die Umleitung direkt an den Webserver erfolgen soll. Ist diese Checkbox nicht aktiviert, kann kein Zugriff auf den Webserver erfolgen. Möchten Sie die Proxy-Funktionalität nicht verwenden, aktivieren Sie die Option AN ANGEFORDERTEN WEBSERVER SENDEN. Sollen sämtliche Zugriffe auf den Webserver nur über den Proxy-Server erfolgen, markieren Sie die Checkbox HTTP-ANFRAGEN VON FIREWALL- UND SECURENAT-CLIENTS VERWERFEN.

POP-Intrusion-Detection-Filter

Dieser Filter überprüft die Daten, die an den POP-Server gesendet werden, damit nicht der interne Pufferspeicher des POP-Servers durch zu große Datenmengen überschrieben wird. Für diesen Filter sind keine weiteren Optionen verfügbar.

RPC-Filter

Dieser Filter wird nicht zum Schutz vor Attacken benutzt. Ist dieser Filter aktiviert, können Server veröffentlicht werden, die das RPC-Protokoll (Remote Procedure Call) verwenden. Für diesen Filter gibt es keine weiteren Optionen.

SMTP-Filter

Standardmäßig ist dieser Filter deaktiviert, da er viel Rechenkapazität auf dem ISA-Server erfordert. Dies liegt darin begründet, dass sowohl die Befehle an den SMTP-Server als auch die Inhalte der E-Mails überprüft werden. Wenn Sie den Filter aktivieren, muss der Firewall-Dienst neu gestartet werden. Sie können dabei entscheiden, ob dieser sofort automatisch oder später manuell neu gestartet werden soll. Die Änderungen werden jedoch erst nach dem Neustart der Firewall wirksam.

Dieser Filter besitzt die umfangreichsten Einstellmöglichkeiten. Über die Registerkarte SCHLÜSSELWÖRTER können Sie die E-Mails nach bestimmten Inhalten durchsuchen. Klicken Sie dazu auf HINZUFÜGEN und geben das Schlüsselwort ein. Wählen Sie dann, ob nach diesem Wort im Nachrichtentitel oder -textfeld bzw. nur im Titel oder Textfeld gesucht werden soll. Dann wählen Sie über AKTION aus, ob die entsprechende E-Mail gelöscht, gehalten oder weitergeleitet werden soll. Haben Sie mehrere Schlüsselwörter ausgewählt, können Sie auch die Priorität der Abarbeitungsreihenfolge bestimmen.

Über BENUTZER/DOMÄNEN können Sie bestimmte Absender herausfiltern und somit blockieren. Unter SENDERNAME können Sie spezielle E-Mail-Adressen angeben, unter DOMÄNENNAME sämtliche Adressen einer E-Mail-Domäne sperren. Diese E-Mails werden nicht mehr an den Exchange-Server weitergeleitet und müssen somit dort auch nicht über den Spamfilter heraussortiert werden.

Auf der Registerkarte ANHÄNGE können Sie über HINZUFÜGEN die Dateianhänge angeben, gemäß denen die E-Mail nicht übertragen werden soll. Sie können dabei sowohl den Namen eines Anhangs, einen Dateityp oder ein Größenlimit festsetzen. Weiterhin können Sie unter AKTION festlegen, ob die entsprechende Nachricht gelöscht, gehalten oder weitergeleitet werden soll. Haben Sie mehrere Kriterien gewählt, kann für diese zudem eine Reihenfolge der Abarbeitung festgelegt werden.

Unter SMTP-BEFEHLE können Sie SMTP-Befehle, die für die Kommunikation zwischen Client und Server verwendet werden, aktivieren, deaktivieren und bearbeiten. Doppelklicken Sie dazu den jeweiligen Befehl und bestimmen, ob dieser Befehl aktiviert ist oder nicht. Zudem können Sie auch die maximale Länge des Befehls in Byte angeben. Damit wird verhindert, dass an einen harmlosen SMTP-Befehl weitere „bösartige“ Parameter angefügt werden können.

SOCKS V4-Filter

Eine Applikation kann über TCP/IP entweder direkt auf einen Server zugreifen oder über einen Proxy-Server. Für die zweite Option dient der ISA-Server als SOCKS V4-Proxy-Server. Damit können beispielsweise Mailclients über den Proxy-Server verwendet werden. Über die Optionen können Sie einen Port für die Kommunikation bestimmen.

Streaming-Media-Filter

Unter Streaming Media versteht man, dass eine Audio- bzw. Videodatei nicht erst komplett downgeloadet und danach abgespielt wird, sondern bereits während des Downloads abgespielt wird. Dazu unterstützt der ISA-Server die Protokolle MMS für den Windows Media Player, RTSP für den RealPlayer G2 sowie QuickTime und PNM für den RealPlayer. Zudem müssen auf dem Server die Windows Media Services installiert sein.

Um die Übertragung der gesplitteten Mediadateien zu gestatten, wählen Sie die Option AKTIVE DATENSTRÖME MIT EINEM LOKALEN WMT-SERVER AUFTEILEN. Die Standardeinstellung untersagt das Übertragen der Daten. Sind die Media Services nicht direkt auf dem ISA-Server installiert, müssen Sie zusätzlich das Benutzerkonto mit Kennwort für diese Dienste angeben.

6.5 Die Überwachungsfunktion des ISA-Servers

Nachdem nun auf dem ISA-Server die Filter und Richtlinien konfiguriert worden sind, geht es nun daran, die ermittelten Angriffe zu registrieren und auszuwerten, um dem Angreifer auf die Spur zu kommen.

Die Einstellungen dazu werden unter ÜBERWACHUNGSKONFIGURATION/ALARME vorgenommen. Dort finden Sie bereits eine umfangreiche Liste vordefinierter Alarme. Um einen bestimmten Alarm zu konfigurieren, doppelklicken Sie diesen. Die Konfiguration geschieht dann über die Registerkarten EREIGNISSE und AKTION.

Unter EREIGNISSE (siehe Abbildung 6.13) können Sie unter EREIGNIS auch ein anderes als das aktuell gewählte bestimmen. Weiterhin geben Sie dort die ANZAHL DER WIEDERHOLUNGEN und/oder die EREIGNISANZAHL PRO SEKUNDE an, bevor der Alarm ausgelöst wird. Werden Aktionen wiederholt, können Sie festlegen, ob diese sofort, nach dem Zurücksetzen des Alarms oder nach einem bestimmten Intervall wieder ausgeführt werden sollen.

Auf der Registerkarte AKTIONEN (siehe Abbildung 6.14) können Sie dann festlegen, welche Ereignisse nach dem Auslösen des Alarms ausgeführt werden sollen.

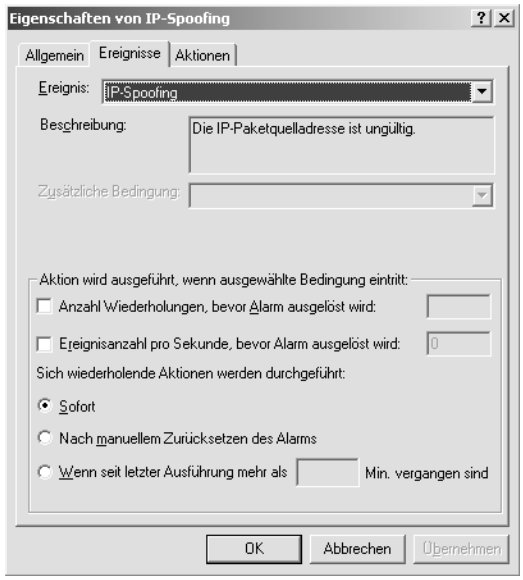


Abbildung 6.13: Das Festlegen der zu überwachenden Ereignisse

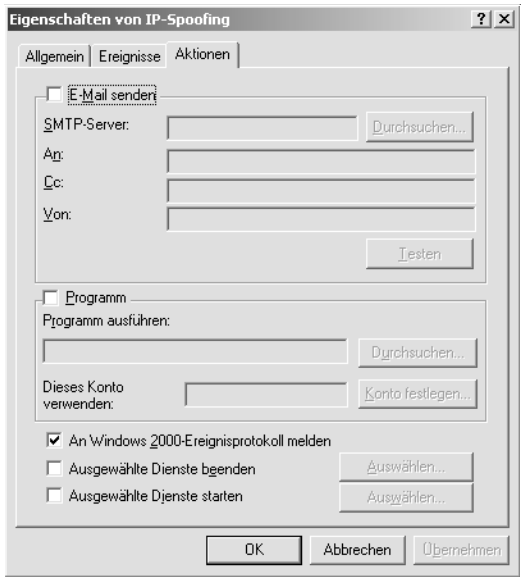


Abbildung 6.14: Einstellung der Aktionen nach einem ermittelten Angriff

Sie haben die Auswahl, eine E-Mail zu versenden. Dazu geben Sie den SMTP-Server sowie den oder die Empfänger an. Zusätzlich oder alternativ können Sie auch ein Programm ausführen. Ist für dieses Programm ein anderes Konto erforderlich, können Sie

auch dieses angeben. Standardmäßig ist bereits die Option aktiviert, den Alarm in das Ereignisprotokoll des Betriebssystems aufzunehmen. Sie können auch noch bestimmte Dienste nach Auslösung des Alarms starten oder beenden.

Zusätzlich zu den vordefinierten Alarmen können Sie diese auch neu benutzerdefiniert erstellen. Wählen Sie dazu aus dem Kontextmenü den Eintrag NEU/ALARM. In den Assistenten geben Sie alle eben beschriebenen gewünschten Einträge ein.

Um die aufgelaufenen Alarme betrachten zu können, für die keine spezielle Aktion konfiguriert wurde, wechseln Sie nach ÜBERWACHUNG/ALARME. Dort finden Sie die Alarme und Meldungen des ISA-Servers, die auch in das Windows-Ereignisprotokoll geschrieben werden.

6.6 Das Zusammenspiel zwischen dem ISA-Server und weiteren Servern

Nachdem Sie nun verschiedene systemimmanente Einstellmöglichkeiten des ISA-Servers kennen gelernt haben, geht es nun um das Zusammenspiel zwischen dem ISA-Server und weiteren Servern. Hier erfahren Sie die notwendigen Einstellungen, die am ISA-Server getroffen werden müssen, damit von außen auf die internen Server zugegriffen werden kann. Gerade im Umfeld des SBS 2003 müssen Sie beispielsweise für den Exchange-Server, einen Webserver oder auch einen Terminalserver den ISA-Server entsprechend konfigurieren. Man spricht hierbei auch vom Veröffentlichen von Servern.

Rein theoretisch könnten Sie jedem Server, auf den der Zugriff vom Internet aus erfolgen soll, eine reservierte, öffentliche IP-Adresse zuweisen. Die Adressumsetzung zwischen der privaten und öffentlichen Adresse wird über NAT (Network Address Translation) geregelt. Der ISA-Server würde in diesem Fall lediglich als Router fungieren. Dagegen spricht jedoch der Kostenfaktor, der für die Reservierung mehrerer öffentlicher IP-Adressen entsteht. Sinnvoller ist es, nur für den ISA-Server eine öffentliche IP-Adresse zu registrieren. Sämtliche Anfragen werden zunächst an den ISA-Server geleitet, der diese dann an die einzelnen Server weiterleitet.

6.6.1 Webserver veröffentlichen

Bei der Anfrage an einen internen Webserver oder FTP-Server erfolgt diese an den ISA-Server. Dieser leitet danach die Anfrage an den Webserver weiter. Der ISA-Server verhält sich dabei nach außen hin wie ein „herkömmlicher" Webserver, der auf den Ports 80 und 443 (http und https) Anfragen entgegennimmt. Auf diese Weise wird verhindert, dass eine direkte Verbindung zwischen einem externen Client und dem Webserver hergestellt wird.

Da der ISA-Server hierfür als Proxy-Server arbeitet, müssen Sie während der Installation auch die Cache-Komponente ausgewählt haben. Die bloße Firewall-Funktionalität des ISA-Servers ist für diese Aufgabe nicht ausreichend.

Damit diese Weiterleitung auch funktioniert, müssen Sie zunächst in den DNS-Einstellungen die IP-Adresse des Webservers und FTP-Servers auf den ISA-Server setzen.

Grundkonfiguration

1. Öffnen Sie über das Kontextmenü die EIGENSCHAFTEN von SERVERNAME und wechseln auf die Registerkarte EINGEHENDE WEBANFRAGEN.
2. Unter IDENTIFIZIERUNG legen Sie fest, ob die Einstellungen für alle IP-Adressen des Servers oder nur für bestimmte gelten sollen. Danach legen Sie fest, welcher TCP-Port und SSL-Port verwendet werden soll. Sie sollten von den beiden Standardwerten 80 und 443 nur dann abweichen, wenn es sich um keinen öffentlichen Server handelt und nur die rechtmäßigen Benutzer die geänderten Ports kennen. In diesem Fall kann die Portänderung sogar zur Sicherheit beitragen. Die SSL-Verschlüsselung kann jedoch nur aktiviert werden, wenn zuvor ein Zertifikat installiert worden ist.

   Über KONFIGURIEREN können Sie festlegen, wie viele gleichzeitige Verbindungen möglich sind. Überlegen Sie sich hinsichtlich möglicher Bandbreiteneinschränkungen, ob Sie die Standardeinstellung, die kein Limit vorsieht, beibehalten möchten. Weiterhin können Sie festlegen, wann eine Verbindung getrennt werden soll, nachdem keine Daten mehr zwischen dem Client und Server übertragen worden sind. Standardmäßig erfolgt die Trennung nach zwei Minuten.

Soll am Webserver eine Authentifizierung der Benutzer durchgeführt werden, markieren Sie die Checkbox IDENTIFIZIERUNG VON NICHTAUTHENTIFIZIERTEN BENUTZERN ANFORDERN. Die Authentifizierung ist beispielsweise dann erforderlich, wenn Sie über Filter nur bestimmten Benutzern den Zugriff gestatten möchten.

Um die Authentifizierungseinstellungen zu bearbeiten, markieren Sie den Eintrag unter IDENTIFIZIERUNG und klicken auf BEARBEITEN. Sie erhalten dann das Fenster ABHÖRER HINZUFÜGEN/ENTFERNEN (siehe Abbildung 6.15).

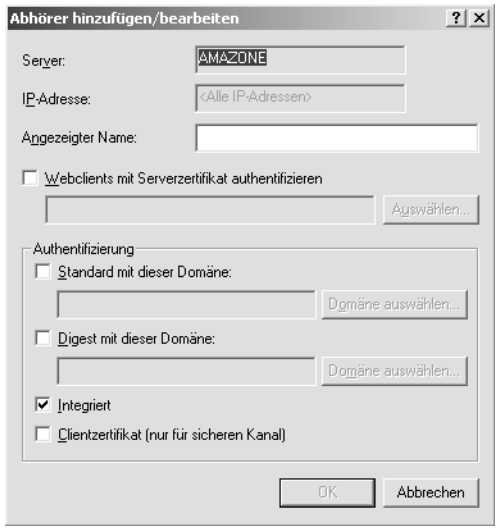


Abbildung 6.15: Konfiguration der Authentifizierungsmethoden

Im Textfeld ANGEZEIGTER NAME legen Sie einen Namen für die jeweilige Schnittstelle fest, beispielsweise Öffentlich, Privat und DMZ, wenn Sie drei Netzwerkkarten für den Anschluss ans LAN, WAN und die DMZ benutzen.

Sie können als Authentifizierungsart entweder ein Zertifikat oder eine der Arten Basisauthentifizierung, Digest-Authentifizierung oder Integrierte Windows-Authentifizierung auswählen. Haben Sie zuvor die SSL-Verschlüsselung aktiviert, müssen Sie nun die Checkbox markieren und ein Zertifikat auswählen. Haben Sie eine Form der Authentifizierung gewählt, fordert der ISA-Server den Benutzer zur Eingabe des Benutzernamens und Kennworts auf, bevor eine Weiterleitung an den Webserver erfolgt.

Konfiguration der Weiterleitung

Standardmäßig ist keine Weiterleitung von Anfragen an den Webserver gestattet. Es gibt nur eine Standardregel, die sämtliche Anfragen verweigert. Die Weiterleitung muss zunächst über eine neue Regel gestattet werden. Hierzu führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü von VERÖFFENTLICHUNG/WEBVERÖFFENTLICHUNGSREGELN den Eintrag NEUE REGEL und geben der Regel einen Namen.
2. Danach geben Sie an, ob diese Regel für alle Ziele, alle internen, externen oder für einen Zielsatz bzw. für alle außer dem Zielsatz gelten soll. Die Beschreibung dieser Optionen haben Sie bereits bei der Konfiguration einer Site- und Inhaltsregel in Kapitel Abbildung 6.4.2 kennen gelernt. Klicken Sie dann auf WEITER.
3. Dann bestimmen Sie, ob die Regel für alle Anfragen oder nur die bestimmter Computer oder Benutzer gelten soll. Diese können Sie dann auswählen. Klicken Sie dann auf WEITER.
4. Auf der Seite REGELAKTION bestimmen Sie, ob die Anfrage verweigert oder an den internen Webserver weitergeleitet werden soll. Im zweiten Fall tragen Sie den Namen oder die IP-Adresse des Webservers ein. Zudem bestimmen Sie die Ports für http, SSL und FTP. Klicken Sie dann auf WEITER und stellen den Assistenten fertig.

Nachdem Sie mehrere Regeln erstellt haben, können Sie über die Kontextmenüeinträge NACH OBEN und NACH UNTEN die Abarbeitungsreihenfolge der Regeln verändern.

6.6.2 Exchange Server veröffentlichen

1. Um einen Mailserver – in unserem Beispiel gehen wir von dem Exchange Server des SBS 2003 aus – zu veröffentlichen, wählen Sie aus dem Kontextmenü von VERÖFFENTLICHUNG/SERVERVERÖFFENTLICHUNGSREGEL den Eintrag MAILSERVER SICHERN.

Damit Sie die Konfiguration durchführen können, müssen Sie bei einer Wahlverbindung zunächst die Internetverbindung herstellen, damit Sie eine IP-Adresse vom Internetdienstanbieter zugewiesen bekommen.

2. Danach wählen Sie für die Protokolle EINGEHENDES und AUSGEHENDES SMTP, EXCHANGE/OUTLOOK, POP3, IMAP4 sowie NNTP aus, ob diese die Standardauthentifizierung oder die SSL-Authentifizierung verwenden sollen. Für SMTP können Sie zusätzlich noch den Inhaltsfilter aktivieren. Klicken Sie dann auf WEITER.

3. Dann wählen Sie die externe IP-Adresse, über die der Mailserver erreicht werden soll. Die Definition interner und externer Adressen geschieht mittels der LAT. Danach geben Sie die IP-Adresse des Mailservers an. Da unter SBS 2003 der Exchange Server auf demselben Computer wie der ISA-Server ausgeführt wird, wählen Sie die Option LOCALHOST.

Während der Fertigstellung wird für den Mailserver ein IP-Paketfilter für die Maildienste auf dem ISA-Server eingerichtet. Würde sich der Mailserver auf einer separaten Maschine befinden, würde eine Serververöffentlichungsregel für den Mailserver eingerichtet werden.

6.6.3 Weitere Server veröffentlichen

Für alle anderen Server außer einem Web-/FTP-Server und einem Mailserver müssen Sie selber eine Regel erstellen, wenn Sie diesen veröffentlichen möchten. Bei diesen zusätzlichen Servern kann es sich beispielsweise um einen Terminalserver oder einen SQL-Server handeln.

1. Wählen Sie aus dem Kontextmenü von VERÖFFENTLICHUNG/SERVERVERÖFFENTLICHUNGSREGELN den Eintrag NEU/REGEL und geben dieser einen Namen.
2. Im Fenster ADRESSZUWEISUNG tragen Sie die IP-Adresse des internen Servers sowie die externe IP-Adresse des ISA-Servers ein. Bei der externen Adresse muss es sich um eine handeln, die nach der LAT nicht als interne Adresse definiert ist. Klicken Sie dann auf WEITER.
3. Als Nächstes wählen Sie das Protokoll aus, das Sie auf dem Server veröffentlichen möchten. Sie können hierbei nur aus den vorgegebenen Einträgen wählen. Die in dieser Liste enthaltenen Einträge basieren auf den Applikationsfiltern (siehe Kapitel Abbildung 6.4.4). Erst wenn dort neue Filter hinzugefügt werden, sind hier auch weitere Protokolle wählbar. Klicken Sie dann auf WEITER.
4. Schließlich entscheiden Sie noch, ob die Regel für die Anfragen aller Clients oder nur bestimmter Computer gelten soll. Klicken Sie dann auf WEITER und beenden den Assistenten.

6.7 Der Firewall-Client des SBS 2003

Der Firewall-Client lässt sich im Zuge der an die Clients verteilbaren Applikationen auf diese heraufbringen. Sobald ein Firewall-Client installiert ist, sichert dieser die Internetnutzung des Clients.

Sämtliche Anforderungen des Firewall-Clients werden an den Firewall-Dienst des ISA-Servers weitergeleitet. Über den Firewall-Dienst wird entschieden, ob der Client diesen Zugriff ausführen darf oder nicht. Die Anforderungen des Firewall-Clients können z.B. über Applikationsfilter überprüft werden. Bei der Anforderung eines http-Objekts wird die Anforderung über den http-Redirector-Dienst an den Webproxy-Dienst (des ISA-Servers) weitergeleitet. Der Webproxy-Dienst leitet das angeforderte Objekt schließlich an den Client weiter.

6.7.1 Die Installation des Firewall-Clients

Nachdem die Installation des ISA Servers 2000 abgeschlossen ist, müssen Sie den Firewall-Client für den Internetzugriff auf die Clientcomputer verteilen.

1. Zunächst erstellen Sie einen freigegebenen Ordner für die Installationsdateien des Firewall-Clients. Wechseln Sie dazu im Windows Explorer in das Verzeichnis \PROGRAMME\MICROSOFT ISA SERVER\CLIENTS.
2. Klicken Sie auf den freigegebenen Ordner CLIENTS. Sie erhalten das Fenster FREIGABEEIGENSCHAFTEN.
3. Auf der Registerkarte SICHERHEIT klicken Sie auf HINZUFÜGEN. Wählen Sie dann die Benutzergruppe DOMÄNENBENUTZER aus und klicken auf ÜBERNEHMEN.

Um den Firewall-Client für die Clients bereitzustellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf dem SBS die Serververwaltung und doppelklicken auf CLIENTCOMPUTER.
2. Wählen Sie dann CLIENTANWENDUNGEN EINRICHTEN.
3. Im Fenster VERFÜGBARE ANWENDUNGEN klicken Sie auf HINZUFÜGEN.
4. Im Fenster ANWENDUNGSINFORMATIONEN geben Sie unter ANWENDUNGSNAME Firewall-Client an und den Pfad *\\SBSServername\MspcInt\Setup.exe*. Sie können die Datei auch über DURCHSUCHEN finden. Folgen Sie den weiteren Anweisungen des Assistenten.
5. Sobald Sie aufgefordert werden, diese neue Anwendung des Clients zuzuweisen, bestätigen Sie dies mit JA. Es erscheint der Assistent zum Zuweisen von Applikationen.

Dieser Assistent kann lediglich für die Zuweisung von Clientanwendungen an Clients unter Windows XP und 2000 verwendet werden. Von allen anderen Client-Betriebssystemen aus müssen Sie auf diesen manuell eine Verbindung zur Freigabe *\\SBSServername\MspcInt\Setup.exe* herstellen und den Firewall-Client manuell installieren.

Sobald sich ein Benutzer auf einem Clientcomputer anmeldet, findet er auf dem Desktop das Symbol für die Installation des Firewall-Clients.

Sobald dieses Symbol doppelgeklickt wird, erfolgt die Installation des Firewall-Clients. Dabei wird automatisch die Verbindung über den ISA-Server hergestellt.

6.8 Die Proxy-Funktion des ISA-Servers

Neben der Firewall-Funktion kann der ISA-Server auch als Proxy eingesetzt werden. Diese Funktion wurde bislang nur kurz angesprochen. Im Gegensatz zur Firewall sind hierzu auch nicht allzu viele Konfigurationseinstellungen möglich. Die Funktion des Proxy-Servers besteht in einem beschleunigten Internetzugriff für die Clients. Dieser Cache enthält häufig angeforderte Objekte, um somit den Netzwerkverkehr zu entlasten.

6.8.1 Konfigurieren des Proxy-Servers

Um den Proxy-Server zu konfigurieren, wechseln Sie auf die Registerkarte AUSGEHENDE WEBANFRAGEN in den Eigenschaften des Servers. Zunächst einmal bestimmen Sie hier wie schon bei den eingehenden Webanfragen (siehe Kapitel 6.6.1), ob die Einstellungen für alle internen IP-Adressen global oder einzeln konfiguriert werden sollen. Ändern Sie hier die Werte für den TCP-Port und SSL-Port, so müssen diese geänderten Einstellungen in die Browser der Clients übernommen werden.

Die Konfiguration der Authentifizierung und der Verbindungseinstellungen verläuft analog zu der der eingehenden Webanfragen. Lesen Sie dazu die Informationen in Kapitel 6.6.1.

6.8.2 Die Cachefunktion des Proxy-Servers

Für die Cachefunktion sind verschiedene Arten verfügbar. Am häufigsten wird sicherlich das Forward Caching verwendet, wobei die Objekte gespeichert werden, welche die Benutzer des lokalen Netzwerks bei der Internetkommunikation am häufigsten verwenden. Umgekehrt bietet der ISA-Server auch die Möglichkeit des Reverse-Caching. Dieses wird angewendet, wenn Benutzer von außen, etwa Benutzer des Remote-Desktops, auf die Ressourcen des lokalen Netzwerks zugreifen.

Insgesamt bietet der ISA Server 2000 fünf verschiedene Cache-Methoden. Diese sind neben den beiden eben bereits erwähnten Methoden Forward und Reverse Caching das Geplante Caching, Verteilte Caching sowie Hierarchische Caching. Diese Methoden werden im Folgenden näher beschrieben.

Forward Caching

Wie schon kurz erwähnt, wird das Forward Caching bei der Zugriffsrichtung interner Clients auf das Internet benutzt. Auf dem ISA-Server befinden sich die von den Benutzern am häufigsten angeforderten Internetobjekte. Diese Speicherung bietet für die Clients einen Geschwindigkeitsvorteil, da ihr Internetbrowser die Objekte, die von der Festplatte des ISA-Servers gelesen werden, schneller verarbeiten kann als die Daten, die direkt aus dem Internet bezogen werden müssen. Neben der kürzeren Antwortzeit des Internetbrowsers minimiert sich durch diese Methode auch die verwendete Bandbreite der Internetverbindung.

Technisch gesehen funktioniert das Forward Caching folgendermaßen: Client A besucht eine Internetseite und fordert ein bestimmtes Internetobjekt an. Auf dem ISA-Server wird über den Webproxy-Dienst ermittelt, ob sich dieses Objekt bereits im Cache befindet oder nicht. Sofern das Objekt noch nicht im Cache gespeichert ist, fordert der ISA-Server dieses Internetobjekt direkt von dem betreffenden Internetserver an. Dieser sendet das Objekt an den ISA-Server. Der ISA-Server speichert dieses Objekt in seinen Cache und reicht das Objekt an Client A weiter. Nun besucht Client B eine Internetseite und fordert dasselbe Objekt an. Der ISA-Server schaut wiederum in seinem Cache nach und findet dort das gewünschte Objekt. Er gibt es direkt aus seinem Cache an Client B zurück, ohne das Objekt dabei ein zweites Mal aus dem Internet anfordern zu müssen.

Reverse Caching

Das Reverse Caching verläuft technisch gesehen identisch mit dem eben beschriebenen Verfahren des Forward Caching. Der einzige Unterschied besteht darin, dass in diesem Fall der Client von außen auf die Webinhalte eines internen Servers zugreift.

Geplantes Caching

Das geplante Caching sollten Sie verwenden, wenn Sie die am häufigsten angeforderten Inhalte in den Cache des ISA-Servers downloaden möchten.

Verteiltes Caching

Das verteilte Caching spielt im Zusammenhang mit dem ISA-Server im Rahmen des SBS 2003-Netzwerks eine eher unbedeutende Rolle. Diese Methode wird benutzt, wenn Sie mehrere ISA-Server verwenden. In diesem Fall werden verschiedene ISA-Server als ein einziger logischer Cache zusammengefasst. Hierfür wird das Cache Array Routing Protocol (CARP) verwendet.

Hierarchisches Caching

Wie das verteilte Caching spielt auch das hierarchische Caching in unserem Zusammenhang eine eher unbedeutende Rolle und ist nur der Vollständigkeit halber erwähnt. Diese Methode verfeinert noch das verteilte Caching. Es können so verschiedene ISA-Server zu einer Hierarchie zusammengefügt werden. Damit wird es Benutzern möglich, immer auf den Cache zuzugreifen, der ihnen geografisch gesehen am nächsten ist.

6.8.3 Konfiguration des Cachings

Nachdem Sie einen Überblick über die verschiedenen Caching-Methoden des ISA-Server erhalten haben, wird nun die Konfiguration beschrieben. Hierbei wird nur auf die Konfiguration des für den SBS 2003 interessanten Forward und Reverse Cachings eingegangen. Die übrigen Einstellungen sind ähnlich. Für weitere Informationen dazu sei jedoch auf die Hilfe des ISA Server 2000 verwiesen.

1. Zur Konfiguration der Einstellungen öffnen Sie die EIGENSCHAFTEN von CACHEKONFIGURATION. Wechseln Sie auf die Registerkarte HTTP.
2. Standardmäßig ist das http-Caching mit der Installation des ISA-Servers aktiviert. Möchten Sie diese Funktion nicht verwenden, so deaktivieren Sie die Checkbox HTTP-ZWISCHENSPEICHERUNG ZULASSEN. Anderenfalls bestimmen Sie auf dieser Seite, wann die im Cache enthaltenen Objekte abgelaufen sind und deshalb aktualisiert werden sollen.

Die folgenden Einstellungen gelten nur, wenn das Objekt auf dem Webserver, von dem es angefordert wird, nicht mit einer eigenen Gültigkeitsdauer (Time to live, TTL) versehen ist.

Sie können entweder eine spezielle Gültigkeitsdauer festlegen oder die Optionen HÄUFIG, NORMAL oder SELTEN auswählen. Mit HÄUFIG wird bei jeder Anfrage an den ISA-Server das Objekt wieder neu vom Webserver geladen, während mit SELTEN nur wenige Übertragungen durchgeführt werden. Jedoch hat der Clientbenutzer die Möglichkeit, eine Aktualisierung über den ISA-Server zu erzwingen, indem er die Reload-Funktion des Webbrowsers (Internet Explorer) ausführt. Hierzu wird die Tastenkombination Strg + R verwendet.

6.9 Konfiguration für den OWA-Zugriff

Dieses Kapitel beschreibt, welche Konfigurationen Sie auf dem ISA-Server vornehmen müssen, um Zugriff auf die Exchange-Postfächer über Outlook Web Access (OWA) zu erhalten.

Der SBS 2003 stellt einen Assistenten bereit, damit Sie die entsprechenden Einstellungen vornehmen können. Um diesen zu starten, geben Sie unter Ausführen den Befehl `iwc` ein.

Zunächst einmal muss der ISA-Server so konfiguriert werden, dass er eingehende Webanfragen an seiner externen Schnittstelle generell akzeptiert. Um dies zu gewährleisten, führen Sie die folgenden Schritte aus:

1. In der mmc des ISA-Servers klicken Sie auf SERVER UND ARRAYS. Wählen Sie dann aus dem Kontextmenü des ISA Servers den Eintrag EIGENSCHAFTEN.
2. Wechseln Sie auf die Registerkarte EINGEHENDE WEBANFRAGEN. Klicken Sie dort auf ABHÖRER INDIVIDUELL PRO IP-ADRESSE KONFIGURIEREN.
3. Klicken Sie dann auf HINZUFÜGEN. Aus der Liste der verfügbaren ISA-Server wählen Sie den Server aus. Sie können hier die IP-Adresse und den Port angeben, der zum Beantworten der http-Anfragen verwendet werden soll. Bestätigen Sie die Eingabe mit OK und wechseln wieder in die ISA-mmc.

Als Zweites wird ein Zielsatz eingerichtet, über den die Clients auf die von der OWA-Webseite benutzten Ordner verwiesen werden können. Dazu sind die folgenden Schritte erforderlich:

1. Erweitern Sie den ISA-Server und klicken auf den Eintrag RICHTLINIENELEMENTE.
2. Erweitern Sie den Eintrag RICHTLINIENELEMENTE und wählen aus dem Kontextmenü von ZIELSATZ den Eintrag NEU und SATZ. Geben Sie dann einen Namen für den neuen Zielsatz an, z.B. OWA.
3. In das Feld ZIEL tragen Sie die URL ein, die von den externen Clients für den OWA-Zugriff verwendet wird. Die URL löst den Internet-DNS-Namen der externen IP-Adresse des ISA-Servers auf. Die URL muss ohne den Zusatz http:// oder https:// eingegeben werden.
4. In das Feld PFAD tragen Sie /exchange* ein. Klicken Sie dann auf OK.
5. Tragen Sie dann in das Feld PFAD /exchweb* für den Ordner Exchweb und /public* für die öffentlichen Ordner ein. Bestätigen Sie jeweils die Eingabe mit OK.

Als Nächstes wird die Webveröffentlichungsregel so konfiguriert, dass sie das eben angelegte Richtlinienelement benutzt. Dazu sind die folgenden Schritte erforderlich:

1. Erweitern Sie den Eintrag VERÖFFENTLICHUNG und wählen aus dem Kontextmenü von WEBVERÖFFENTLICHUNGSREGELN den Eintrag NEU und REGEL.
2. Als Namen für die neue Regel geben Sie beispielsweise OWA-Zugriffsregel an und klicken dann auf WEITER. Im Feld für den ZIELSATZ klicken Sie auf den zuvor erstellten OWA-Satz und klicken dann auf WEITER.
3. Stellen Sie mit der Auswahl JEDE ANFRAGE sicher, dass diese Regel für jede Webanfrage übernommen wird, und klicken dann auf WEITER.
4. Klicken Sie dann auf ANFRAGE AN INTERNEN WEBSERVER (NAME ODER IP-ADRESSE) UMLEITEN. Geben Sie dann die interne IP-Adresse an und *nicht* den Servernamen, da im SBS-Umfeld der ISA-Server auf demselben Server ausgeführt wird wie OWA. Werden beide Dienste auf verschiedenen Servern ausgeführt, können Sie auch den Servernamen angeben. Beim SBS 2003 besteht dann jedoch die Gefahr, dass der Servername an der externen IP-Adresse aufgelöst wird, so dass lediglich innerhalb des Netzwerks ein Zugriff auf OWA besteht, jedoch nicht für die externen Clients.

   Markieren Sie dann die Checkbox ORIGINAL HOSTHEADER ANSTELLE DES OBEN ANGEGEBENEN AN DEN VERÖFFENTLICHUNGSSERVER SENDEN. Klicken Sie dann auf WEITER und FERTIG STELLEN.
5. Erweitern Sie in der ISA-mmc den Eintrag ÜBERWACHEN und klicken dann auf DIENSTE.
6. Beenden Sie nun die Webproxy- und Firewall-Dienste, und starten Sie diese anschließend neu.
7. Um testweise auf den Server zuzugreifen, geben Sie in einem Browser die Adresse *http://URL/exchange* ein. Die URL ersetzen Sie durch die Adresse, die Sie im vorigen Kapitel unter Schritt 3 in das Feld ZIEL eingetragen haben.

Wird OWA über SSL-Verbindungen (Secure Sockets Layer) verwendet, so müssen Sie zusätzlich eine Serververöffentlichungsregel erstellen, welche die https-Serverprotokolldefinition verwendet. Danach geben Sie den internen OWA-Server sowie die externe Adresse des ISA-Servers an. Dabei muss der OWA-Server den ISA-Server als Standard-Gateway benutzen.

Um den OWA auf dem ISA-Server hosten zu können, muss auf diesem das Socket-Pooling deaktiviert werden. Standardmäßig ist dieses ab IIS 5.0 aktiviert, so dass der IIS gezwungen ist, alle IP-Adressen an Port 80 abzuhören. Um das Socket-Pooling zu deaktivieren, führen Sie die im folgenden Kapitel beschriebenen Schritte durch.

Nachdem das Socket-Pooling deaktiviert worden ist, wird die OWA-Seite so konfiguriert, dass die http-Anfragen an der internen Schnittstelle verarbeitet werden. Dazu sind die folgenden Schritte erforderlich:

1. Öffnen Sie die IIS-mmc. Wählen Sie aus dem Kontextmenü der Website, welche die OWA-Seite hostet, den Eintrag EIGENSCHAFTEN.
2. Aus der Liste der IP-Adressen wählen Sie die interne IP-Adresse des ISA-Servers aus. Bestimmen Sie dann den Port, den die OWA-Seite abfragen soll. Standardmäßig handelt es sich dabei um Port 80. Dieser Schritt ist erforderlich, da sich der IIS- und der ISA-Server unter dem SBS auf demselben Server befinden.

3. Weiterhin darf auf dem ISA-Server die automatische Suche nicht aktiviert sein, wenn Port 80 zum Beantworten der Anfragen benutzt wird. Um diese zu deaktivieren, öffnen Sie die ISA-mmc und wählen aus dem Kontextmenü des Servers den Eintrag EIGENSCHAFTEN. Wechseln Sie auf die Registerkarte AUTOMATISCHE SUCHE und deaktivieren dort die Checkbox AUTOMATISCHE SUCHINFORMATIONEN VERÖFFENTLICHEN.

Danach richten Sie einen Webabhörer, einen Zielsatz sowie eine Webveröffentlichungsregel wie oben beschrieben ein.

Deaktivieren des Socket-Poolings

Solange das Socket-Pooling aktiviert ist, was ab IIS 5.0 standardmäßig der Fall ist, werden vom IIS sämtliche IP-Adressen abgehört. Verfügt dabei eine Domäne über mehrere Netzwerke, so kann das Socket-Pooling u.U. zu einem Sicherheitsrisiko werden. Zum Deaktivieren des Socket-Poolings führen Sie die folgenden Schritte aus:

1. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis \INETPUB\ADMINSCRIPTS.
2. Geben Sie den folgenden Befehl ein:

   ```
   cscript adsutil.vbs set w3svc/disablesocketpooling true ↵
   ```

   Sie sollten danach die folgende Ausgabe erhalten:

   ```
   disablesocketpooling : (BOOLEAN) True
   ```

3. Danach müssen Sie den Dienst IIS-Verwaltungsdienst beenden und neu starten. Auch der Dienst WWW-Publishing-Dienst muss neu gestartet werden.

6.10 Veröffentlichen des Ordners http://Companyweb

Dieses Kapitel beschreibt die Veröffentlichung der internen Firmenwebseite *http://Companyweb*, wenn der ISA-Server eingesetzt wird. Ziel soll es sein, dass die externen Clients Zugriff auf diese Seite erlangen, indem sie die Adresse *https://FQDN des SBS 2003:444* oder alternativ über das Features des Remote-Webarbeitsplatzes die Adresse *https://FQDN des SBS 2003/remote* eingeben.

Vor der Veröffentlichung der Firmenwebseite müssen Sie eine Protokolldefinition und eine Server-Veröffentlichungsregel erstellen. Zusätzlich müssen Sie der Firmenwebseite ein Zertifikat hinzufügen. Zum Schluss werden einige Registry-Änderungen für den Remote-Webarbeitsplatz vorgenommen, so dass dieser auch vom Internet aus erreichbar ist.

6.10.1 Erstellen einer neuen Protokolldefinition

Um auf dem ISA Server 2000 eine neue Protokolldefinition zu erstellen, müssen Sie die folgenden Schritte durchführen:

1. Öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT ISA SERVER/ISA-VERWALTUNG.
2. Erweitern Sie den Eintrag RICHTLINIENELEMENTE, und wählen Sie aus dem Kontextmenü von PROTOKOLLDEFINITIONEN den Eintrag NEU und DEFINITION.

3. Auf der Willkommensseite des Assistenten geben Sie als Namen für die Protokolldefinition z.B. Companyweb 444 ein und klicken dann auf WEITER.
4. Im Fenster PRIMÄRE VERBINDUNGSINFORMATIONEN geben Sie unter PORTNUMMER der Wert 444 ein. Der Protokolltyp muss TCP sein. Aus der Liste DIRECTION wählen Sie INBOUND und klicken dann auf WEITER.
5. Im Fenster SEKUNDÄRE VERBINDUNGEN markieren Sie unter MÖCHTEN SIE SEKUNDÄRE VERBINDUNGEN BENUTZEN? den Eintrag NEIN und klicken auf FERTIG STELLEN.

6.10.2 Veröffentlichen des Companyweb

Um das Companyweb über den ISA-Server zu veröffentlichen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT ISA SERVER/ISA-VERWALTUNG.
2. Erweitern Sie dort den Eintrag VERÖFFENTLICHEN und wählen aus dem Kontextmenü von SERVER-VERÖFFENTLICHUNGSREGELN den Eintrag NEU und REGEL.
3. Geben Sie dann einen Namen für die neue Regal an, z.B. Companyweb, und klicken dann auf WEITER.
4. Tragen Sie unter IP-ADRESSE DES INTERNEN SERVERS die interne Netzwerkadresse des SBS 2003 ein. Danach tragen Sie unter EXTERNE IP-ADRESSE DES ISA-SERVERS die IP-Adresse für das Netzwerkgerät ein, das die externe Verbindung herstellt. Sie sollten als externe Adresse immer eine statische IP-Adresse verwenden. Anderenfalls müssen Sie die Veröffentlichungsrolle jedes Mal bearbeiten, wenn sich die dynamisch zugewiesene Adresse geändert hat. Klicken Sie dann auf WEITER.
5. Im Fenster PROTOKOLLEINSTELLUNGEN wählen Sie aus der Liste ANWENDEN DER REGEL AUF DIESES PROTOKOLL den Eintrag „Companyweb 444“. Hierbei muss es sich um den Namen des Protokolls handeln, das Sie wie im vorigen Kapitel beschrieben erstellt haben. Klicken Sie danach auf WEITER.
6. Auf der Seite CLIENTTYP wählen Sie aus der Liste ANWENDEN DER REGEL AUF ANFRAGEN VON den gewünschten Clienttyp aus. Erfolgen auf den Server Zugriffe von Clients über das Internet, so sollten Sie die Auswahl ALLE ANFRAGEN auswählen. Klicken Sie dann auf WEITER und FERTIG STELLEN.
7. Danach muss der ISA Server 2000-Firewall-Dienst beendet und neu gestartet werden. Öffnen Sie dazu in der ISA-mmc den Eintrag SERVERS UND ARRAYS, NAME DES ISA-SERVERS, ÜBERWACHUNG und klicken dann auf DIENSTE. In der rechten Fensterhälfte klicken Sie auf FIREWALL und wählen aus dem Kontextmenü BEENDEN und danach STARTEN.

Befindet sich der ISA-Server hinter einer zusätzlichen Hardware-Firewall, so müssen Sie sicherstellen, dass der Port 444 auf dieser freigeschaltet ist.

6.10.3 Vergabe eines Webserver-Zertifikats

Im nächsten Schritt müssen Sie ein Webserver-Zertifikat für *http://Companyweb* über die IIS hinzufügen. Dazu sind die folgenden Aktionen erforderlich:

1. Öffnen Sie im Startmenü die VERWALTUNG/INTERNET INFORMATION SERVICES (IIS)-VERWALTUNG.
2. Klicken Sie in der linken Fensterhälfte auf den Namen des IIS, und rechts doppelklicken Sie auf INTERNETSEITEN.
3. Wählen Sie aus dem Kontextmenü von COMPANYWEB den Eintrag EIGENSCHAFTEN.
4. Klicken Sie auf VERZEICHNISSICHERHEIT und dann auf ZERTIFIKAT. Auf der Begrüßungsseite des folgenden Assistenten klicken Sie auf WEITER.
5. Auf der Seite SERVERZERTIFIKAT klicken Sie EIN VORHANDENES ZERTIFIKAT ANWENDEN und dann auf WEITER.
6. Im Fenster VERFÜGBARE ZERTIFIKATE wählen Sie ein installiertes Zertifikat aus, das Sie der Webseite zuweisen möchten, und klicken auf WEITER. Der Name des Zertifikats muss mit dem Namen übereinstimmen, den Sie beim Ausführen des Assistenten zur Konfiguration von E-Mail und Internetverbindung in der Aufgabenliste gewählt haben. Klicken Sie nicht auf PUBLISHING. Dieses Zertifikat wird nur für interne Zwecke benutzt. Das Zertifikat, das Sie der Webseite zuweisen möchten, muss mit einer URL übereinstimmen, damit die Benutzer über das Internet eine Verbindung zum Server herstellen können.
7. Im Fenster SSL-PORT tragen Sie die Portnummer 444 ein und klicken auf WEITER.
8. Sie erhalten eine Zusammenfassung Ihrer Angaben. Sind diese zutreffend, klicken Sie auf FERTIG STELLEN und OK.

6.10.4 Konfiguration des Remote-Webarbeitsplatzes

Um die Seite *http://Companyweb* im Remote-Webarbeitsplatz verfügbar zu machen, müssen Sie einige Änderungen an der Registry vornehmen.

1. Öffnen Sie mit dem Befehl regedit den Registrierungseditor und navigieren zum Schlüssel

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SmallBusinessServer\
   RemoteUserPortal\AdminLinks
   ```

2. Setzen Sie hier den Wert des Schlüssels HELPDESK auf 1.
3. Ändern Sie danach den Schlüssel STS ebenfalls auf den Wert 1 ab.
4. Danach öffnen Sie den Schlüssel

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SmallBusinessServer\
   RemoteUserPortal\KWLinks
   ```

5. Setzen Sie auch unter diesem Schlüssel die Werte für HELPDESK und STS auf 1 und schließen danach den Registrierungseditor.

Wenn Sie nach den Änderungen an der Registry erneut den Konfigurationsassistenten für E-Mail und Internetverbindung starten, werden die geänderten Werte automatisch wieder von 1 auf 0 zurückgesetzt. Sie müssen die Registry danach erneut anpassen.

7 Der SQL Server 2000

Der SQL Server 2000 ist wie der ISA Server 2000 nur in der Premium-Version des SBS 2003 verfügbar. Sie finden den SQL Server 2000 auf der CD Windows Small Business Server Premium Technologies.

Der SQL-Server kann als Datenbank für Ihre Geschäftsapplikationen verwendet werden. Sie können aber auch die von den SharePoint Services verwendete Instanz der MSDE (Microsoft SQL Server Desktop Engine) aktualisieren. Es ist jedoch auch möglich, anstelle des SQL-Servers lediglich die MSDE zu verwenden, sofern die Anforderungen des Unternehmens nicht deren Funktionsumfang überschreiten.

Ohne Datenbanken ist es heutzutage nahezu unmöglich, innerhalb eines Unternehmens Informationen und Aufgaben zu verwalten. Mit Hilfe einer strukturierten Aufbereitung der Daten können Sie für jeden Bereich und für die Mitarbeiter des Unternehmens einen schnellen und effektiven Zugriff auf die Daten sicherstellen.

Die Implementierung einer Datenbankumgebung setzt sich aus mehreren Schritten zusammen. Ist bislang noch keine Datenbank im Unternehmen implementiert, so müssen Sie zunächst eine Planung der zu installierenden Datenbank durchführen. Je umsichtiger Sie dabei vorgehen, desto effektiver werden später die Daten nutzbar sein. Nach der Planung erfolgen die Installation des SQL-Servers und das Erstellen der einzelnen Datenbanken. Damit die Datenbank auch immer auf einem aktuellen Stand verbleibt, muss diese später auch gepflegt, aktualisiert und verwaltet werden.

7.1 Vorüberlegungen zur Implementierung

Im Folgenden finden Sie eine Übersicht über die Features des MSDE sowie des SQL Servers 2000. Da der SQL-Server lediglich Bestandteil der Premium Edition ist, stellt sich natürlich die Frage, ob diese Komponente überhaupt erforderlich ist und so die zusätzlichen Kosten gerechtfertigt sind. Dies ist besonders wichtig, da im Gegensatz zum SQL-Server Microsoft die MSDE kostenlos bereitstellt und beispielsweise die SharePoint Services auch auf diese zurückgreifen können.

7.1.1 SQL-Server oder MSDE

Die Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) verwendet als Datenbankmodul die SQL-Server-Technologie. Als Hintergrundprogramm unterstützt MSDE transaktionale Desktop-Anwendungen, besitzt jedoch keine eigene Benutzeroberfläche oder weitere Steuerungs- und Verwaltungsprogramme. Die Kommunikation der Benutzer mit der MSDE erfolgt über die Applikation, in der sie enthalten ist. Die MSDE liegt als selbstentpackendes Archiv vor. Damit ist eine simple Verteilung und Integration sichergestellt.

Die MSDE ist an keine Lizenz gebunden und darf zudem weitergegeben werden. Sie fungiert als eine eingebettete Datenbank für Applikationen, die ein Datenbankmodul benötigen. Die MSDE kann unter den folgenden Betriebssystemen eingesetzt werden: Microsoft Windows 98, ME, NT 4.0 ab SP5, 2000, XP und 2003. Aufgrund der Kompatibilität zum SQL-Server sowie derselben Codegrundlage kann auch eine Anwendung später schnell auf den SQL-Server portiert werden, wenn diese nicht mehr den Anforderungen der MSDE entspricht.

Die MSDE verfügt über die folgenden Features, aber auch Beschränkungen gegenüber dem SQL Server 2000:

- *Funktionsumfang*: Die MSDE ist ein Datenbankmodul auf lokaler Ebene. Es kann ein gemeinsamer Zugriff darauf erfolgen. Allerdings besteht dabei eine Begrenzung auf fünf gleichzeitige Arbeitszugriffe. Werden mehr als fünf Zugriffe gleichzeitig ausgeführt, kommt es zu einem deutlichen Leistungsabfall in der Verarbeitungszeit der Datenbank. Dies liegt in der Überwachung des Systems begründet. Hierin liegt auch das Hauptargument für die Verwendung des SQL-Servers. Benötigen Sie dauerhaft mehr als fünf gleichzeitige Zugriffe, sollten Sie aus Performance-Gründen nicht mehr die MSDE verwenden.
- *Unterstützung mehrerer Instanzen*: Die MSDE unterstützt pro Computer bis zu 16 Datenbankserverinstanzen.
- *Größe der Datenbank*: Die MSDE unterstützt eine Datenbankgröße von bis zu 2 GB pro Datenbank. Auf einem Computer können sich auch mehrere MSDE-Instanzen befinden, deren Datenbank je bis zu 2 GB groß sein kann.
- *Remote-Verwaltung*: Die Verwaltung der MSDE kann sowohl lokal als auch remote durchgeführt werden. Lediglich bei einer Multiserverumgebung, in der Transaktionen zwischen mehreren Servern durchgeführt werden, kann keine Remote-Verwaltung der MSDE erfolgen.
- *Data Transformation Services (DTS)*: Die MSDE kann zwar Data Transformation Services-Pakete ausführen, jedoch keine Pakete designen, weil die MSDE keinen DTS-Designer besitzt.
- *Dienstprogramm osql.exe*: Mit diesem Programm können an der Eingabeaufforderung interaktiv Transact-SQL-Anweisungen sowie Skripte ausgeführt werden. Die Ausgabe erfolgt ebenfalls über die Eingabeaufforderung.

Systemanforderungen

Um die MSDE auszuführen zu können, müssen die folgenden Minimalanforderungen erfüllt sein:

- Betriebssystem: Windows 98, ME, NT 4.0 ab SP5, 2000, XP und 2003
- Hardware: Prozessor ab 166 MHz, mindestens 32 MB RAM, empfohlen 64 MB sowie 44 MB Festplattenkapazität

7.1.2 Organisation der Datenbank

Für die Umsetzung des Datenbankmodells können Sie entscheiden, ob Sie eine Client-Server-Lösung implementieren möchten oder die Datenbank vollständig auf einem Server belassen wollen.

Datenbank auf einem Server

Bei diesem Modell befindet sich die Datenbankdatei auf dem Server. Sobald ein Benutzer auf die Daten zugreifen möchte, wird die Datenbank über das Netzwerk an den Client übertragen. Auf dem Client befindet sich ein Datenbanktreiber (Jet-Engine), mit dessen Hilfe die Auswertungen der Datenbank durchgeführt werden. Bei diesem Modell liefert der Server lediglich die Daten, während der Client mit den Daten arbeitet.

Client-Server-Datenbanklösung

Das eben beschriebene Modell ist jedoch nur bedingt für komplexe Datenbankdateien anwendbar. Beim Client-Server-Modell hingegen befindet sich die relationale Datenbank auf dem Server, während die Datenbankanwendung auf den Client und Server verteilt ist. Für die Kommunikation zwischen Client und Server benutzt die Datenbankanwendung die Sprache SQL (Structured Query Language). Um bestimmte Daten zu erhalten, wird eine SQL-Abfrage vom Client aus gestartet. Der Server übernimmt dann die Aufgabe, die gewünschten Daten aus der Datenbank herauszufiltern und in Form von Tabellen an den Client zurückzugeben.

Das Datenbankprogramm auf den einzelnen Clients bildet das Front-End, während die Datenbank selbst auf dem Server das Back-End darstellt. Der Server sorgt für das Management der Datenbank, während als User-Interface ein Datenbankprodukt wie beispielsweise Microsoft Access eingesetzt werden kann.

Gegenüber dem Datenbankmodell auf einem Server bietet die Client-Server-Lösung den Vorteil von höherer Zuverlässigkeit und Skalierbarkeit.

Beim SQL Server 2000 handelt es sich um ein relationales Client-Server-Datenbank-Managementsystem (RDBMS). Die Einsatzgebiete des SQL-Servers umfassen Webanwendungen wie z.B. E-Commerce oder B2B, Online Transactional Processing-Lösungen (OLTP) sowie Datawarehousing über OLAP-Services.

7.1.3 Der Client-Zugriff auf die Datenbank

Besonders wichtig beim Einsatz eines Datenbankservers ist auch die Integrationsmöglichkeit zu einem breiten Spektrum an Clientbetriebssystemen. Selbst in einem relativ kleinen Umfeld wie einem Unternehmen, das den Small Business Server einsetzt, ist nicht unbedingt eine homogene Clientstruktur gegeben.

Der SQL Server 2000 bietet für die folgenden Client-Betriebssysteme Zugriffsmöglichkeiten auf seine Instanzen: Windows 9x, ME, NT, 2000, XP, Apple Macintosh, OS/2 sowie Unix/Linux.

Diese Clients können verschiedene Anwendungstypen verwenden. Dazu zählen etwa ODBC-Anwendungen, OLE DB-Consumer oder DB-Library-Clients. Bei den Clients der Betriebssysteme Apple Macintosh, OS/2 sowie Unix/Linux ist zu bedenken, dass diese nicht die grafischen Programme des SQL-Servers unterstützen (z.B. SQL Server Query Analyzer). Hierzu sind ODBC-Programme eines Drittanbieters erforderlich.

7.1.4 Der Entwurf der Datenbank

Sofern Sie in Ihrem Unternehmen noch über keine Datenbank verfügen, stellen der Entwurf und die sorgfältige Planung einen entscheidenden Anteil für den späteren Erfolg der Datenbank dar. Zudem ist während der Planung zu überlegen, welche Programme clientseitig für den Zugriff auf die Datenbank verwendet werden sollen.

Beim Entwurf der Datenbank sollten Sie zunächst festhalten, welche Informationen in der Datenbank enthalten sein sollen. Diese Daten sind später in einzelnen Tabellen der Datenbank enthalten. Dabei ist in jedem Fall darauf zu achten, dass innerhalb der Datenbank keinerlei Informationen doppelt vorkommen. Eine Redundanz der Inhalte ist nicht notwendig. Die sinnvolle Verknüpfung der Fülle von Daten erfolgt über die Verknüpfung von Tabellen.

Insgesamt erfolgt die Implementierung der Datenbank in den folgenden Schritten:

1. Analyse der Daten, die in der Datenbank aufgenommen werden sollen. Diese Analyse ist abhängig von den speziellen Geschäftsprozessen und Bedürfnissen des Unternehmens.
2. Konzeption der Datenbank sowie Modellierung. In diesem Zusammenhang spricht man auch von ERM (Entity-Relationship-Methode).
3. Danach erfolgt der logische Entwurf der Datenbank. Dabei wird bestimmt, welche Tabellen und welche Verknüpfungen der Tabellen untereinander in der Datenbank vorliegen sollen.
4. Sind die Planungs- und Entwurfsschritte abgeschlossen, wird die Datenbank auf dem SQL-Server physisch erstellt. Dabei werden sämtliche Tabellen sowie weitere Datenbankobjekte angelegt und nacheinander mit Daten gefüllt. Danach ist ein ausgiebiger Test sämtlicher Datenbankfunktionalitäten eine Pflichtaufgabe.
5. Als letzter Schritt erfolgt die Installation der Datenbank im produktiven Umfeld, so dass die Benutzer Zugriff haben. Dieses darf jedoch erst nach einem Test der Datenbank erfolgen.

7.2 Die Installation des SQL Servers 2000

Der im Lieferumfang des SBS 2003 enthaltenen SQL-Server entspricht der Version SQL Server 2000 Standard Edition.

Dieses Kapitel beschreibt verschiedene Installationsszenarien des SQL Servers 2000. Bei der Installation des SQL Servers 2000 müssen Sie sich entscheiden, ob Sie eine neue SQL-Instanz installieren und/oder die bestehende MSDE-Instanz SHAREPOINT der SharePoint Services aktualisieren möchten.

Nach der Installation der Installation des SQL Servers 2000 sollten Sie in jedem Fall das Service Pack 3a mitinstallieren. Dieses Update schließt wichtige Sicherheitslücken wie beispielsweise gegen den Slammer-Wurm.

7.2.1 Installation einer neuen Instanz des SQL Servers 2000

Um eine neue Instanz des SQL Servers 2000 durchzuführen, nehmen Sie die folgenden Schritte vor:

1. Nach dem Autostart der Installations-CD Premium Technologies klicken Sie auf MICROSOFT SQL SERVER 2000 INSTALLIEREN.
2. Sie erhalten das Hinweisfenster SQL SERVER 2000 SP2 AND BELOW (siehe Abbildung 7.1). Klicken Sie hier auf WEITER, da das angezeigte Problem nach der Installation des Service Packs 3 behoben ist.

Abbildung 7.1: Hinweis bei der Installation des SQL Servers 2000 ohne Service Pack

3. Nach der Willkommensmeldung wählen Sie im Fenster COMPUTERNAME (siehe Abbildung 7.2) aus, ob die neue Instanz auf dem lokalen oder einem Remote-Computer installiert werden soll. In unserem Beispiel wählen wir den lokalen Computer und klicken auf WEITER.

Abbildung 7.2: Auswahl des Servers für die Installation

4. Im Fenster INSTALLATIONSAUSWAHL (siehe Abbildung 7.3) bestimmen Sie, welche der drei verfügbaren Optionen ausgeführt werden soll. Sie können EINE NEUE INSTANZ VON SQL SERVER ERSTELLEN ODER CLIENTTOOLS INSTALLIEREN, EINE VORHANDENE INSTANZ VON SQL SERVER AKTUALISIEREN, ENTFERNEN ODER KOMPONENTEN HINZUFÜGEN oder ERWEITERTE OPTIONEN wählen. Letztere Option ist interessant für das Erstellen einer Antwortdatei für eine unbeaufsichtigte Installation. Klicken Sie dann auf WEITER.

Abbildung 7.3: Auswahl der zu installierenden oder aktualisierenden Instanz

5. Nachdem Sie sich für die Installation einer neuen Instanz entschieden haben, geben Sie Ihren Namen und optional den der Firma an. Klicken Sie auf WEITER und stimmen dem angezeigten Lizenzvertrag zu.
6. Nun müssen Sie den 25-stelligen Lizenzschlüssel des SQL Servers 2000 eingeben. Klicken Sie dann auf WEITER.
7. Im Fenster INSTALLATIONSDEFINITION (siehe Abbildung 7.4) wählen Sie die Installationsart aus. Sie können entweder NUR CLIENTTOOLS, SERVER- UND CLIENTTOOLS oder NUR KONNEKTIVITÄT auswählen. Die zweite Option installiert den Server mitsamt den Clienttools, so dass verwaltet werden kann. Klicken Sie dann auf WEITER.
8. Als Nächstes müssen Sie im Fenster INSTANZNAME (siehe Abbildung 7.5) festlegen, ob Sie eine Standardinstallation durchführen möchten. Möchten Sie einen eigenen Namen für die neue Instanz vergeben (maximal 16 Zeichen), so deaktivieren Sie die Checkbox STANDARD und geben in das Textfeld INSTANZNAME den gewünschten Namen ein. Der Name muss mit einem Buchstaben, einer Zahl oder einem der Zeichen &, _ oder # beginnen. Der Name darf nicht Default oder MSSQLServer lauten. Unter SQL Server 2000 ist es erstmals möglich, auf einer Maschine mehrere SQL-Instanzen gleichzeitig zu installieren. Klicken Sie dann auf WEITER.

Abbildung 7.4: Auswählen der Installationsart

Abbildung 7.5: Die zu erstellende oder bearbeitende Instanz auswählen

9. Im Fenster SETUP-TYP (siehe Abbildung 7.6) bestimmen Sie schließlich, ob Sie eine Standard-, benutzerdefinierte oder Minimuminstallation durchführen möchten und in welches Verzeichnis der SQL-Server installiert werden soll. Nach Möglichkeit sollten Sie immer die Programmdateien und die Datendateien in zwei unterschiedlichen Ordnern installieren. Ändern Sie am besten das Zielverzeichnis für die Datendateien. Klicken Sie dann auf WEITER und wählen ggf. bei einer benutzerdefinierten Installation die gewünschten Komponenten aus.

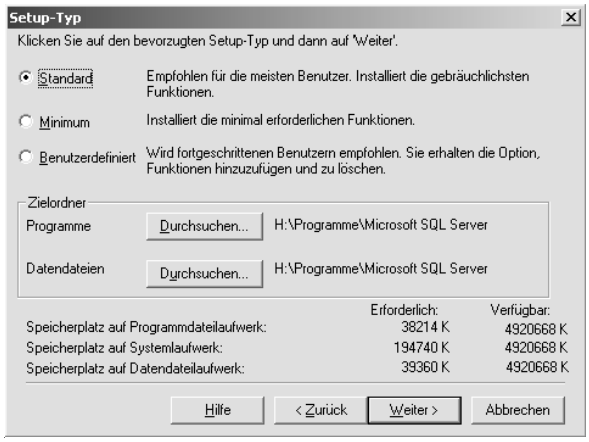


Abbildung 7.6: Bestimmen des Setup-Typs und des Installationsordners

10. Sie erhalten nun das Fenster DIENSTKONTEN (siehe Abbildung 7.7). Wählen Sie hier, ob Sie für die beiden Dienste SQL-Server und SQL-Server-Agent dasselbe Konto verwenden oder EINSTELLUNGEN FÜR JEDEN DIENST ANPASSEN möchten. Sie können entweder das Dienstkonto LOKALES SYSTEM oder ein DOMÄNENBENUTZERKONTO auswählen. Geben Sie dazu den Kontonamen, das Passwort und die Domäne an. Klicken Sie dann auf WEITER.

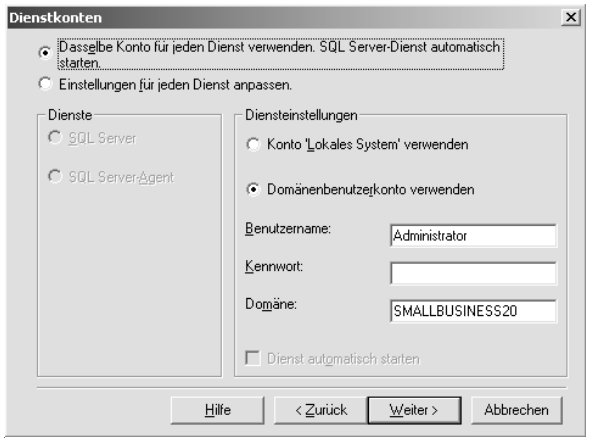


Abbildung 7.7: Angabe des Dienstkontos für die SQL-Serverdienste

11. Als Nächstes wählen Sie unter AUTHENTIFIZIERUNGSMODUS (siehe Abbildung 7.8), ob Sie den WINDOWS-AUTHENTIFIZIERUNGSMODUS verwenden möchten. Dies ist die Standardeinstellung. So können sich Benutzerkonten unter Windows NT, 2000, XP und 2003 am Server authentifizieren. Sie können aber auch den GEMISCHTEN MODUS verwenden, der aus dem Windows-Authentifizierungsmodus und der SQL-Server-Authentifizierung besteht, so dass beide Authentifizierungsmethoden benutzt werden können. Diese Einstellung müssen Sie vornehmen, wenn Sie Clients unter Win-

dows 9x oder ME betreiben, da diese die Windows-Authentifizierung nicht durchführen können. In diesem Fall geben Sie den Kontonamen und das Kennwort für die Systemadministratoranmeldung an. Klicken Sie dann auf WEITER.

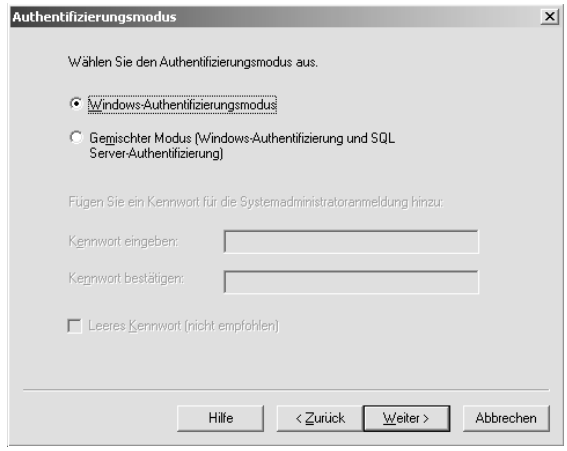


Abbildung 7.8: Auswahl der Authentifizierungsmethode

12. Im Fenster SORTIERUNGSEINSTELLUNGEN (siehe Abbildung 7.9) legen Sie unter SORTIERUNGSKENNZEICHEN fest, welche Spracheinstellung für die Sortierreihenfolge der Datensätze verwendet werden soll. Die standardmäßige Einstellung LATIN1_GENERAL sollten Sie beibehalten. Zusätzlich können Sie unter SORTIERREIHENFOLGE weitere Sortieroptionen bestimmen. Müssen Sie jedoch aus Kompatibilitätsgründen mit früheren SQL-Versionen zusammenarbeiten, verwenden Sie die Option SQL-SORTIERUNGEN. Klicken Sie dann auf WEITER.

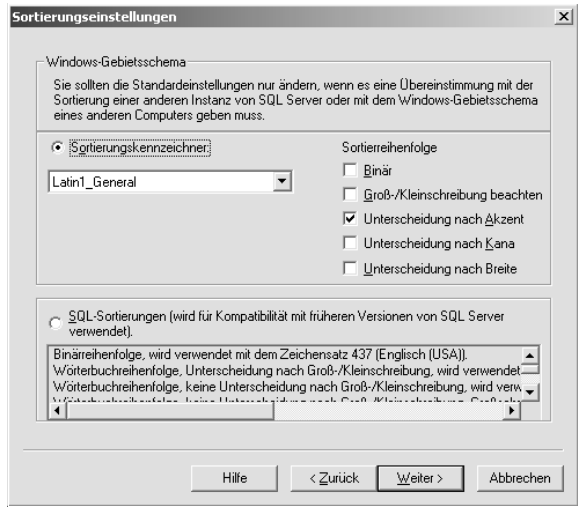


Abbildung 7.9: Das Festlegen von Sortierreihenfolgen und Sortierungskennzeichnern

Die Sortierungsreihenfolgen müssen bei der Installation des SQL Servers 2000 nur dann angegeben werden, wenn Sie nicht die Standardeinstellungen der Sortierung beibehalten können. Dies ist der Fall, wenn eines der folgenden Szenarien auf Ihre SQL-Umgebung zutrifft:

- Sie möchten eine neue Instanz installieren, und es ist bereits eine alte Version des SQL-Servers vorhanden.
- Eine Applikation ist auf eine ältere Version des SQL-Servers angewiesen, da sie nicht mit SQL Server 2000 kompatibel ist.
- Der SQL-Server wird in einer anderen Sprache als die derjenigen Clients ausgeführt, die sich mit der Datenbank verbinden.

13. Unter NETZWERKBIBLIOTHEKEN (siehe Abbildung 7.10) wählen Sie die Verbindungen aus, die für die Kommunikation mit dem SQL-Server verwendet werden sollen. Standardmäßig sind nur die Optionen NAMED PIPES sowie TCP/IP-SOCKETS ausgewählt. Dort wird der TCP-Port 1433 für die Kommunikation vorgeschlagen. Sie können jedoch auch noch weitere Bibliotheken wie z.B. AppleTalk ADSP oder NWLink IPX/SPX hinzufügen. Klicken Sie dann auf WEITER. Damit wird die Installation eingeleitet.

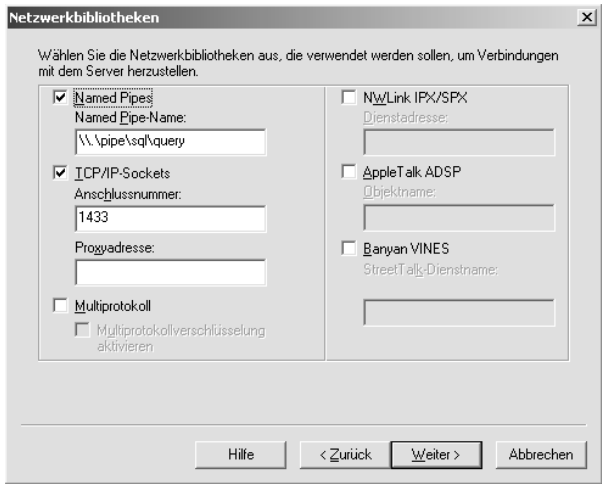


Abbildung 7.10: Die Auswahl der zu verwendenden Netzwerkbibliotheken

7.2.2 Installation des Service Packs 3a für eine neue Instanz

Für die Installation des SQL Service Packs 3 führen Sie die folgenden Schritte durch: Die Installation des Service Packs sollte in jedem Fall vorgenommen werden.

1. Auf der Autostartseite der Premium Technologies wählen Sie die Option SQL SERVER 2000 SERVICE PACK 3A INSTALLIEREN.
2. Stimmen Sie nach der Willkommensmeldung dem Lizenzvertrag zu und klicken dann auf JA.

3. Je nachdem, ob Sie in Schritt 8 der Installation des SQL-Servers den Standardnamen oder einen benutzerdefinierten für die SQL-Instanz gewählt haben, wählen Sie im Fenster INSTANZNAME jetzt dieselbe Option. Klicken Sie dann auf WEITER.
4. Im Fenster VERBINDUNG MIT DEM SERVER HERSTELLEN legen Sie die Authentifizierungsmethode für die Verbindungsherstellung fest. Diese ist abhängig von der unter Schritt 11 der Installation getroffenen Entscheidung. Klicken Sie dann auf WEITER.
5. Wurde vom Setup ermittelt, dass das Kennwort des Benutzers sa (Systemkonto) leer ist, können Sie im Fenster KENNWORTWARNUNG FÜR ‚SA' (siehe Abbildung 7.11) ein neues Kennwort bestimmen. Klicken Sie dann auf WEITER.

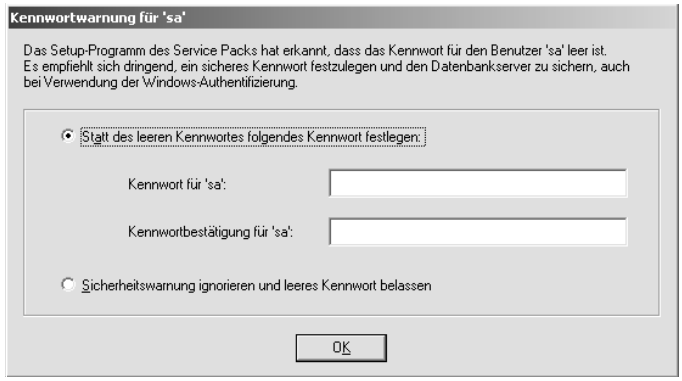


Abbildung 7.11: Kennwortwarnung, wenn für das Konto ‚sa' kein Kennwort festgelegt wurde

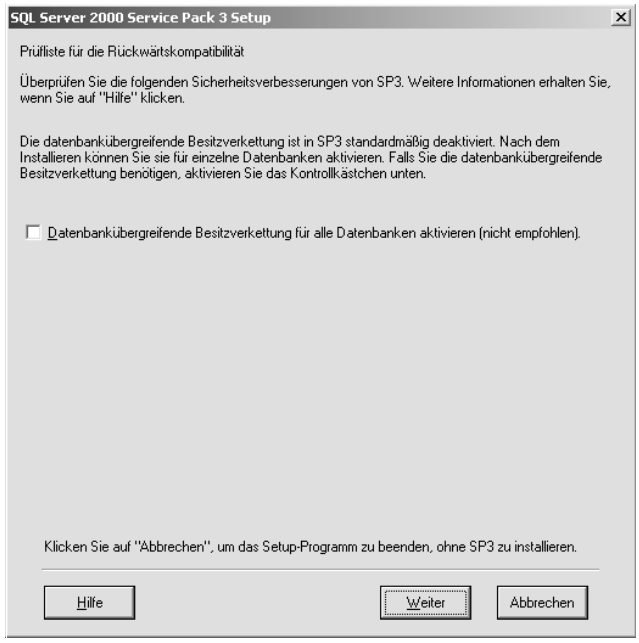


Abbildung 7.12: Aktivieren oder Deaktivieren der Besitzverkettung für sämtliche Datenbanken

6. Im nächsten Fenster (siehe Abbildung 7.12) können Sie die Checkbox DATENBANKÜBERGREIFENDE BESITZVERKETTUNG FÜR ALLE DATENBANKEN AKTIVIEREN. Es ist empfohlen, diese Option nicht zu wählen, sondern stattdessen nach der Installation für einzelne Datenbanken die Besitzverkettung zu aktivieren. Klicken Sie dann auf WEITER.
7. Als Nächstes können Sie festlegen, ob der SQL-Server automatisch nach schwerwiegenden Fehlern Fehlerberichte an Microsoft senden soll. Um die Funktion zu aktivieren, markieren Sie die entsprechende Checkbox. Klicken Sie dann auf OK und danach auf WEITER. Danach wird das Service Pack 3 installiert. Es wird dabei der Installationsfortschritt der einzelnen Update-Skripte angezeigt.
8. Im Laufe der Installation erhalten Sie den Hinweis, dass Sie die Datenbanken *master* und *msdb* sichern sollten, da ihre Inhalte aktualisiert werden. Danach muss der Server neu gestartet werden. Klicken Sie dazu auf BEENDEN.

Probleme bei der Service Pack-Installation

- Erhalten Sie bei der Installation des Service Packs 3 die Meldung, dass die Datei *scm.exe* gerade verwendet wird, so starten Sie den Server neu und wählen erneut das Installationsmenü für Service Pack 3a.
- Sie erhalten die Fehlermeldung Fehler beim Ausführen eines Skripts: sp3_serv_uni.sql(1). Um die Installation des Service Packs 3 zu beenden, klicken Sie auf OK, so müssen Sie den Server neu starten und die Installation des Service Packs erneut durchführen.
- Tritt bei der Installation des Service Packs die Fehlermeldung Setup initialization error: Source \SQL2000_SP3a\x86\Setup\Sqlspre.ini auf, gibt es ein Problem beim Kopieren der Datei *setupsql.ini* in das Verzeichnis %TEMP%. Es befindet sich im %TEMP%-Verzeichnis bereits eine frühere Version dieser Datei, die als schreibgeschützt gekennzeichnet ist. Das Setup-Programm kann diese Datei nicht überschreiben. Um die Installation fortzusetzen, löschen Sie aus dem %TEMP%-Verzeichnis die vorhandene Version der Datei *setupsql.ini* oder heben zumindest ihren Schreibschutz auf. Starten Sie danach das Setup neu.

7.2.3 Aktualisieren der von den SharePoint Services verwendeten MSDE-Instanz

Die Aktualisierung der MSDE-Instanz SHAREPOINT verläuft in weiten Teilen identisch mit der Installation des SQL Servers 2000.

1. Zunächst führen Sie die Installation wie in Kapitel Abbildung 7.2.1 beschrieben bis Schritt 7 aus.
2. Im Fenster INSTANZNAME müssen Sie die Checkbox STANDARD deaktivieren und in das Namensfeld den Instanznamen SHAREPOINT eintragen.

Sie dürfen jedoch nicht die Instanz SBSMONITORING, die für die Überwachung des Small Business Servers verwendet wird, aktualisieren. Eine Aktualisierung dieser Instanz wird nicht unterstützt.

3. Im Fenster VORHANDENE INSTALLATION übernehmen Sie die Standardeinstellung DIE VORHANDENE INSTALLATION AKTUALISIEREN. Klicken Sie dann auf WEITER.
4. Als Nächstes erhalten Sie das Fenster AKTUALISIEREN. Aktivieren Sie hier die Checkbox JA, DIE PROGRAMME SOLLEN INSTALLIERT WERDEN. Klicken Sie auf WEITER und bei der Meldung zur Installation zusätzlicher Komponenten auf JA.
5. Im Fenster KOMPONENTEN AUSWÄHLEN markieren Sie unter UNTERKOMPONENTEN die Checkbox VOLLTEXTSUCHE. Zusätzlich können Sie auch über ONLINEDOKUMENTATION des SQL Servers 2000 auswählen. Klicken Sie dann auf HIER und auf der nächsten Seite auf WEITER, damit die Installation erfolgen kann.

7.2.4 Installation des Service Packs 3a für die Instanz SHAREPOINT

Auch die Installation des Service Packs für die Instanz SHAREPOINT verläuft ähnlich wie die Installation des Service Packs bei einer Neuinstallation.

1. Folgen Sie zunächst den in Kapitel Abbildung 7.2.2 beschriebenen Schritten 1 und 2.
2. Im Fenster INSTANZNAME deaktivieren Sie die Checkbox STANDARD und tragen in das Textfeld den Namen SHAREPOINT ein.
3. Folgen Sie dann den weiteren in Kapitel Abbildung 7.2.2 beschriebenen Schritten.
4. Nach Abschluss der Installation öffnen Sie STARTMENÜ/PROGRAMME/MICROSOFT SQL SERVER/ENTERPRISE MANAGER. Doppelklicken Sie dort MICROSOFT SQL SERVERS und wählen aus dem Kontextmenü von SQL SERVER-GRUPPE den Eintrag NEUE SQL SERVER-REGISTRIERUNG. Unter SERVERNAME geben Sie „Name des Servers\SHAREPOINT“ ein. Als AUTHENTIFIZIERUNGSMETHODE wählen Sie die Windows-Authentifizierung.

Erhalten Sie bei der Aktualisierung der SHAREPOINT-Instanz eine Fehlermeldung, überprüfen Sie, ob der Dienst MSSQL$SHAREPOINT beendet ist. Ist dies nicht der Fall, müssen Sie den Dienst manuell beenden und nach Abschluss der Aktualisierung wieder neu starten.

7.2.5 Sortierungseinstellungen für den SQL Server 2000

Wie bereits in Kapitel Abbildung 7.2.1 unter Schritt 12 erwähnt, sollten Sie die standardmäßige Sortierreihenfolge nur ändern, wenn einer der folgenden Gründe zutrifft:

- Sie verwenden eine ältere Version eines SQL-Servers. Aus Gründen der Abwärtskompatibilität benutzen Sie die SQL-Sortierreihenfolge.
- Eine Applikation ist auf eine ältere Version des SQL-Servers angewiesen, da sie nicht mit SQL Server 2000 kompatibel ist. Die Dokumentation dieser Applikation sollte Aufschluss über die erforderlichen Sortierreihenfolgen geben.
- Ein vorhandener SQL-Server verwendet ein anderes Gebietsschema oder eine abweichende Sortierreihenfolge.

Verwendet der SQL-Server eine andere Sprache als die Clients, die sich mit seiner Datenbank verbinden, so müssen Sie zusätzlich noch Sortierungskennzeichner für die zu wählende Sortierreihenfolge angeben.

Überprüfen von Sortierreihenfolgen anderer SQL-Server

Um die Sortierreihenfolgen weiterer SQL-Server zu prüfen, verwenden Sie das Programm *Query Analyzer* aus der SQL-Server-Programmgruppe.

1. Tragen Sie dort unter SQL SERVER den Namen des zu überprüfenden Servers ein.
2. Nachdem die Verbindung mit diesem hergestellt wurde, geben Sie im ABFRAGEBEREICH folgende Zeilen ein:

   ```
   Sp_helpsort
   Go
   ```

3. Drücken Sie dann die Taste F5, um den Befehl auszuführen. Die Ergebnisse werden im Ergebnisabschnitt des Abfragefensters angezeigt (siehe Abbildung 7.13).

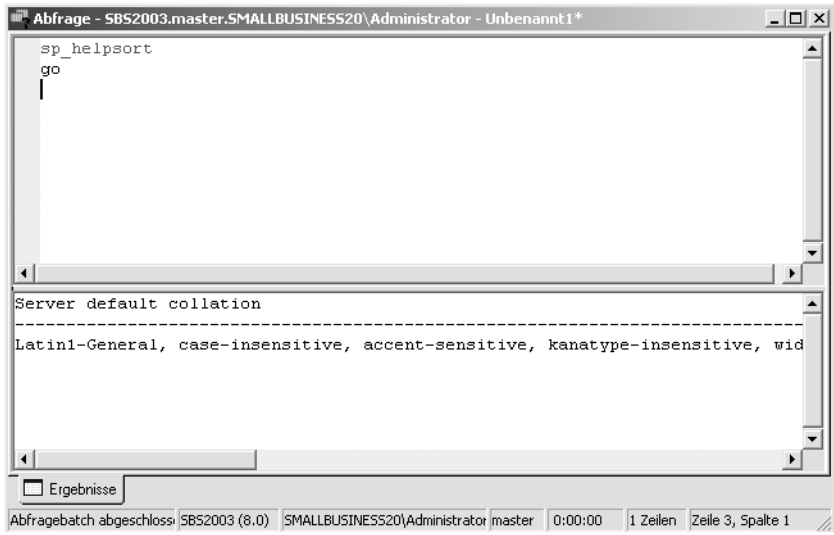


Abbildung 7.13: Abfrage der Sortierungseinstellungen für einen SQL-Server

Bedenken Sie, dass zahlreiche Vorgänge zwischen den SQL-Servern fehlschlagen können, wenn auf den Servern voneinander abweichende Sortierreihenfolgen eingestellt sind.

Die Sortierreihenfolgen können auch später neu eingestellt werden. Allerdings ist es dazu notwendig, die Datenbanken neu zu erstellen und die Daten neu in diese einzufügen.

7.3 Die Datenbanken des SQL-Servers

Während der Installation des SQL-Servers werden auf diesem sechs verschiedene Datenbanken mit jeweils einer dazugehörigen Protokolldatei angelegt. Dabei handelt es sich um die folgenden Komponenten:

Datenbankname	Datenbankdatei	Protokolldatei	Größe nach der Installation
Master	Master.mdf	Mastlog.ldf	17 MB
Model	Model.mdf	Modellog.ldf	0,76 MB
Msdb	Msdbdata.mdf	Msdblog.ldf	12 MB
Tempdb	Tempdb.mdf	Templog.ldf	8,1 MB
Pubs	Pubs.mdb	Pubs_log.ldf	1,8 MB
Northwind	Northwind.mdf	Northwnd.ldf	3,3 MB

Tabelle 7.1: Die Datenbanken und Protokolldateien des SQL-Servers

Bei den vier erstgenannten Datenbanken handelt es sich um Systemdatenbanken. Die einzelnen Datenbanken haben die folgenden Funktionen:

Master: In der Master-Datenbank befinden sich sämtliche Informationen für die Systemebene des SQL-Servers. Dazu zählen die Systemkonfiguration, Anmeldekonten, Initialisierungsinformationen sowie die Speicherorte sämtlicher Datenbanken.

Für die Funktion des SQL-Servers ist es sehr wichtig, dass Sie regelmäßig eine Sicherung der Master-Datenbank durchführen und diese Sicherung im Bedarfsfall zurückspielen können. Weitere Hinweise zur Sicherung der Datenbank finden Sie in Kapitel Abbildung 7.6.

Model: Sie dient als Vorlage für alle neu erstellten Datenbanken. Beim Erstellen einer neuen Datenbank werden die Inhalte der Datenbank Model kopiert und der Rest der neuen Datenbank mit leeren Seiten aufgefüllt. Die Model-Datenbank dient auch als Grundlage für die Tempdb.

Msdb: Diese Datenbank wird vom SQL-Server-Agent verwendet, der sie für die Planung von Aufträgen und Warnungen sowie die Aufzeichnung von Operatoren verwendet.

Tempdb: In dieser Datenbank sind sämtliche temporäre Tabellen und temporär gespeicherte Prozeduren enthalten. Sie wird bei jedem Neustart des SQL-Servers wieder neu erstellt. Sobald der SQL-Server heruntergefahren wird, befinden sich in der temporären Datenbank keine Inhalte, da die temporären Inhalte beim Trennen der Clientverbindungen automatisch gelöscht werden. Beim Neustart hat die Datenbank stets die Anfangsgröße von 8 MB. Diese Größe kann jedoch während der Ausführung des SQL-Servers zunehmen.

Pubs und *Northwind*: Bei diesen beiden Datenbanken handelt es sich um Beispieldatenbanken, um den Umgang mit dem SQL-Server zu erlernen.

7.3.1 Der Aufbau einer Datenbank

In einer Datenbank befindet sich eine Reihe verschiedener Objekte. Alle diese Objekte können Sie sehen, wenn Sie im Enterprise Manager (siehe nächstes Kapitel) im Container DATENBANKEN eine beliebige Datenbank öffnen.

Komponente	Beschreibung
Diagramme	Die Beziehungen zwischen den einzelnen Tabellen der Datenbank werden grafisch dargestellt.
Tabellen	Die Inhalte der Tabellen sind die eigentlichen Objekte der Datenbank. Wie in einer Excel-Tabelle sind die Daten in Spalten und Zeilen angeordnet.
Sichten	Eine Sicht ist eine Tabelle, die auf der Grundlage einer bestimmten Abfrage gebildet wird.
Gespeicherte Prozeduren	Dabei handelt es sich um bereits kompilierte Transact-SQL-Anweisungen (siehe). Eine Prozedur besteht aus einem Satz an SQL-Befehlen. Die Prozeduren werden zur Anzeige von Informationen sowie zur Verwaltung des Servers bereitgestellt. So können Sie beispielsweise mit Hilfe einer Prozedur eine Datenbank auf ihre Integrität hin überprüfen.
Benutzer	Vom System aus Sicherheitsgründen identifizierte Benutzer.
Rollen	Rollen sind Gruppen mit bestimmten Berechtigungen.
Regeln	Regeln werden an Spalten gebunden. Dennoch werden sie als eigenständige Komponente angezeigt.
Standards	Ein Standardwert kann für Spalten definiert werden, der gesetzt wird, wenn ein Benutzer keinen Wert für die Spalte angibt.
Benutzerdefinierte Datentypen	Es können eigene, z.B. von einer bestimmten Applikation benötigte Datentypen bestimmt werden.
Benutzerdefinierte Funktionen	Hierbei handelt es sich um Unterroutinen, die aus einer oder mehreren Transact-SQL-Anweisungen bestehen. Die Benutzer können eigene Transact-SQL-Anweisungen verfassen und sind so nicht auf die integrierten Funktionen beschränkt.
Volltextkataloge	Diese dienen dem Durchsuchen der Datenbank.

Tabelle 7.2: Die Komponenten einer Datenbank

7.4 Die Verwaltung des SQL-Servers

In diesem Kapitel werden Sie mit den häufigsten Verwaltungsaufgaben sowie den gebräuchlichen Verwaltungswerkzeugen vertraut gemacht.

7.4.1 Der Enterprise Manager

Die zentrale Verwaltung des SQL-Servers wird über den Enterprise Manager vorgenommen. Dieser wird aufgerufen über STARTMENÜ/PROGRAMME/MICROSOFT SQL SERVER/ENTERPRISE MANAGER. In dieser Verwaltungskonsole können Sie beispielsweise Datenbanken erstellen, Tabellen, Prozeduren oder Indizes verwalten, Benutzer und Berechtigungen bearbeiten und Datenbanken sichern (siehe Abbildung 7.14).

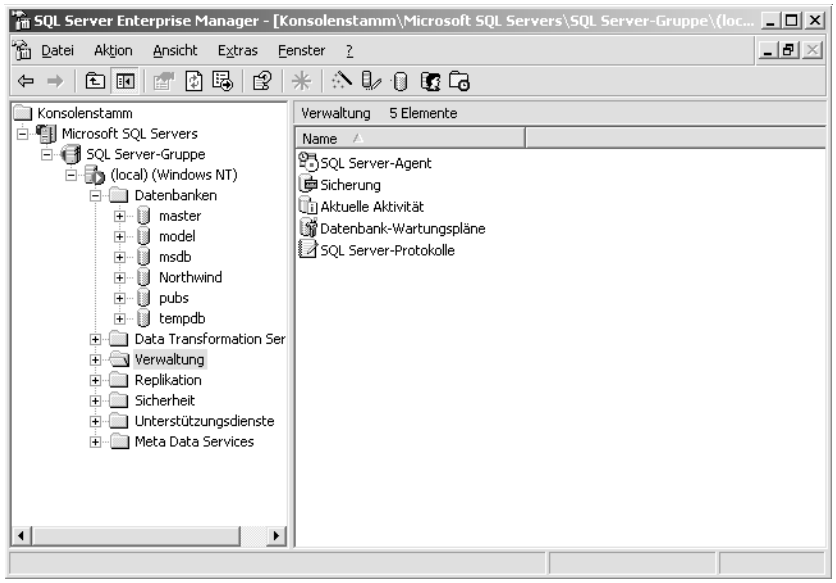


Abbildung 7.14: Der Enterprise Manager ist das zentrale Verwaltungsinstrument für den SQL Server 2000.

Innerhalb der Konsolenstruktur befinden sich unter dem SQL-Server die folgenden Container:

Container	Beschreibung
Datenbanken	In den Datenbanken sind die Tabellen und Objekte enthalten.
Data Transformation Services	Die Data Transformation Services (DTS) beinhalten eine Reihe von grafischen Programmen sowie Objekten zum Extrahieren und Konsolidieren von Daten verschiedener Quellen.
Verwaltung	Hier finden Sie verschiedene grafische Programme sowie programmierbare Objekte zur Verwaltung des SQL-Servers.

Container	Beschreibung
Replikation	Hier finden Sie verschiedene Verwaltungsobjekte für die Verteilung von Datenbankobjekten und Daten in andere Datenbanken. Dadurch wird die Verteilung von Daten an verschiedene Standorte ermöglicht. Die Verteilung kann über eine LAN- oder WAN-Strecke durchgeführt werden.
Sicherheit	Hier werden der Zugriff und die Berechtigungen für den SQL-Server konfiguriert.
Unterstützungsdienste	In diesem Container befinden sich verschiedene Dienstprogramme für den SQL-Server.
Meta Data Services	Mit Meta Data Services wird ein objektorientiertes Repository verwirklicht. Darüber ist eine Integration mit Informationssystemen oder anderen Anwendungen, die Metadaten verarbeiten, möglich.

Tabelle 7.3: Die Container des SQL-Servers im Enterprise Manager

Bevor Sie mit dem Enterprise Manager den SQL-Server verwalten können, müssen Sie den SQL-Server registrieren.

1. Wählen Sie dazu aus dem Kontextmenü eines Servers oder einer Servergruppe den Eintrag NEUE SQL SERVER-REGISTRIERUNG.
2. Klicken Sie im Registrierungsassistenten auf WEITER und wählen dann aus der Liste VERFÜGBARE SERVER über HINZUFÜGEN aus.
3. Im Fenster AUTHENTIFIZIERUNGSMODUS AUSWÄHLEN bestimmen Sie, ob für die Verbindungsherstellung die Windows-Authentifizierung oder die SQL Server-Authentifizierung verwendet werden soll. Klicken Sie dann auf WEITER.

Sie werden nun aufgefordert, einen Benutzernamen und das Kennwort anzugeben. Markieren Sie dabei aus Sicherheitsgründen die Checkbox BENUTZERNAMEN UND KENNWORT IMMER ANFORDERN. Damit ist sichergestellt, dass die Anmeldeinformationen nicht in der Registry gespeichert werden.

4. In der Liste SERVERGRUPPE markieren Sie eine oder mehrere der Checkboxen. Über SQL SERVER-STATUS AN KONSOLE ANZEIGEN können Sie das Abrufen des Dienstes aktivieren. SYSTEMDATENBANKEN UND SYSTEMOBJEKTE ANZEIGEN bewirkt, dass Sie alle diese Objekte anzeigen können. Über SQL SERVER AUTOMATISCH BEIM STARTEN VERBINDEN wird eine Instanz des SQL-Servers automatisch gestartet.

Damit Sie über den Enterprise Manager eine Verbindung zu einer Instanz herstellen können, muss zunächst der Dienst gestartet sein. Den korrekt laufenden Dienst erkennen Sie an dem Symbol des grünen Pfeils neben dem Server-Icon. Um den Dienst zu beenden, wählen Sie aus dem Kontextmenü des Servers den Eintrag ANHALTEN. Optional können Sie dabei auch eine Meldung an die Clients senden, die mit dem SQL-Server verbunden sind, damit sich diese abmelden. Nach einem angemessenen Zeitraum für die Abmeldung wählen Sie aus dem Kontextmenü SQL SERVER-AGENT den Eintrag BEENDEN. Wählen Sie dann aus dem Kontextmenü des Servers den Eintrag BEENDEN.

7.4.2 Starten von Diensten und Instanzen

Nach der Installation des SQL-Servers können Sie außer über den Enterprise Manager auch an anderen Stellen Dienste und Instanzen des SQL-Servers starten und beenden.

Über den SQL-Server-Dienst-Manager können Sie eine Instanz des SQL-Servers oder den SQL-Server-Agent-Dienst starten, beenden und fortsetzen. Dies ist für einen lokalen und einen Remote-Computer möglich.

Über SYSTEMSTEUERUNG/DIENSTE können Sie auf dem lokalen Computer eine Instanz des SQL-Servers oder den SQL-Server-Agent-Dienst starten, beenden und fortsetzen.

Zusätzlich können Sie auch über die Eingabeaufforderung eine Instanz des SQL-Servers oder den SQL-Server-Agent-Dienst starten. Verwenden Sie dazu einen der folgenden Befehle:

```
Net start mssqlserver
Net start sqlservr
Net start SQLServerAgent
```

Möchten Sie eine bestimmte Instanz starten, so verwenden Sie einen der folgenden Befehle:

```
Net start mssql$Instanzname
Net start SQLAgent$Instanzname
```

Alternativ können Sie auch die Datei *SQLSERVR.EXE* ausführen.

7.4.3 Installation von vorhandenen Datenbanken

Ist bereits eine Datenbank vorhanden und soll nun unter SQL Server 2000 weiter genutzt werden, müssen Sie diese Datenbank zunächst installieren. Wählen Sie dazu im Enterprise Manager aus dem Kontextmenü von DATENBANKEN den Eintrag DATENBANK WIEDERHERSTELLEN. Hier wählen Sie die zu installierende Datenbank unter WIEDERHERSTELLEN DER DATENBANK aus. Weitere Hinweise zum Wiederherstellen von Datenbanken finden Sie in Kapitel Abbildung 7.6.4.

7.4.4 Dienstprogramme des SQL-Servers

Neben der Hauptverwaltung über den Enterprise Manager verfügt der SQL-Server auch noch über einige weitere Dienstprogramme. Diese finden Sie unter dem Startmenüeintrag von MICROSOFT SQL SERVER.

SQL-Server-Netzwerkkonfiguration

Mit Hilfe der SQL-Server-Netzwerkkonfiguration können Sie die Netzwerkeinstellungen bearbeiten, die Sie im Zuge der Installation festgelegt haben. So können Sie beispielsweise Netzwerkprotokolle aktivieren und deaktivieren sowie deren Eigenschaften bearbeiten, eine Verschlüsselung hinzufügen oder einen Winsockproxy eintragen (siehe Abbildung 7.15).

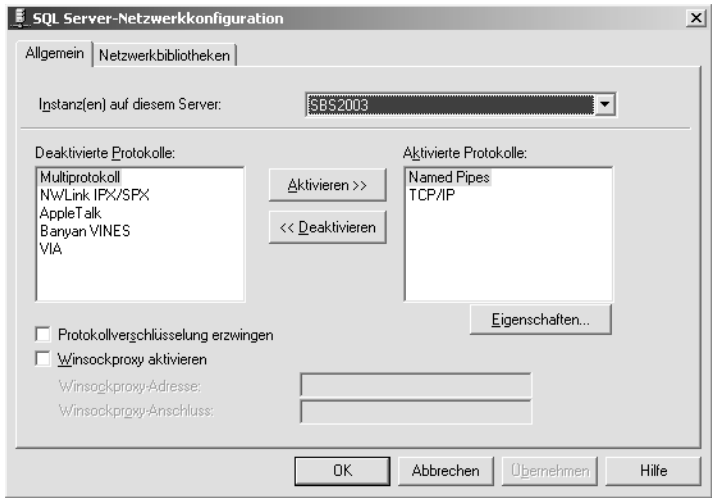


Abbildung 7.15: Die SQL-Server-Netzwerkkonfiguration

SQL-Server-Clientkonfiguration

Über das Programm SQL-Server-Clientkonfiguration können Sie für die Clients Netzwerkbibliotheken für den Zugriff auf den SQL-Server konfigurieren. Weiterhin können Sie auch die Netzwerkprotokolle sowie die Zugriffsmethoden für die Clients festlegen (siehe Abbildung 7.16).

Abbildung 7.16: Die SQL-Server-Clientkonfiguration

7.5 Berechtigungen für den Datenbankzugriff

Durch eine Vergabe von angemessenen Berechtigungen schützen Sie die Datenbank einerseits vor Schäden, welche die Benutzer aus versehentlicher Fehlbedienung an der Datenbank verursachen, als auch vor Schäden, die durch mutwilligen bösartigen Zugriff entstehen können. Zur Steuerung der Sicherheit verwendet der SQL Server 2000 zum einen die Authentifizierung und zum anderen die Berechtigungen für den Zugriff auf die einzelnen Datenbankobjekte.

7.5.1 Die Authentifizierung an der Datenbank

Zur Authentifizierung an der Datenbank verwendet der SQL-Server die Windows NT-Authentifizierung und die SQL-Server-Authentifizierung. Welche Form der Authentifizierung verwendet werden soll, legen Sie während der Installation des SQL-Servers fest. Um die dort vorgenommene Einstellung zu ändern, öffnen Sie im Enterprise Manager das Menü EXTRAS/SERVER-KONFIGURATIONSEIGENSCHAFTEN. Auf der Registerkarte SICHERHEIT können Sie die Einstellung ändern.

Bei der Windows NT-Authentifizierung verwendet der SQL-Server den Benutzernamen und das Kennwort des Betriebssystems. Sobald sich der Benutzer erfolgreich am Betriebssystem authentifiziert hat, muss er für den Zugriff auf die Datenbank keine weiteren Anmeldeinformationen angeben.

Damit der Benutzer auf die Datenbank zugreifen kann, muss er in seinem Konto jedoch über die Berechtigung verfügen, auf den SQL-Server zugreifen zu dürfen.

Die SQL-Server-Authentifizierung wird auch als gemischter Modus bezeichnet. Bei dieser Form prüft der SQL-Server zunächst das Betriebssystemkonto des Benutzers. Ermöglicht dieses keinen Zugriff auf den Server, wird die SQL-Server-Anmeldung verwendet. Sofern diese für den Benutzer durchführbar ist, erlangt er Zugriff auf die Datenbank. Den gemischten Modus müssen Sie auf jeden Fall für Clients der Betriebssysteme Windows 9x und ME anwenden, da diese keine Windows NT-Authentifizierung unterstützen.

7.5.2 Berechtigungen an der Datenbank

Sobald sich ein Benutzer erfolgreich authentifiziert hat, wird anhand der Berechtigungen bestimmt, in welcher Form er Aktionen an der Datenbank vornehmen kann. Bei den Berechtigungen wird zwischen Objektberechtigungen und Anweisungsberechtigungen unterschieden.

Die Objektberechtigungen regeln, in welcher Weise der Benutzer auf die Objekte der Datenbank (Tabellen, Spalten, Sichten und Prozeduren) zugreifen darf. Dabei gibt es die folgenden Berechtigungen:

Berechtigung	Verfügbar für die Objekte
DELETE	Tabellen, Spalten, Sichten
EXECUTE	Prozeduren, benutzerdefinierte Funktionen
INSERT	Tabellen, Spalten, Sichten
REFERENCES (DRI)	Tabellen
SELECT	Tabellen, Spalten, Sichten
UPDATE	Tabellen, Spalten, Sichten

Tabelle 7.4: Die Objektberechtigungen für die verschiedenen Datenbankobjekte

Die verschiedenen Berechtigungen haben die folgenden Bedeutungen:

Berechtigung	Beschreibung
DELETE	Vorhandene Datensätze der Datenbank dürfen gelöscht werden.
DRI	Es dürfen Fremdschlüssel für den Verweis auf die Datenbank erstellt werden.
EXEC	Über diese Berechtigung können Prozeduren ausgeführt werden.
INSERT	Es dürfen Datensätze in die Datenbank eingefügt werden.
SELECT	Das Lesen der Datenbankinhalte ist möglich.
UPDATE	Vorhandene Datensätze dürfen modifiziert werden.

Tabelle 7.5: Die Bedeutungen der verschiedenen Objektberechtigungen

Die Anweisungsberechtigungen hingegen gelten nicht für „herkömmliche“ Benutzer der Datenbank. Über diese Berechtigungen wird vielmehr festgelegt, wer in welcher Weise die Objekte der Datenbank bearbeiten darf. Derartige Berechtigungen lauten beispielsweise CREATE DATABASE, CREATE VIEW oder BACKUP DATABASE.

7.5.3 Berechtigungen über Rollen

Zur Vereinfachung der Berechtigungsvergabe für die einzelnen Benutzer werden unter dem SQL Server 2000 Rollen verwendet. Diese Rollen können Sie prinzipiell mit Gruppen vergleichen, die in der Benutzerverwaltung von Windows verwendet werden. Bei den Rollen wird zwischen Serverrollen und Datenbankrollen unterschieden.

Datenbankrollen

Die Datenbankrollen regeln die Berechtigungen für die Datenbank. Dabei hat eine Datenbankrolle immer nur für diejenige Datenbank Gültigkeit, für die sie vergeben worden ist. Insgesamt gibt es zehn vordefinierte Datenbankrollen. Über diese hinaus können Sie jedoch noch weitere Datenbankrollen festlegen.

Datenbankrolle	Beschreibung
Db_accessadmin	Über diese Rolle wird der Zugriff auf die Datenbank festgelegt, indem bestimmte Benutzer hinzugefügt oder entfernt werden.
Db_backupoperator	Diese Rolle berechtigt zum Sichern der Datenbank.
Db_datareader	Hiermit werden uneingeschränkte Leserechte für die Datenbank vergeben.
Db_datawriter	Hiermit werden uneingeschränkte Schreibrechte für die Datenbank vergeben. Diese beinhalten das Einfügen, Aktualisieren sowie Löschen von Daten (Berechtigungen INSERT, UPDATE und DELETE).
Db_denydatareader	Diese Rolle verweigert vollständig das Lesen (Recht SELECT) der Datenbankinhalte.
Db_denydatawriter	Diese Rolle verweigert vollständig das Schreiben (Berechtigungen INSERT, UPDATE und DELETE) in der Datenbank.
Db_ddladmin	Mit dieser Rolle können Datenbankobjekte erstellt, modifiziert und gelöscht werden. DDL steht für Data Definition Language.
Db_owner	Diese Rolle kennzeichnet den Besitzer einer Datenbank. Er besitzt für diese Datenbank sämtliche Berechtigungen, die in den übrigen Datenbankrollen enthalten sind.
Db_securityadmin	Die Rolle berechtigt zur Vergabe von Anweisungs- und Objektberechtigungen.
public	Diese Rolle besitzen automatisch alle Benutzer, die über irgendeine Berechtigung an der Datenbank verfügen.

Tabelle 7.6: Übersicht über die verschiedenen Datenbankrollen

Serverrollen

Im Gegensatz zu den Datenbankrollen werden die Serverrollen für die Berechtigungsvergabe für bestimmte Aufgaben am SQL-Server verwendet. Die Rollen finden Sie im Enterprise Manager unter SICHERHEIT/SERVERROLLEN. Es gibt die folgenden festen Serverrollen:

Serverrolle	Beschreibung
Bulkadmin	Diese Rolle gestattet das Durchführen von Masseneinfügeoperationen.
Dbcreator	Hiermit wird das Erstellen und Bearbeiten von Datenbanken ermöglicht.
Diskadmin	Über diese Rolle werden Datenträgerdateien verwaltet.
Processadmin	Diese Rolle ermöglicht die Steuerung von SQL-Server-Prozessen.
Securityadmin	In dieser Rolle können Berechtigungen für die Datenbank sowie die Anmeldemöglichkeit am Server vergeben werden.

Serverrolle	Beschreibung
Serveradmin	Es ist über diese Rolle möglich, den Server und dessen Einstellungen zu administrieren sowie den Server herunterzufahren.
Setupadmin	Hiermit wird die Replikationskonfiguration auf dem Server ermöglicht.
Sysadmin	Hierbei handelt es sich um die höchste Berechtigung. Sie umfasst die Berechtigungen aller anderen Rollen.

Tabelle 7.7: Übersicht über die verschiedenen Serverrollen

Über diese acht Serverrollen hinaus können Sie im Unterschied zu den Datenbankrollen und auch Benutzergruppen keine weiteren Rollen erstellen. Auch die Berechtigungen der einzelnen Serverrollen können nicht modifiziert werden.

7.5.4 Die Berechtigung für einen Benutzer konfigurieren

Nachdem Sie nun in der Theorie die verschiedenen Authentifizierungsmethoden, Berechtigungen und Rollen kennen gelernt haben, wird in diesem Kapitel die Berechtigungskonfiguration für einen Benutzer beschrieben.

1. Wählen Sie dazu im Enterprise Manager aus dem Kontextmenü von SICHERHEIT/BENUTZERNAME den Eintrag NEUER BENUTZERNAME.
2. Auf der Registerkarte ALLGEMEIN müssen Sie zunächst entscheiden, welche Form der Authentifizierung der Benutzer verwenden soll (siehe Abbildung 7.17).

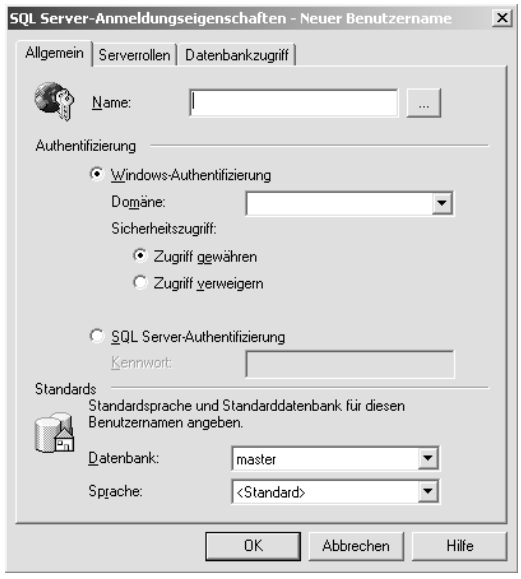


Abbildung 7.17: Die Benutzer-Authentifizierung festlegen

Bei der Option WINDOWS-AUTHENTIFIZIERUNG geben Sie die Domäne an. Deren Name wird automatisch in das Feld NAME eingefügt, wo Sie dann noch den Benutzernamen hinzufügen. Das Kennwort wird in diesem Fall nicht angegeben, da der Benutzer dieses schon bei der Anmeldung an der Domäne angegeben hat. Bedenken Sie, dass diese Form der Authentifizierung nur für Clients der Betriebssysteme Windows NT, 2000, XP und 2003 möglich ist. Für ältere Client-Betriebssysteme müssen Sie die SQL-Authentifizierung verwenden. Wählen Sie die Methode SQL-SERVERAUTHENTIFIZIERUNG, geben Sie unter NAME den Namen und das Kennwort des Benutzers an. Zusätzlich können Sie für den Benutzer eine Standarddatenbank und die bevorzugte Sprache angeben.

3. Als Nächstes können Sie für den Benutzer die Serverrollen festlegen. Wechseln Sie dazu auf die gleichnamige Registerkarte (siehe Abbildung 7.18).

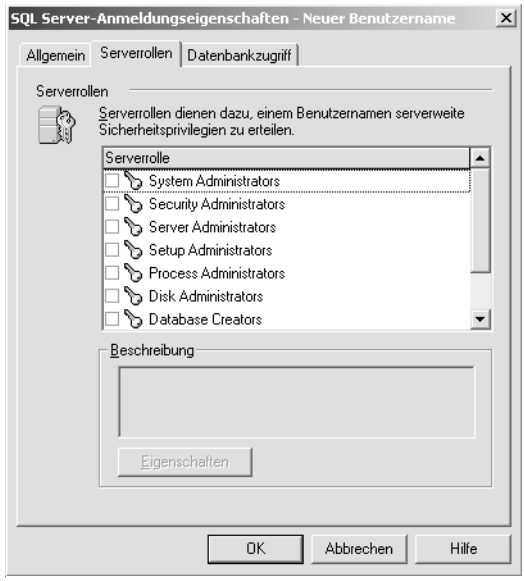


Abbildung 7.18: Die Serverrollen festlegen

Bei einem herkömmlichen Benutzer wird in aller Regel keine der Serverrollen vergeben. Es ist jedoch möglich, einem Benutzer zu einem späteren Zeitpunkt eine Serverrolle zuzuweisen.

4. Wechseln Sie dann auf die Registerkarte DATENBANKZUGRIFF (siehe Abbildung 7.19).

   Dort markieren Sie zunächst alle Datenbanken, für die der Benutzer Zugriff erhalten soll. Sobald Sie eine Datenbank markiert haben (das Häkchen gesetzt), können Sie unter DATENBANKROLLEN FÜR DATENBANKNAME die Datenbankrollen auswählen, die dem Benutzer für die Datenbank zugewiesen werden sollen. Sobald eine Datenbank ausgewählt ist, wird der Benutzername für die Datenbank automatisch angelegt. Standardmäßig wird derselbe Name verwendet, den Sie in Schritt 2 vergeben haben. Möchten Sie diesen ändern, doppelklicken Sie in die Spalte BENUTZER.

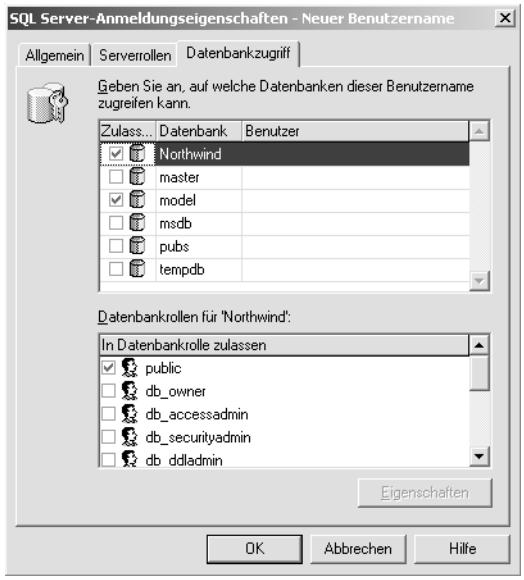


Abbildung 7.19: Die Auswahl der Datenbankrollen für eine Datenbank

Standardmäßig sollten Sie für einen Benutzer die Datenbankrollen db_datareader und db_datawriter zuteilen. Haben Sie für einen Benutzer keine Datenbankrolle zugewiesen, erhalten Sie eine Fehlermeldung. Dennoch ist es möglich, diesen Benutzer zunächst anzulegen.

Gleichzeitig wird geprüft, wenn Sie die Windows-Authentifizierung gewählt haben, ob der entsprechende Benutzer in der Domäne vorhanden ist. Ist dies nicht der Fall, kann der Benutzer für den SQL-Zugriff nicht angelegt werden.

7.5.5 Weitere Konfigurationsoptionen für Berechtigungen

In diesem Kapitel werden Ihnen weitere Konfigurationsoptionen für die Berechtigungsvergabe vorgestellt.

Einen Datenbankbenutzer anlegen und hinzufügen

Sofern Sie eine Datenbank erstellt, aber noch keinem Benutzer den Datenbankzugriff für diese zugeteilt haben, ist für die Datenbank noch kein Datenbankbenutzer zur Anmeldung eingerichtet. Um einen Benutzer anzulegen, markieren Sie die gewünschte Datenbank und wählen aus dem Kontextmenü den Eintrag NEUER DATENBANKBENUTZER. Auf der Registerkarte ALLGEMEIN wählen Sie unter BENUTZERNAME einen Benutzernamen aus. Hier finden Sie alle Benutzer aufgelistet, für die eine Anmeldung am SQL-Server konfiguriert ist. Sobald Sie einen Benutzernamen ausgewählt haben, wird dieser ohne den Zusatz des Domänennamens in das Feld NAME eingetragen. Sie können diesen Namen jedoch auch ändern. Danach können Sie die gewünschten Datenbankrollen für den Benutzer auswählen.

Wenn der Benutzer neu angelegt wird, ist die Schaltfläche BERECHTIGUNGEN neben dem Feld BENUTZERNAME noch nicht anklickbar. Um darüber spezielle Berechtigungen zu vergeben, müssen Sie zunächst mit OK das Anlegen des Benutzers bestätigen, das Fenster schließen und erneut öffnen.

Anlegen zusätzlicher Datenbankrollen

Wie Sie bereits in Kapitel Abbildung 7.5.3 erfahren haben, können Sie zusätzlich zu den vordefinierten Datenbankrollen noch eigene Datenbankrollen hinzufügen. Markieren Sie dazu im Enterprise Manager in der gewünschten Datenbank den Eintrag ROLLEN und wählen aus dem Kontextmenü NEUE DATENBANKROLLE.

Im Feld NAME legen Sie den Namen für die neue Datenbankrolle fest. Danach müssen Sie entscheiden, ob es sich um eine STANDARDROLLE oder ANWENDUNGSROLLE handeln soll. Eine Standardrolle bezieht sich immer nur auf bestimmte Benutzer. Die Benutzer, für die diese Rolle gelten soll, wählen Sie über HINZUFÜGEN aus. Eine Anwendungsrolle hingegen wird mit einem Kennwort versehen. Diese Rolle kann jeder Benutzer erhalten, der das Kennwort für die Rolle kennt.

Vergeben von Berechtigungen

Berechtigungen können sowohl für eine Rolle als auch für einen Benutzer definiert werden. Jedoch sollten Sie immer bedenken, dass die Konfiguration von Berechtigungen für die Benutzer wesentlich mehr Verwaltungsaufwand bedeutet als die Konfiguration von Rollen. Sofern Sie die Berechtigungen über Rollen regeln, müssen Sie den einzelnen Benutzern keine Berechtigungen zuweisen.

Möchten Sie einem Benutzer Berechtigungen zuweisen, wählen Sie den Datenbankbenutzer aus und klicken auf EIGENSCHAFTEN. Danach klicken Sie auf BERECHTIGUNGEN. Dadurch erhalten Sie das Fenster DATENBANKBENUTZER – EIGENSCHAFTEN – DATENBANKNAME (siehe Abbildung 7.20).

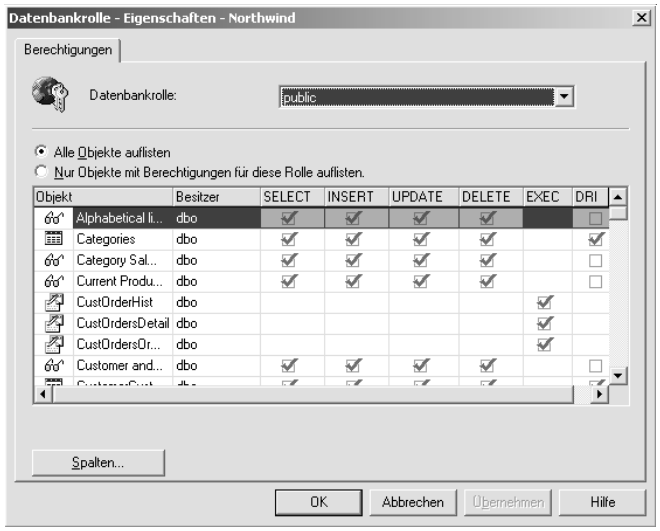


Abbildung 7.20: Die Anzeige der Berechtigungen für alle Datenbankobjekte der gewählten Datenbank

Sie sehen dort alle Datenbankobjekte, die zu der gewählten Datenbank gehören. Für jedes Objekt können Sie die Berechtigungen SELECT, INSERT, UPDATE, DELETE, EXEC und DRI vergeben. Eine Berechtigung ist nur anwählbar, wenn Sie für das jeweilige Objekt auch zur Verfügung steht (siehe Tabelle 7.4).

Um die Berechtigungen SELECT und UPDATE noch feiner steuern zu können, klicken Sie auf SPALTEN. Sie sehen nun die einzelnen Spalten der Tabelle und können für jede einzeln die Berechtigung bestimmen.

Insgesamt gibt es bei der Berechtigungsvergabe drei Arten. Diese lauten ERTEILT, NEUTRAL und ENTZOGEN. Ist eine Berechtigung erteilt, wird diese durch das grüne Häkchen dargestellt, eine entzogene Berechtigung wird durch das rote Kreuzchen angezeigt. Darüber ist es möglich, einem Benutzer eine bestimmte Berechtigung zu entziehen, die ihm eigentlich aufgrund seiner Rollenmitgliedschaft zusteht. Eine neutrale Berechtigung wird dem Benutzer nicht direkt zugewiesen. Eine solche Berechtigung kann er über die Mitgliedschaft in einer bestimmten Rolle erhalten.

Um die Berechtigungen für eine Datenbankrolle zuzuweisen, folgen Sie den eben beschriebenen Schritten. Sie müssen lediglich anstelle des Benutzers eine Rolle auswählen. Bedenken Sie jedoch, dass die Berechtigungen für die standardmäßigen Datenbankrollen nicht geändert werden können. Die einzige Ausnahme bildet die Rolle Public. Ansonsten kann die Berechtigungszuweisung nur für selbst definierte Datenbankrollen erfolgen.

7.6 Sicherung und Wiederherstellung der Datenbank

Damit bei einem Ausfall einer Datenbank der Zeitraum bis zur Wiederherstellung möglichst gering bleibt, sollten Sie über eine effektive Sicherungsstrategie nachdenken. Dabei ist es zunächst unerheblich, ob es sich bei dem aufgetretenen Problem um einen Hardwarefehler oder um einen Fehler an der Datenbank handelt.

Um eine möglichst effektive Wiederherstellung der Daten gewährleisten zu können, sollten Sie zum einen verschiedene Sicherungsmedien verwenden, zum anderen aber auch die verschiedenen Sicherungsoptionen des SQL Servers 2000 sinnvoll miteinander kombinieren. Zudem können Sie mit Hilfe einer aktuellen Sicherung schnell eine Kopie der Datenbank auf einem zweiten Server anlegen. Bei der Sicherung müssen Sie unbedingt die Datenbanken *master*, *msdb* sowie *model* einbeziehen. Die Sicherung der Datenbank *model* ist jedoch nur dann notwendig, wenn Änderungen durchgeführt worden sind. Dient der SQL-Server auch als Replikationsverteiler, müssen Sie auch die Datenbank *distribution* regelmäßig sichern.

Die Sicherung des SQL-Servers kann im laufenden Betrieb vorgenommen werden. Es ist nicht notwendig, dass sich die Benutzer vom Server abmelden müssen.

Sofern Sie eine Sicherung der Datenbank durchführen, um die Datenbank von einem SQL-Server auf einen anderen zu transferieren, sollten Sie die Sicherungsdatei mit einem Komprimierungsprogramm verkleinern. Die Komprimierung der Sicherungsdatei ist sehr effektiv.

7.6.1 Arten der Sicherung

Neben der herkömmlichen Sicherung bietet der SQL-Server auch eine differenzielle Datenbanksicherung sowie eine Transaktionsprotokollsicherung. Zudem können Sie noch eine Datei- und Dateigruppensicherung durchführen.

Vollständige Datenbanksicherung

Mit dieser Option wird eine vollständige Sicherung durchgeführt. In dieser Sicherung ist genau der Stand enthalten, der zum Zeitpunkt der Sicherung in der Datenbank vorlag. Da in der Sicherung auch die Transaktionsprotokolle enthalten sind, können Sie nach der Durchführung einer vollständigen Sicherung das Transaktionsprotokoll löschen.

Differenzielle Datenbanksicherung

Bei einer differenziellen Sicherung werden lediglich die Änderungen gespeichert, die seit der letzten vollständigen Sicherung an der Datenbank vorgenommen worden sind. Diese Art der Sicherung ist besonders bei großen Datenbanken sinnvoll, da Sie auf diese Art Zeit und Speicherplatz sparen. Um die Datenbank wieder auf den Stand vor der Sicherung zu bringen, müssen Sie zusätzlich noch Transaktionsprotokollsicherungen durchführen.

Transaktionsprotokollsicherung

In einer Transaktionsprotokollsicherung befinden sich sämtliche Transaktionen, die seit der letzten vollständigen, differenziellen oder Transaktionsprotokollsicherung abgeschlossen worden sind. Mit Hilfe dieser Sicherung können Sie den Zustand der Datenbank bis zum Zeitpunkt der Sicherung wiederherstellen. Es werden sämtliche nicht aktiven Transaktionen gespeichert und danach aus dem Protokoll entfernt, so dass der Speicherplatz wieder verwendet werden kann.

Datei- und Dateigruppensicherung

Dieses Verfahren wird bei sehr großen Datenbanken verwendet, bei denen aufgrund ihrer Größe eine vollständige Sicherung nur schwer durchgeführt werden kann. Deshalb wird die gesamte Datenbank in mehrere Teilstücke zerlegt, und diese werden dann gesichert. Diese Sicherungsmethode ist jedoch nur dann verfügbar, wenn die Datenbank aus mehreren Datendateien (mdf-Dateien) besteht.

7.6.2 Anlegen einer Sicherung

Als Sicherungsziel unterstützt der SQL-Server eine Datei auf der Festplatte oder ein Bandlaufwerk. Sinnvoll ist hierbei die Methode, die Sicherung zunächst in einer Datei anzulegen und diese im Zuge des Backups des SBS auf das Bandlaufwerk zu speichern.

Damit Sie die Sicherungen einfacher verwalten können, bietet der SQL-Server die Möglichkeit, Sicherungsmedien anzulegen. Wenn Sie ein Sicherungsmedium auswählen, müssen Sie nicht jedes Mal das komplette Sicherungsziel mit seinem vollständigen Pfad angeben. Sie wählen lediglich den vergebenen Namen des Sicherungsmediums aus.

Um ein neues Sicherungsmedium anzulegen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie im Enterprise Manager den Ordner VERWALTUNG unter dem SQL-Server. Wählen Sie aus dem Kontextmenü den Eintrag NEUES SICHERUNGSMEDIUM aus.
2. Geben Sie unter NAME eine Bezeichnung für das Sicherungsmedium an. Unter DATEINAME wird Ihnen standardmäßig das Verzeichnis angegeben, das Sie beim Setup des SBS als Sicherungsverzeichnis festgelegt haben. Sie können jedoch auch ein anderes Verzeichnis auswählen oder ein Bandlaufwerk angeben.

Sofern Sie ein Verzeichnis auswählen, das sich auf einem Netzlaufwerk befindet, muss der SQL-Serverdienst dort über die entsprechenden Berechtigungen verfügen. Dies ist jedoch nicht der Fall, wenn der Server unter dem lokalen Systemkonto gestartet wird.

Sobald Sie nun eine Sicherung durchführen möchten, wird Ihnen dieses Sicherungsmedium angezeigt.

7.6.3 Der Sicherungs-Assistent und die manuelle Sicherung

Die Sicherung der Datenbank können Sie entweder über den Sicherungs-Assistenten oder auch manuell vornehmen.

Der Sicherungs-Assistent

Nachdem Sie ein Sicherungsmedium angelegt haben, können Sie mit Hilfe des Sicherungs-Assistenten eine Sicherung vornehmen. Führen Sie dazu die folgenden Schritte durch:

1. Wählen Sie im Enterprise Manager aus dem Menü EXTRAS den Eintrag ASSISTENTEN. Im Fenster ASSISTENTEN AUSWÄHLEN markieren Sie unter VERWALTUNG den Eintrag SICHERUNGS-ASSISTENT und klicken auf OK.
2. Nach dem Begrüßungsbildschirm wählen Sie unter DATENBANK die zu sichernde Datenbank aus. Klicken Sie dann auf WEITER.
3. Als Nächstes geben Sie einen Namen für die Sicherung an. Unter diesem Namen ist die Sicherung später im Enterprise Manager aufzufinden. Zusätzlich können Sie auch noch eine Beschreibung der Sicherung angeben. Klicken Sie dann auf WEITER.
4. Dann wählen Sie die gewünschte Sicherungsmethode aus. Die verschiedenen Sicherungsmethoden wurden bereits in Kapitel Abbildung 7.6.1 beschrieben. In unserem Beispiel wählen wir die Option DATENBANKSICHERUNG – GESAMTE DATENBANK SICHERN. Klicken Sie dann auf WEITER.

5. Im Fenster SICHERUNGSZIEL UND -AKTIONEN AUSWÄHLEN (siehe Abbildung 7.21) können Sie bestimmen, ob als Sicherungsziel ein SICHERUNGSMEDIUM, ein BAND oder eine DATEI verwendet werden soll.

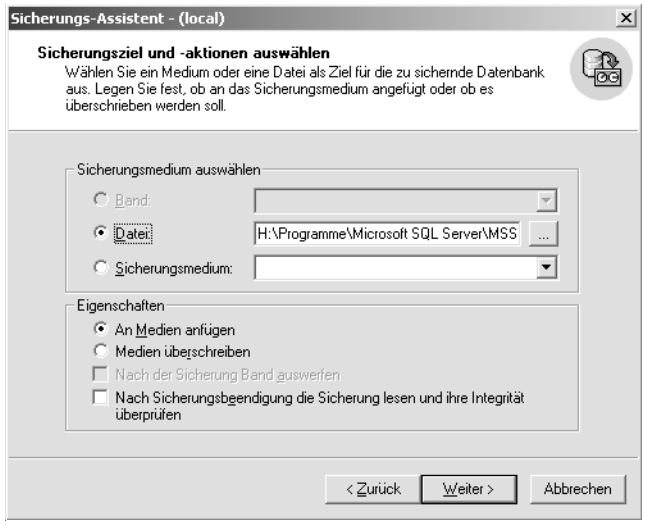


Abbildung 7.21: Das Festlegen des Sicherungsziels und der Sicherungsaktionen im Sicherungs-Assistenten

Zusätzlich können Sie noch die folgenden Sicherungsoptionen auswählen. Klicken Sie dann auf WEITER.

- AN MEDIEN ANFÜGEN: Mit dieser Option werden auf dem Medium mehrere Sicherungssätze erstellt. Vorherige Sicherungssätze werden dabei nicht überschrieben.
- MEDIEN ÜBERSCHREIBEN: Hierdurch wird ein bereits vorhandener Sicherungssatz überschrieben und kann nicht wiederhergestellt werden.
- NACH DER SICHERUNG BAND AUSWERFEN: Diese Option ist nur verfügbar, wenn Sie als Sicherungsmedium ein Bandlaufwerk ausgewählt haben. Nach der Sicherung wird das Band ausgeworfen, um ein Überschreiben zu verhindern.
- NACH SICHERUNGSBEENDIGUNG DIE SICHERUNG LESEN UND IHRE INTEGRITÄT ÜBERPRÜFEN: Über diese Option wird nach der Sicherung die Lesbarkeit der Sicherungsdatei sowie deren inhaltliche Übereinstimmung mit den zu sichernden Daten überprüft. Diese Integritätsprüfung kann jedoch besonders bei großen Datenbanken einige Zeit in Anspruch nehmen.

6. Weiterhin können Sie den Sicherungssatz überprüfen, einen Zeitplan erstellen und ein Ablaufdatum für den Sicherungssatz definieren. Wenn Sie einen Sicherungszyklus einrichten möchten, geben Sie unter MEDIENSATZNAME einen Namen an. Geben Sie weiterhin das Ablaufdatum an. Damit wird verhindert, dass eine Sicherungsdatei vorzeitig überschrieben wird. Sofern das Datum noch nicht abgelaufen ist, wird jeweils eine neue Sicherungsdatei angelegt. Diese unterscheidet sich durch die Kennung des Datums oder einer Nummernkennung. Ist der Zeitstempel abgelaufen, werden die Dateien von der ersten an überschrieben.

Weiterhin können Sie auch einen Zeitplan für die Sicherung erstellen. Um diesen anzupassen, klicken Sie unter ZEITPLAN auf ÄNDERN. Im Fenster ZEITPLAN BEARBEITEN geben Sie zunächst einen Namen für den Zeitplan an. Achten Sie darauf, dass die Checkbox AKTIVIERT markiert ist, damit der Zeitplan auch umgesetzt wird. Zur Erstellung des Zeitplans können Sie eine der folgenden Optionen wählen:

- AUTOMATISCH STARTEN, WENN DER SQL SERVER-AGENT STARTET: Die Sicherung wird automatisch gestartet, sobald der Dienst SQL-Server-Agent gestartet wird.
- STARTEN, SOBALD DIE CPU(S) IM LEERLAUF IST (SIND): Diese Option ist sinnvoll, wenn Sie eine Hardware verwenden, die bereits durch die standardmäßige Belastung genügend Last hat. So ist sichergestellt, dass die Sicherung erst zu einem Zeitpunkt durchgeführt wird, wenn nicht mehr viel Datenverkehr auf dem SQL-Server stattfindet.
- EINMAL: Über die anzugebende Zeit und das Datum legen Sie einen einmaligen Sicherungsvorgang fest.

Die einmalige Sicherung wird automatisch sofort gestartet, nachdem Sie den Sicherungs-Assistenten abgeschlossen haben.

- WIEDERHOLT: Über ÄNDERN legen Sie einen immer wiederkehrenden Sicherungszeitplan fest. Das Sicherungsintervall können Sie individuell an Ihre Firmenbedürfnisse anpassen.

Der Zeitplan für die wiederkehrenden Sicherungen kann nur umgesetzt werden, wenn der Dienst SQL-Server-Agent läuft. Um Komplikationen zu verhindern, sollten Sie für diesen Dienst den Starttyp AUTOMATISCH festlegen. Sofern der Dienst nicht läuft, nachdem Sie den Sicherungsauftrag erstellt haben, werden Sie darauf hingewiesen. Die zeitgesteuerten Sicherungsaufträge können Sie auch im Enterprise Manager unter VERWALTUNG/AUFTRÄGE einsehen.

7. Zum Abschluss zeigt Ihnen der Assistent eine Zusammenfassung der Angaben, die Sie jetzt noch ändern können. Klicken Sie dann auf FERTIG STELLEN.

Die manuelle Sicherung

Wenn Sie den Assistenten nicht benutzen möchten, können Sie die Sicherung auch manuell durchführen. Wählen Sie dazu im Enterprise Manager aus dem Kontextmenü der gewünschten Datenbank den Eintrag ALLE TASKS/DATENBANK SICHERN.

Wie auch im Assistenten geben Sie einen Namen für die Sicherung an, wählen die Art der Sicherung, bestimmen das Sicherungsziel, entscheiden, ob die Sicherung eine vorhandene überschreiben oder an diese angehängt werden soll, und erstellen einen Zeitplan. Alle diese Angaben werden auf der Registerkarte ALLGEMEIN vorgenommen. Auf der Registerkarte OPTIONEN finden Sie die übrigen Einstellmöglichkeiten des Assistenten wie die Überprüfung der Sicherung oder das Ablaufdatum des Sicherungssatzes.

Modifizieren von Sicherungsaufträgen

Alle zeitgesteuerten Sicherungen finden Sie im Enterprise Manager unter VERWALTUNG/AUFTRÄGE. Hier haben Sie die Möglichkeit, bestehende Sicherungsaufträge per Doppelklick zu modifizieren.

Auf der Registerkarte BENACHRICHTIGUNGEN können Sie zudem einstellen, ob und über welche Methode die Benachrichtigung über eine Sicherung vorgenommen werden soll. Sie können wählen zwischen E-Mail, Pager, Net Send-Befehl und Eintragung in das Windows-Ereignisprotokoll.

7.6.4 Wiederherstellen der Datenbank

Eine Wiederherstellung der Datenbank wird entweder nach einem Fehler an der Datenbank oder dem Server oder aber auch beim Wiederherstellen auf einem anderen Server durchgeführt.

1. Um die Datenbank wiederherzustellen, markieren Sie im Enterprise Manager die gewünschte Datenbank und wählen aus dem Kontextmenü den Eintrag ALLE TASKS/DATENBANK WIEDERHERSTELLEN.
2. Im Fenster DATENBANK WIEDERHERSTELLEN sehen Sie auf der Registerkarte ALLGEMEIN unter PARAMETER alle verfügbaren Sicherungen der gewählten Datenbank. Automatisch wird immer die neueste Sicherung eingeblendet. Haben Sie die Option VON MEDIEN ausgewählt, erhalten Sie die Schaltfläche MEDIEN AUSWÄHLEN, über die Sie eine Sicherungsdatei wählen können. Diese Option werden Sie auch dann benutzen, wenn die Datenbank auf einem anderen Server wiederhergestellt werden soll. Sie ist aber auch erforderlich, wenn auf dem SQL-Server ein derart schwerwiegendes Problem vorliegt, dass die Historie der vorhandenen Sicherungen nicht mehr verfügbar ist.

8 Die Administration des SBS 2003

In diesem Kapitel lernen Sie die tägliche Administration des SBS 2003 unter ihrem vielfältigen Aufgabenspektrum kennen. Außer den verschiedenen durchzuführenden Verwaltungsaufgaben lernen Sie auch die Konsolen, Werkzeuge und Tools kennen, die Ihnen die Verwaltung des SBS 2003 vereinfachen.

8.1 Die Serververwaltung als zentrale Administrationsinstanz

Die Serververwaltungskonsole ist die zentrale Schaltstelle für die Administration des SBS 2003. In dieser Konsole finden Sie eine große Anzahl von Verwaltungskomponenten (siehe Abbildung 8.1). Sie finden diese Konsole unter STARTMENÜ/PROGRAMME/VERWALTUNG.

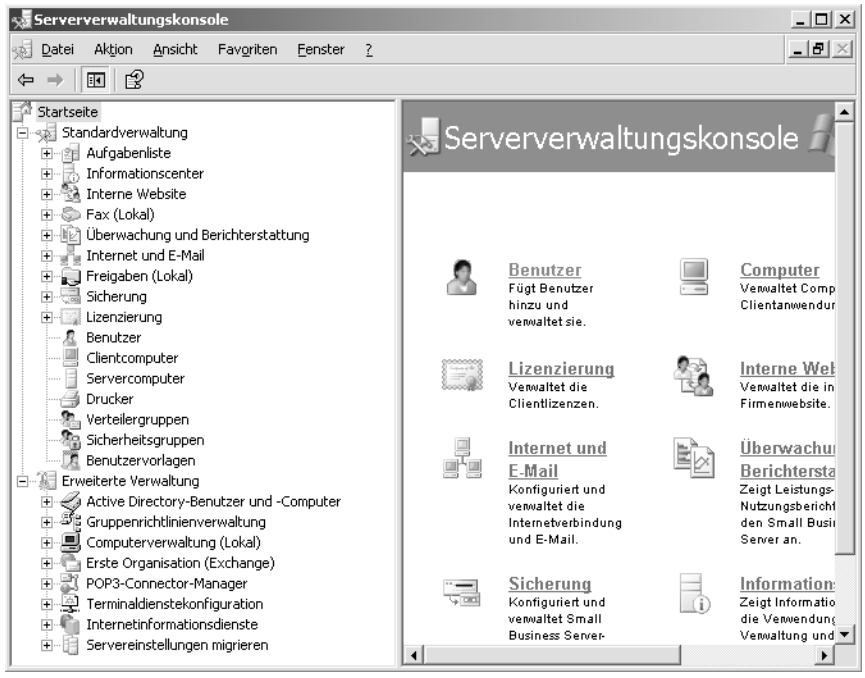


Abbildung 8.1: Die Serververwaltungskonsole als zentrales Verwaltungselement

Die folgende Tabelle gibt Ihnen einen ersten Überblick über die verschiedenen Verwaltungskomponenten.

Verwaltungskomponente	Beschreibung
Aufgabenliste	Die in dieser Liste enthaltenen Aufgaben sind für die Konfiguration des SBS 2003 unabdingbar und müssen nach der Installation und Grundkonfiguration ausgeführt werden. Die Abarbeitung der Aufgabenliste wurde bereits in Kapitel besprochen.
Informationscenter	Hier finden Sie Links zur Dokumentation und zu Webressourcen des SBS 2003. Dabei handelt es sich um die Themen der Windows-Hilfe, die Ressourcenseiten auf *http://www.microsoft.com* sowie Links zur Windows Small Business Server-Community.
Interne Webseite	Programme zur Verwaltung der internen Webseite. Diese werden in Kapitel näher erläutert.
Überwachung und Berichterstattung	Werkzeuge für die Anzeige und Konfiguration der Serverleistungs- und Nutzungsberichte, Ereignisprotokolle sowie Überwachung. Weitere Einzelheiten finden Sie in Kapitel .
Internet und E-Mail	Konfiguration der Firewall, der E-Mail-, Telefon- und Modemoptionen sowie des Internet- und Remote-Zugriffs. Diese Werkzeuge werden in Kapitel 8.x beschrieben.
Freigaben (lokal)	Anzeige und Verwaltung aller auf dem SBS 2003 eingerichteten Freigaben. Eine detaillierte Beschreibung finden Sie in Kapitel .
Sicherung	Werkzeuge zum Anzeigen und Ändern des Sicherungszeitplans und des Sicherungsstatus. Weitere Hinweise finden Sie in Kapitel .
Lizenzierung	Verwaltungstools zum Anzeigen und Bearbeiten der SBS 2003-Clientzugriffslizenzen (CALs).
Benutzer	Werkzeuge für die Verwaltung von Benutzerkonten.
Clientcomputer	Werkzeuge für die Verwaltung von Clientcomputern.
Servercomputer	Werkzeuge für die Verwaltung von Servercomputern.
Drucker	Werkzeuge für die Verwaltung von Druckern und Druckaufträgen.
Verteilergruppen	Werkzeuge für die Verwaltung von Verteilergruppen.
Sicherheitsgruppen	Werkzeuge für die Verwaltung von Sicherheitsgruppen.
Benutzervorlagen	Werkzeuge für die Verwaltung von Benutzervorlagen.

Verwaltungskomponente	Beschreibung
Erweiterte Verwaltung	**Unter der erweiterten Verwaltung finden Sie die folgend aufgeführten Verwaltungsinstrumente:**
• Active Directory-Benutzer und -Computer	Hier werden die Computer und Benutzer des Active Directory verwaltet.
• Gruppenrichtlinienverwaltung	Werkzeug für die Erstellung und Verwaltung von Gruppenrichtlinien.
• Lokale Computerverwaltung	Hierüber öffnen Sie die Verwaltungskonsole Computerverwaltung.
• Erste Organisation (Exchange)	Hier gelangen Sie zu den Exchange-Einstellungen, die Sie auch über die Exchange-Verwaltung vornehmen können.
• POP3-Connector Manager	Konfiguration des POP3-Connectors für die Verwaltung von POP3-E-Mails.
• Terminaldienstkonfiguration	Hier gelangen Sie direkt zur Konfiguration und Verwaltung der Terminaldienste des Servers.
• Internetinformationsdienste	Konfiguration der Internetinformationsdienste (IIS 6.0)
• Servereinstellungen migrieren	der Migration können die Einstellungen von einem Server auf einen anderen übertragen werden, siehe Kapitel .

Tabelle 8.1: Die Verwaltungskomponenten der Serververwaltungskonsole

8.1.1 Serververwaltung für Hauptbenutzer

Abbildung 8.2: Die Serververwaltung für Hauptbenutzer

Die Verwaltungskonsole Serververwaltung für Hauptbenutzer besitzt eine begrenzte Anzahl von Verwaltungskomponenten für Benutzer, an die vom Administrator beschränkte Bereiche der Serververwaltung delegiert worden sind. Auf diese Konsole können nur Benutzer zugreifen, die Mitglied der Gruppe Hauptbenutzer sind. Für ein Mitglied der Gruppe Hauptbenutzer ist die Konsole unter STARTMENÜ/PROGRAMME/

VERWALTUNG verfügbar. Möchten Sie diese Konsole als Administrator anzeigen, so öffnen Sie %SYSTEMDRIVE%\DOKUMENTE UND EINSTELLUNGEN\ALL USERS\ANWENDUNGSDATEN\MICROSOFT\SMALLBUSINESSSERVER\ADMINISTRATION\MYSBSCONSOLE.MSC.

Ein wichtiger Unterschied zur Konsole Serververwaltung besteht darin, dass in dieser die eigentliche Konsolenstruktur nicht verfügbar ist (siehe Abbildung 8.2). Damit wird verhindert, dass der Benutzer auf erweiterte Verwaltungsfeatures Zugriff bekommt. So ist z.B. das Löschen von Benutzern oder Computern nicht möglich.

In dieser Konsole sind die folgenden Verwaltungskomponenten verfügbar:

Verwaltungskomponente	Beschreibung
Benutzer	Es können Benutzerkonten hinzugefügt und verwaltet, jedoch nicht gelöscht werden.
Computer	Hier werden Computer sowie Clientanwendungen verwaltet, sind jedoch nicht löschbar.
Gruppen	Es können Sicherheits- und Verteilergruppen hinzugefügt und verwaltet, jedoch nicht gelöscht werden.
Drucker und Faxgeräte	Hinzufügen und Verwalten von Druckern und Faxgeräten
Interne Website	Administration der internen Firmenwebseite
Freigegebene Ordner	Hinzufügen und verwalten von freigegebenen Ordnern.

Tabelle 8.2: Die Verwaltungskomponenten der Konsole Serververwaltung für Hauptbenutzer

8.2 Die Benutzerverwaltung

Unter dem Eintrag BENUTZERVERWALTUNG finden Sie die Links zu den am häufigsten verwendeten benutzerbezogenen Verwaltungsaufgaben. Dabei handelt es sich um die Einträge EINEN BENUTZER HINZUFÜGEN, MEHRERE BENUTZER HINZUFÜGEN, BENUTZERBERECHTIGUNGEN ÄNDERN, KENNWORTRICHTLINIEN KONFIGURIEREN, Weiterleitung des Ordners EIGENE DATEIEN KONFIGURIEREN, Postfach- und Datenträgerkontingenteinstellungen ändern, Remote-Unterstützung anbieten und Computer verwalten.

In der mmc sehen Sie in der Spalte NAME die Benutzerkonten Administrator und Gast sowie sämtliche Benutzerkonten der SBS 2003-Domäne. Der Speicherort der beiden erstgenannten Konten im Active Directory lautet DOMÄNENNAME\USERS, der der SBS-Benutzerkonten DOMÄNENNAME\MYBUSINESS\USERS\SBSUSERS. Dort finden Sie die Benutzer, wenn Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER öffnen.

8.2.1 Einen Benutzer hinzufügen

Hier werden Sie nun Schritt für Schritt durch die Erstellung eines neuen SBS 2003-Benutzerkontos sowie die damit verbundenen weiteren Konfigurationen geleitet.

Um ein Benutzerkonto anzulegen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den Link BENUTZER HINZUFÜGEN.

Dieser Konfigurationsschritt beinhaltet eine Reihe von Aufgaben. Es werden für jeden Benutzer ein Benutzerkonto, Postfach und Basisordner eingerichtet. Weiterhin werden die Mitgliedschaften des Benutzers in den Sicherheits- und Verteilergruppen festgelegt. Auch die SharePoint-Zugriffe sowie die Datenträgerkontingente werden konfiguriert. Schließlich wird dem Benutzer noch ein Clientcomputer zugewiesen.

2. Bevor Sie den Benutzer erstellen, müssen Sie für ihn im Fenster VORLAGENAUSWAHL eine Benutzervorlage auswählen (siehe Abbildung 8.3). Standardmäßig sind bereits die folgenden vier Benutzervorlagen vorhanden:

- USER TEMPLATE: In dieser Vorlage ist der Zugriff auf das Internet, E-Mail, Netzwerkdrucker, Faxgeräte und freigegebene Ordner gestattet. Diese Vorlage sollte für normale Benutzerkonten angewendet werden.
- MOBILE USER TEMPLATE: In dieser Vorlage sind alle Berechtigungen des User Templates enthalten. Zusätzlich kann eine Verbindung auf den SBS 2003 per VPN-Zugriff oder DFÜ-Zugriff hergestellt werden.
- POWER USER TEMPLATE: Diese Vorlage beinhaltet alle Berechtigungen des Mobile User Templates. Weiterhin können Benutzer, die auf dieser Vorlage basieren, Benutzer, Gruppen, Drucker, Faxe und freigegebene Ordner verwalten. Sie können auch eine Remote-Verbindung mit dem Server herstellen. Eine lokale Anmeldung am Server ist jedoch nicht möglich.
- ADMINISTRATOR TEMPLATE: Diese Vorlage verfügt über einen uneingeschränkten Zugriff für die Server- und Domänenverwaltung.

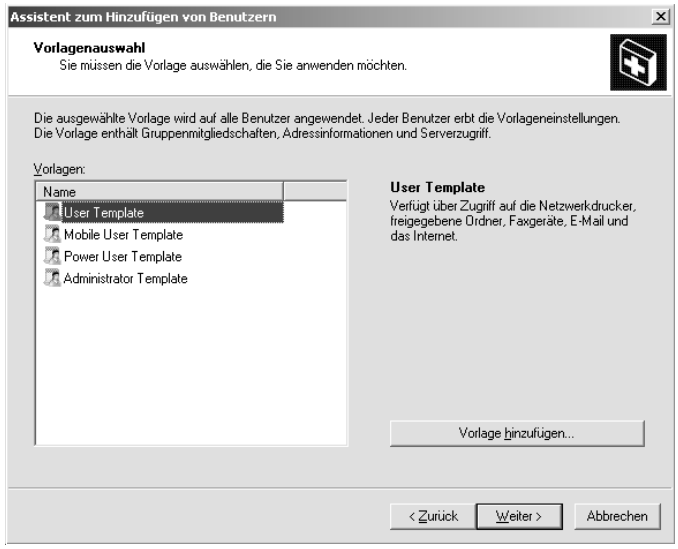


Abbildung 8.3: Auswahl der Benutzervorlage, die auf den Benutzer angewendet werden soll

Neben diesen vordefinierten Benutzervorlagen können Sie auch noch eigene Benutzervorlagen erstellen. Dieses Verfahren wird in Kapitel 8.3, Verwaltung, beschrieben. Weiterhin können Sie zu einem späteren Zeitpunkt für jeden Benutzer die Benutzervorlage ändern. Dieses wird in Kapitel 8.2.3 beschrieben.

Nachdem Sie die passende Vorlage gewählt haben, klicken Sie auf WEITER.

3. Im Fenster BENUTZERINFORMATIONEN (siehe Abbildung 8.4) können Sie über HINZUFÜGEN einen neuen Benutzer für die gewählte Vorlage erstellen. Haben Sie bereits einige neue Benutzer für die Vorlage erstellt, so finden Sie diese unter BENUTZER aufgelistet.

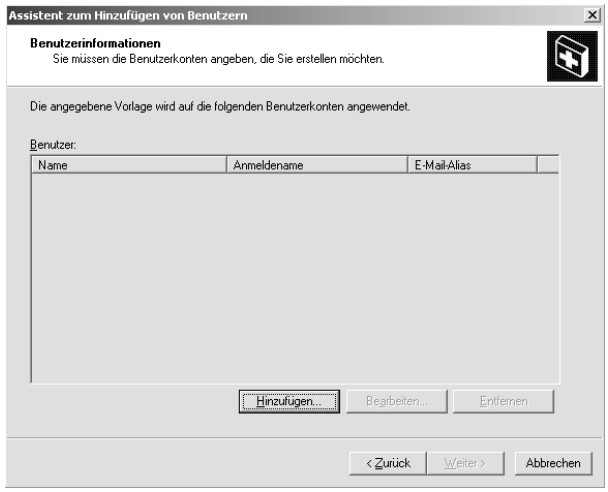


Abbildung 8.4: Die Benutzerinformationen

4. Nachdem Sie eben auf HINZUFÜGEN geklickt haben, füllen Sie im Fenster BENUTZERINFORMATIONEN ANGEBEN (siehe Abbildung 8.5) die entsprechenden Felder aus. Für das Feld ANMELDENAME können Sie aus der Liste eines von vier verfügbaren Formaten auswählen, wie der Anmeldename lauten soll. In unserem Beispiel können Sie zwischen *Pmustermann*, *MustermannPeter*, *PMustermann* und *PeterM* wählen. Diese vorgeschlagenen Werte bieten gegenüber Windows Server 2000 und 2003 den Vorteil, dass Sie als Administrator schnell eine einheitliche Struktur bei der Vergabe der Anmeldenamen realisieren können. In den vorherigen Versionen wurde keine Namensstruktur vorgeschlagen.

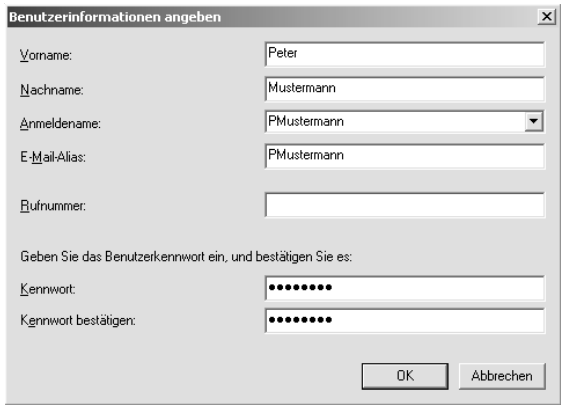


Abbildung 8.5: Die Eingabe der Benutzerinformationen

Der hier gewählte Wert für den Anmeldenamen wird standardmäßig auch für das Feld E-Mail-Alias übernommen, jedoch können Sie dieses auch ändern. Haben Sie die Eingaben abgeschlossen, klicken Sie auf OK.

5. Im Fenster CLIENTCOMPUTER (siehe Abbildung 8.6) können Sie für den Benutzer auch einen Computer einrichten. Wenn Sie die Option COMPUTER JETZT EINRICHTEN wählen, wird dieser in den folgenden Schritten konfiguriert. Klicken Sie dann auf WEITER.

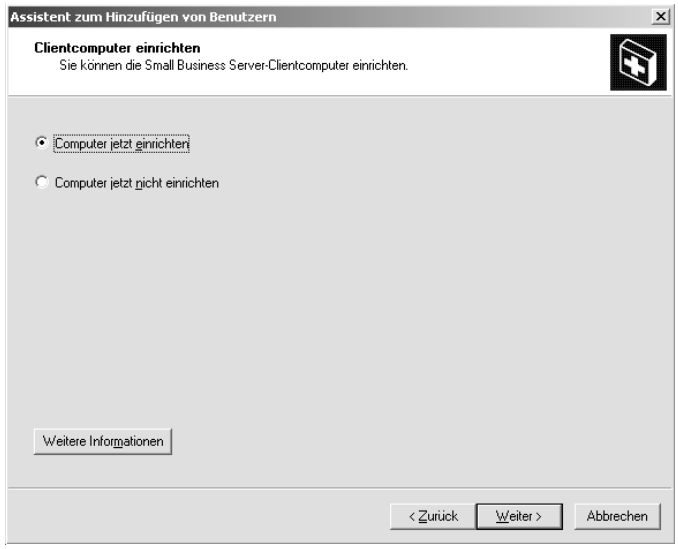


Abbildung 8.6: Dem Benutzerkonto einen Clientcomputer zuweisen

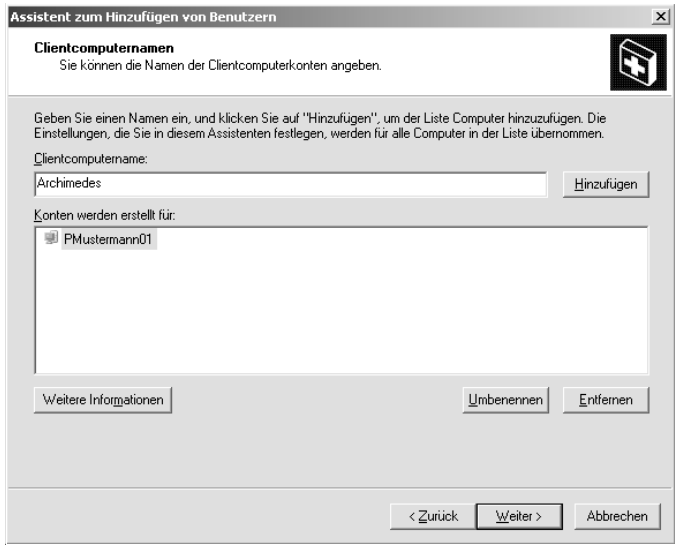


Abbildung 8.7: Bestimmen des Computers für den Benutzer

6. Im Fenster CLIENTCOMPUTERNAMEN (siehe Abbildung 8.7) geben Sie den Namen des Computers an und klicken dann auf HINZUFÜGEN. Gültige Zeichen für den Computernamen sind A–Z, a–z, 0–9 sowie - (Bindestrich). Alle Informationen, die Sie über den Assistenten festlegen, werden für sämtliche Computer übernommen, die sich in der Liste KONTEN WERDEN ERSTELLT FÜR befinden. Aus dieser Liste können Sie auch wieder Computer entfernen. Der standardmäßige Name des Computerkontos lautet immer *Benutzername01*, in unserem Beispiel *PMustermann01*. Dieser Name kann jedoch gelöscht und durch einen anderen ersetzt werden. Klicken Sie dann auf WEITER.
7. Als Nächstes werden im Fenster CLIENTANWENDUNGEN (siehe Abbildung 8.8) die Applikationen ausgewählt, die auf dem Computer installiert werden sollen. Standardmäßig werden dort die Applikationen *Clientbetriebssystem-Service Packs*, *Internet Explorer 6.0*, *Outlook 2003* sowie der *Faxclient* installiert. Diese Auswahl können Sie jedoch ändern und ergänzen.

Deaktivieren Sie die Checkbox vor einer bereits installierten Applikation, so wird diese dadurch *nicht* vom Clientcomputer deinstalliert.

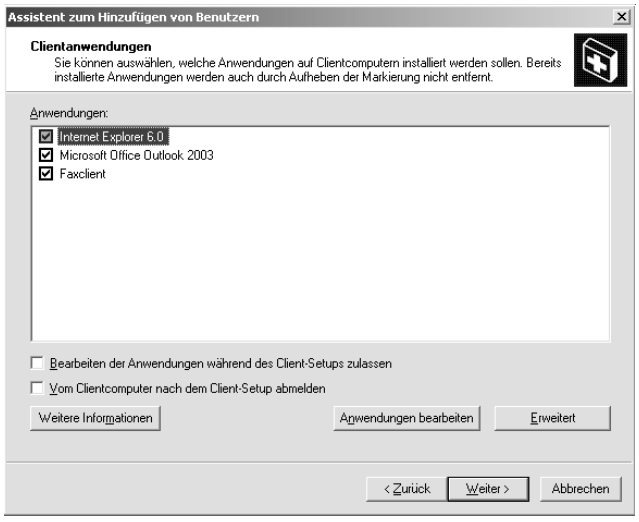


Abbildung 8.8: Festlegen der Clientapplikationen, die auf dem Computer installiert werden sollen

Haben Sie Outlook 2003 für die Installation ausgewählt und ist auf den Clients bereits eine frühere Outlook-Version installiert, müssen Sie auf den Clients die COM-Add-ins deaktivieren. Führen Sie dazu auf dem Client unter Outlook die folgenden Schritte aus:

- Wählen Sie aus dem Menü EXTRAS den Eintrag OPTIONEN und wechseln dann auf die Registerkarte WEITERE.
- Klicken Sie auf ERWEITERTE OPTIONEN und danach auf COM-ADD-INS.
- Deaktivieren Sie die Checkbox bei dem ADD-IN.

8. Markieren Sie im Fenster CLIENTANWENDUNGEN die Checkbox BEARBEITEN DER ANWENDUNGEN WÄHREND DES CLIENT-SETUPS ZULASSEN, wenn Sie dem Benutzer während der Installation gestatten möchten, einen anderen Installationspfad oder eine Applikation nicht zu installieren. Die Checkbox VOM CLIENTCOMPUTER NACH DEM CLIENT-SETUP ABMELDEN sollten Sie dann aktivieren, wenn das Beenden des Setups vom Benutzer nicht abgewartet werden kann und niemand nach Ende der Installation unbefugt auf den Computer zugreifen soll.
9. Klicken Sie auf ANWENDUNGEN BEARBEITEN, erhalten Sie das Fenster VERFÜGBARE ANWENDUNGEN (siehe Abbildung 8.9). Hier sind alle Applikationen aufgelistet, die für die Installation bereitstehen. Über HINZUFÜGEN können Sie noch weitere Applikationen für die Installation auf den Clients bereitstellen.

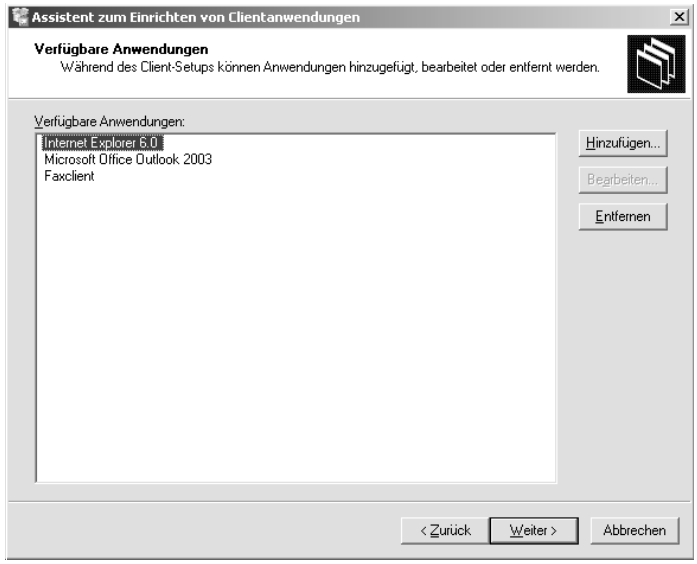


Abbildung 8.9: Für die Clientinstallation verfügbare Applikationen

Haben Sie sich entschieden, eine weitere Applikation hinzuzufügen, erhalten Sie das Fenster ANWENDUNGSINFORMATIONEN (siehe Abbildung 8.10).

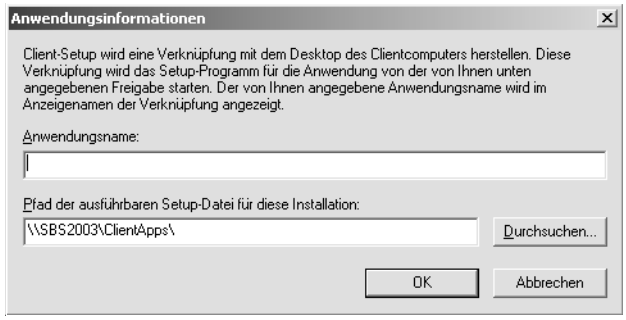


Abbildung 8.10: Angabe der weiteren zu installierenden Clientapplikationen

Bevor Sie hier eine Applikation hinzufügen können, müssen Sie das Installationsprogramm in eine Freigabe kopieren. Am sinnvollsten ist es, diese Applikationen in das Standardverzeichnis \CLIENTAPPS auf dem SBS2003 aufzunehmen. Für den freigegebenen Ordner müssen die Domänenbenutzer über die Berechtigung *Lesen* und *Ausführen* verfügen. Ansonsten können Sie die Installation nicht ausführen.

10. Geben Sie im Textfeld ANWENDUNGSNAME einen Namen für die Applikation an und wählen über DURCHSUCHEN den Pfad zu der Applikation. Für diese Applikation wird auf dem Desktop des Clients eine Verknüpfung angelegt. Klicken Sie dann auf OK. Sie gelangen wieder auf das Fenster VERFÜGBARE ANWENDUNGEN zurück. Dort können Sie die hinzugefügten Applikationen jederzeit bearbeiten. Für die standardmäßig vorhandenen ist die Funktion BEARBEITEN nicht verfügbar. Auch das Löschen von Applikationen aus der Liste ist möglich. Klicken Sie hier auf WEITER, und der Assistent zum Hinzufügen neuer Anwendungen wird beendet.
11. Sie gelangen dann wieder auf die Seite CLIENTANWENDUNGEN. Wenn Sie dort auf ERWEITERT klicken, erhalten Sie das Fenster ERWEITERTE CLIENTCOMPUTEREINSTELLUNGEN (siehe Abbildung 8.11).

Abbildung 8.11: Erweiterte Einstellungen für den Clientcomputer

Für jeden der aufgeführten Punkte können Sie die Standardeinstellung für den Clientcomputer übernehmen, indem Sie die jeweilige Checkbox markieren.

Für die einzelnen Punkte sind die folgenden Standardeinstellungen festgelegt:

- INTERNET EXPLORER-EINSTELLUNGEN: Als Startseite ist die interne Firmenwebsite (*http://Companyweb*) eingestellt. In den Favoriten befinden sich Links zu verschiedenen internen Webseiten. Wurde der ISA-Server installiert, ist der Internet Explorer auch für die Verwendung des Proxy-Servers eingerichtet.
- OUTLOOK-PROFILEINSTELLUNGEN: Outlook ist für die Benutzung des Exchange Servers konfiguriert. So werden in den Profilen für neue Benutzer die Kontoinformationen sowie die Exchange Server-Einstellungen verwendet. Sind auf dem Computer bereits Profile vorhanden, wird das Exchange-Profil des SBS hinzugefügt und als Standard festgelegt. Zusätzlich ist der Faxmailtransport konfiguriert. Dieser ermög-

licht das Senden von Faxen aus Outlook und anderen E-Mail-Applikationen heraus. Ist für den Clientcomputer die Remote-Verwendung eingestellt, wird unter Outlook die manuelle Synchronisation von Outlook-Ordnern eingerichtet.

- DESKTOP-EINSTELLUNGEN: Im Ordner Netzwerkumgebung werden Verknüpfungen und Links erstellt.
- FAXDRUCKER: Auf dem Computer wird ein Faxdrucker eingerichtet, der die Verbindung zum Faxserver verwendet.
- DRUCKER: Es wird der im Active Directory veröffentlichte Drucker vom SBS den Clients als Standarddrucker hinzugefügt. Sind im Active Directory jedoch mehrere Drucker veröffentlicht oder ist an den Client ein lokaler Drucker angeschlossen, so wird kein Standarddrucker festgelegt.
- FAXKONFIGURATIONSINFORMATIONEN: Es werden die vom SBS gespeicherten Faxinformationen an die Clients weitergegeben. Dazu zählt beispielsweise das Faxdeckblatt mit den Absenderinformationen, so dass die Benutzer diese Angaben nicht für jedes Fax erneut angeben müssen.
- REMOTE-DESKTOP: Für die Clients werden der Remote-Desktop sowie die Remote-Desktop-Unterstützung aktiviert. Über den RemoteDesktop können die Benutzer beispielsweise von zu Hause oder von unterwegs eine Sitzung mit ihrem Clientcomputer herstellen. Über die Remote-Desktop-Unterstützung wird es anderen Benutzern ermöglicht, eine Verbindung zum Client herzustellen und beim Beheben von Problemen einzugreifen.

  Wird die Checkbox deaktiviert, können Sie die Einstellung auf dem Client manuell konfigurieren. Klicken Sie dann auf OK.

12. Als Nächstes erhalten Sie die Seite MOBILCLIENT UND OFFLINEVERWENDUNG (siehe Abbildung 8.12).

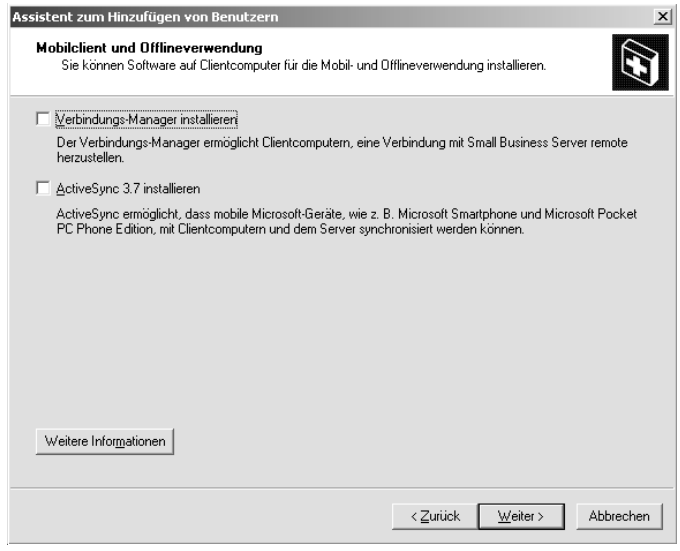


Abbildung 8.12: Konfiguration des Computers für die Mobil- und Offlinebenutzung

Sie haben hier die Möglichkeit, den Verbindungs-Manager und ActiveSync 3.7 zu installieren.

- VERBINDUNGS-MANAGER: Mit Hilfe des Verbindungs-Managers können die Benutzer eine Remote-Verbindung mit dem SBS 2003 herstellen.
- ACTIVESYNC 3.7: Über ActiveSync können die Benutzer mobile Geräte, wie z.B. Microsoft Smartphone oder Microsoft Pocket PC Phone Edition, mit dem Clientcomputer und Server synchronisieren.

Damit die Benutzer die Remote-Verbindung nutzen können, müssen Sie den Assistenten für die RAS-Verbindung in der Aufgabenliste abgeschlossen haben. Zusätzlich muss der Benutzer zu der Benutzervorlage Mobile Users (siehe Schritt 1 in diesem Kapitel) hinzugefügt worden sein.

Klicken Sie anschließend auf WEITER.

13. Sie erhalten nun das Fenster FERTIGSTELLEN DES ASSISTENTEN (siehe Abbildung 8.13). Sofern Sie mit den Einstellungen einverstanden sind, klicken Sie auf FERTIG STELLEN. Über ZURÜCK können Sie noch Änderungen an der Konfiguration vornehmen.

Abbildung 8.13: Fertigstellen des Assistenten für das Hinzufügen von Benutzern

14. Während die Einstellungen für den Benutzer konfiguriert werden, erhalten Sie ein Hinweisfenster (siehe Abbildung 8.14). Um die Konfiguration des Clientcomputers inklusive seiner Netzwerkkonfiguration und der Anwendungsbereitstellung abzuschließen, müssen Sie sich auf dem Client anmelden und im Browser die Adresse *http://SBSServername/ConnectComputer* eingeben. Klicken Sie zum Bestätigen auf OK.

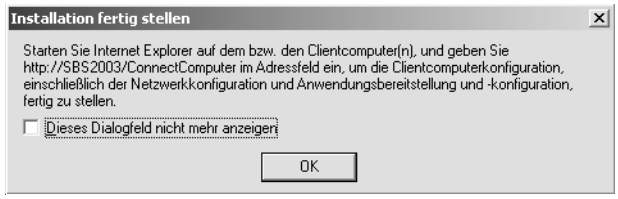


Abbildung 8.14: Hinweis für den Abschluss der Clientcomputerkonfiguration

15. Nachdem das Benutzerkonto erstellt worden ist, werden Sie gefragt, ob Sie den Assistenten erneut starten möchten, um einen neuen Benutzer anzulegen. Haben Sie hier NEIN gewählt, erfolgt noch ein Hinweisfenster (siehe Abbildung 8.15), das Sie darüber informiert, dass Sie nun für die Benutzerkonten die Übermittlung von POP3-E-Mail konfigurieren können. Bestätigen Sie dieses Fenster mit OK.

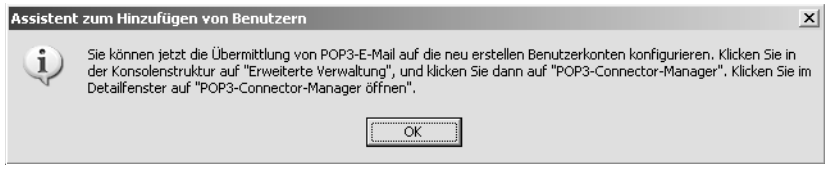


Abbildung 8.15: Hinweisfenster für die Konfiguration von POP3-E-Mail

Eigenschaften von Benutzerkonten

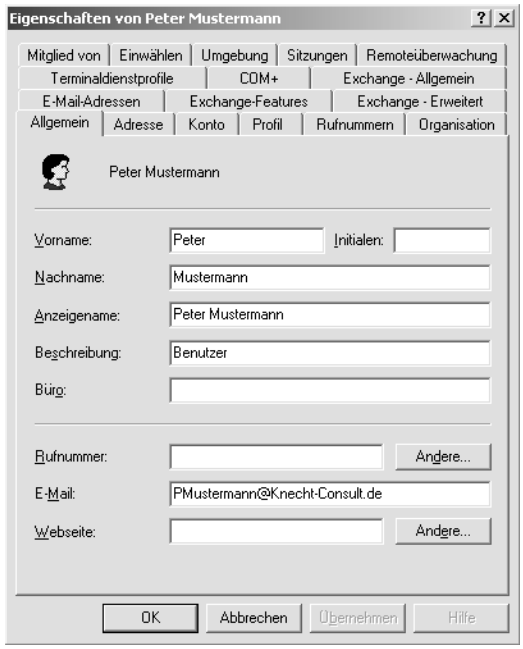


Abbildung 8.16: Die Eigenschaften eines Benutzerkontos

Nachdem Sie nun das neue Benutzerobjekt erstellt haben, finden Sie es in der Serververwaltung unter dem Link BENUTZER sowie in der mmc Active Directory-Benutzer und -Computer in dem Container DOMÄNENNAME/MYBUSINESS/USERS/SBSUSERS. Jedes Benutzerkonto verfügt über einen vordefinierten Satz an Eigenschaften, den Sie für jeden Benutzer individuell konfigurieren können. Um auf die Eigenschaften eines Benutzers zuzugreifen, wählen Sie den gleichnamigen Eintrag aus dem Kontextmenü (siehe Abbildung 8.16).

Die Eigenschaften sind in 17 Kategorien eingeteilt. Für jede Kategorie steht eine Registerkarte bereit. Ein lokales Benutzerkonto enthält nur drei Registerkarten, nämlich ALLGEMEIN, PROFIL und MITGLIED VON. Die Bedeutung der einzelnen Registerkarten wird in der folgenden Tabelle erläutert. Die wichtigsten dieser Eigenschaften werden im Anschluss detailliert vorgestellt.

Registerkarte	Beschreibung
Allgemein	Hier können Sie den Namen des Benutzers, eine optionale Beschreibung sowie Angaben zu seinem Büro, seiner Telefonnummer, E-Mailadresse und Webseite vornehmen. Einträge müssen nur in den Feldern Vorname, Nachname und Anzeigename vorhanden sein. Der Rest ist optional.
Adresse	Tragen Sie hier die Adresse (Straße, Postfach, Stadt, Bundesland, PLZ sowie Land/Region) ein. Auch diese Einträge sind optional.
Konto	Sie finden hier den Benutzeranmeldenamen sowie weitere Optionen zum Benutzerkonto. Diese werden weiter unten gesondert erklärt. Außerdem können Sie die Anmeldezeiten sowie die Liste der Computer, von denen aus sich der Benutzer aus anmelden darf, begrenzen.
Profil	Hier können Sie den Pfad zu einem Benutzerprofil, ein Anmeldeskript sowie einen Basisordner für Dokumente angeben.
Rufnummern	Hier können Sie zusätzliche Rufnummern des Benutzers angeben (Privat, Funkruf, Mobil, Fax und IP-Telefon).
Organisation	Hier können Sie firmenbezogene Angaben wie Anrede, Abteilung, Firma und Vorgesetzter eintragen.
E-Mail-Adressen	Bearbeiten der E-Mail-Antwortadressen für die verschiedenen Adresstypen wie SMTP oder X400.
Exchange-Features	Anzeigen und Ändern des Status für mobile Dienste wie OMA oder Synchronisierung und Protokolle wie OWA, POP3 und IMAP4.
Exchange – Erweitert	Hier finden Sie erweiterte Exchange-Einstellungen wie Aufnahme in Adresslisten, Postfachberechtigungen und erweiterte Attribute.
Terminaldienstprofile	Hier können Sie ein Benutzerprofil und das Basisverzeichnis für die Terminaldienstsitzungen angeben.
COM+	Bestimmen der COM+-Partitionsgruppe
Exchange – Allgemein	Einstellungen des E-Mail-Alias, der Zustellungsoptionen, Empfangseinschränkungen und Speichergrenzwerte.

Registerkarte	Beschreibung
Mitglied von	Hier können Sie festlegen, in welchen Gruppen der Benutzer Mitglied sein soll. Standardmäßig gehört er nur der Gruppe Domänenbenutzer an. Jeder Benutzer hat eine Gruppe als seine primäre Gruppe definiert. Wenn er mehreren Gruppen angehört, können Sie die Einstellung über „Primäre Gruppe festlegen“ ändern.
Einwählen	Hier können Sie die Optionen für RAS-Zugriff konfigurieren. Standardmäßig ist kein RAS-Zugriff erlaubt.
Umgebung	Sie bestimmen hier, ob bei der Anmeldung Netzlaufwerke und Drucker automatisch verbunden werden und welche Programme beim Start der Terminaldienste ausgeführt werden sollen.
Sitzungen	Hier werden Optionen für die Terminalsitzungen vorgenommen.
Remote-Überwachung	Hier können Sie die Remote-Überwachung für die Terminaldienste aktivieren oder deaktivieren sowie die Benutzererlaubnis zur Überwachung ein- und ausschalten.

Tabelle 8.3: Die Registerkarten in den Eigenschaften eines Benutzerkontos

8.2.2 Mehrere Benutzer hinzufügen

Das Hinzufügen mehrerer Benutzer beinhaltet dieselben im letzten Kapitel beschriebenen Einstellungen. Für diesen Vorgang wählen Sie aus dem Kontextmenü von BENUTZER den Eintrag MEHRERE BENUTZER HINZUFÜGEN.

Das Hinzufügen mehrerer Benutzer gleicht dem eben beschriebenen Prozess, einen neuen Benutzer zu erstellen. Sie beginnen hier damit, für die zu erstellenden Benutzer eine Vorlage auszuwählen (siehe Abbildung 8.3) und dieser Vorlage dann eine Reihe von Benutzern hinzuzufügen. Danach können Sie den weiteren in Kapitel Abbildung 8.2.1 beschriebenen Schritten folgen.

8.2.3 Benutzerberechtigungen ändern

Nachdem Sie einen Benutzer erstellt haben, können Sie diesem auf Basis seiner Benutzervorlage die Berechtigungen ändern.

1. Um die Berechtigungen zu ändern, wählen Sie aus dem Kontextmenü von BENUTZER den Eintrag BENUTZERBERECHTIGUNGEN ÄNDERN.
2. Im Fenster VORLAGENAUSWAHL (siehe Abbildung 8.17) wählen Sie zunächst die neue Vorlage aus, die für den Benutzer gelten soll. Danach können Sie eine der folgenden Optionen wählen: ALLE BERECHTIGUNGEN ERSETZEN, DIE DEN BENUTZERN ZUVOR ERTEILT WURDEN oder BERECHTIGUNGEN ZU DEN BERECHTIGUNGEN HINZUFÜGEN, DIE DEN BENUTZERN ZUVOR ERTEILT WURDEN. Im ersten Fall werden alle bestehenden Berechtigungen des Benutzers durch die Berechtigungen überschrieben, welche die neue Vorlage liefert. Durch die zweite Option werden die bereits erteilten Berechtigungen des Benutzers mit den durch die neue Vorlage gegebenen Berechtigungen addiert. Klicken Sie dann auf WEITER.

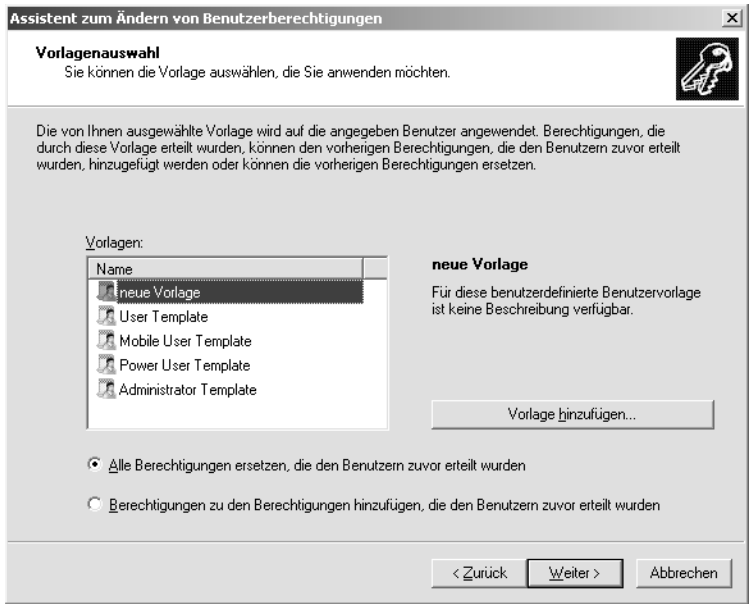


Abbildung 8.17: Das Ändern der Benutzerberechtigungen auf Basis der Vorlagen

3. Danach wählen Sie die Benutzer aus, deren Berechtigungen durch die neue Vorlage definiert werden sollen. Markieren Sie dazu im linken Fenster die gewünschten Benutzer und klicken auf HINZUFÜGEN. Klicken Sie dann auf WEITER. Stellen Sie danach den Assistenten fertig.

8.2.4 Kennwortrichtlinien konfigurieren

1. Nachdem Sie erstmalig einen neuen Benutzer angelegt und in diesem Vorgang das Hinweisfenster für POP3-E-Mail (siehe Abbildung 8.18) geschlossen haben, erhalten Sie ein neues Fenster, das Sie zur Konfiguration der Kennwortrichtlinien auffordert. Bestätigen Sie mit JA. Es erscheint das Fenster KENNWORTRICHTLINIEN KONFIGURIEREN (siehe Abbildung 8.18). Alternativ können Sie auch den Link KENNWORTRICHTLINIEN KONFIGURIEREN auswählen, wenn Sie in der Serververwaltung den Eintrag BENUTZER geöffnet haben.
2. Aus Sicherheitsgründen sollten Sie über die Kennwortrichtlinien die Anforderungen für die Vergabe von Kennwörtern festlegen. Markieren Sie die Checkbox KENNWORT MUSS MINIMALEN LÄNGENVORAUSSETZUNGEN ENTSPRECHEN und wählen eine Zeichenlänge aus. Kennwörter, die kürzer als die vorgegebene Länge sind, werden nicht akzeptiert. Die Mindestlänge beträgt sieben Zeichen.

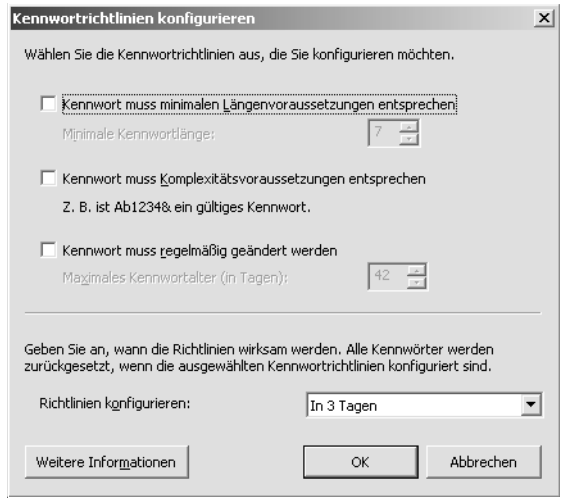


Abbildung 8.18: Die Konfiguration der Kennwortrichtlinien

3. Ist die Checkbox KENNWORT MUSS KOMPLEXITÄTSVORAUSSETZUNGEN ERFÜLLEN aktiviert, müssen die Kennwörter Zeichen aus drei der vier folgenden Kategorien enthalten:
   1. Großbuchstaben A–Z
   2. Kleinbuchstaben a–z
   3. Ziffern 0–9
   4. Sonderzeichen wie z.B. %, # oder $.

   Zudem darf das Kennwort nicht dem Kontonamen des Benutzers (auch nicht in Teilen) entsprechen.
4. Ist die Checkbox KENNWORT MUSS REGELMÄSSIG GEÄNDERT WERDEN aktiviert, können Sie bestimmen, nach wie vielen Tagen das Kennwort geändert werden muss. Die längste Gültigkeitsdauer für ein Kennwort beträgt 42 Tage.
5. Schließlich geben Sie unter RICHTLINIEN KONFIGURIEREN an, ab wann die neuen Richtlinien wirksam werden sollen. Standardmäßig geschieht dies nach drei Tagen. Sie sollten zunächst dieses Intervall beibehalten, damit Sie im Zuge der Clientkonfiguration bei der Anmeldung an den Clients noch keine komplexen Kennwörter verwenden müssen. Nach Abschluss der Clientkonfiguration sollten Sie den Wert auf SOFORT setzen.
6. Klicken Sie dann zum Übernehmen der Einstellungen auf OK.

Möchten Sie später für einen Benutzer weitere Kennworteinstellungen vornehmen, so wechseln Sie in dessen EIGENSCHAFTEN auf die Registerkarte KONTO. Dort finden Sie unter KONTOOPTIONEN die folgenden Einträge:

Kennwortoption	Beschreibung
Benutzer muss Kennwort bei der nächsten Anmeldung ändern.	Bei der ersten Anmeldung erhält der Benutzer einen Hinweis, dass er sein Kennwort ändern muss. Damit liegt die Verantwortung für das Kennwort beim Benutzer.
Benutzer kann Kennwort nicht ändern.	In diesem Fall kann nur der Administrator das Kennwort ändern. Diese Option ist beispielsweise für das Gastkonto sinnvoll, da dieses von mehreren Benutzern verwendet werden kann.
Kennwort läuft nie ab.	Das Kennwort muss nie, kann aber jederzeit geändert werden.
Konto ist deaktiviert.	Das Konto ist zwar eingerichtet, kann aber noch nicht verwendet werden.
Kennwort mit reversibler Verschlüsselung speichern	Standardmäßig sind die Kennwörter in der Kennwortdatenbank verschlüsselt. Die standardmäßige Verschlüsselung ist nicht umkehrbar. Bei Verwendung der reversiblen Verschlüsselung können Kennwörter aus der Datenbank wiederhergestellt werden. Bei Verwendung der reversiblen Verschlüsselung muss die Passwortdatenbank gut gegen Angriffe von außen abgesichert sein. Für Benutzer eines Apple Macintosh-Clients müssen Sie diese Option aktivieren, da diese Clients ausschließlich mit reversibler Verschlüsselung arbeiten.
Benutzer muss sich mit einer Smartcard anmelden.	Der Benutzer muss sich anhand einer Smartcard über ein Kartenlesegerät authentifizieren.
Konto wird für Delegierungszwecke vertraut.	Dieser Benutzer hat das Recht, anderen Benutzern oder Gruppen Teile des Domänen-Namensraums zur Verwaltung zu übergeben.
Konto kann nicht delegiert werden.	Diesem Konto kann von keinem anderen Benutzer die Delegierung von Verwaltungsaufgaben übergeben werden.
DES-Verschlüsselungstypen für dieses Konto benutzen	Hiermit können Sie die Unterstützung für DES (Data Encryption Standard) aktivieren. DES unterstützt verschiedene Verschlüsselungsmechanismen, z.B. MPPE 40, 64 und 128 Bit oder IPSec in verschiedenen Stufen.
Keine Kerberos-Präauthentifizierung erforderlich	Aktivieren Sie diese Option nur, wenn für das Konto nicht die Kerberosimplementierung von Windows 2000 eingesetzt wird, sondern beispielsweise ein Unix-Implementierung, die einen anderen Zeitmechanismus für die Ausgabe des ticketgenehmigenden Tickets durch das KDC (Key Distribution Center) verwendet.

Tabelle 8.4: Die Kennwortoptionen für ein Benutzerkonto

Außerdem können Sie festlegen, ob das Konto zu einem bestimmten Zeitpunkt ablaufen soll oder nicht (Letzteres ist Standard). Dies ist sinnvoll, wenn einige Mitarbeiter nur zeitweise beschäftigt sind. Soll das Konto zu einem bestimmten Zeitpunkt ablaufen, markieren Sie die entsprechende Checkbox und wählen aus dem Kalenderelement das gewünschte Datum.

Anmeldezeiten eines Benutzers festlegen

Weiterhin befindet sich auf der Registerkarte KONTO auch die Schaltfläche ANMELDEZEITEN. Darüber können Sie festlegen, wann sich der Benutzer an der Domäne anmelden darf. Standardmäßig kann sich der Benutzer jeden Tag in der Woche rund um die Uhr anmelden. Um die Anmeldezeiten einzuschränken, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche ANMELDEZEITEN. Sie sehen, dass die Zeiten nicht eingeschränkt sind.
2. Markieren Sie nun die Zeiten, zu denen eine Anmeldung nicht notwendig ist, so dass sie weiß hinterlegt sind, und markieren für diese die Checkbox ANMELDUNG VERWEIGERN. In unserem Beispiel (siehe Abbildung 8.19) ist die Anmeldezeit auf werktags von 8:00 h bis 18:00 h beschränkt. Für einen herkömmlichen Büroangestellten sollten diese Zeiten ausreichen. Klicken Sie dann auf OK.

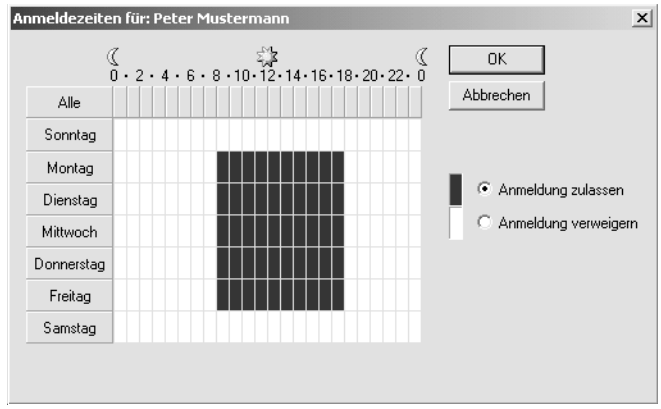


Abbildung 8.19: Die Anmeldezeiten für einen Benutzer beschränken

Die Anmeldung auf bestimmte Computer beschränken

Über die Schaltfläche ANMELDEN auf der Registerkarte KONTO können Sie bestimmen, von welchen Computern aus sich der Benutzer anmelden darf. Wenn ein Benutzer nur an einem festen Arbeitsplatz oder von seinem Laptop aus arbeitet, können Sie ihm nur diesen Rechner zuweisen. Standardmäßig kann er sich von allen Computern aus anmelden. Um die Anmelderechner einzuschränken, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche ANMELDEN. Sie sehen, dass die Option ALLE COMPUTER aktiviert ist (siehe Abbildung 8.20).
2. Um den Anmeldevorgang auf einen oder mehrere Computer zu beschränken, geben Sie in das Textfeld COMPUTERNAME den Namen des Computers ein und klicken auf HINZUFÜGEN. Wiederholen Sie diesen Prozess, bis Sie alle gewünschten Rechner in die Liste aufgenommen haben. Um später wieder Rechner aus der Liste zu löschen, markieren Sie die gewünschten Computer und klicken auf ENTFERNEN. Über die Schaltfläche BEARBEITEN können Sie den Namen eines in der Liste vorhandenen Computers ändern. Klicken Sie dann auf OK.

Abbildung 8.20: Auswahl der Computer, von denen aus sich der Benutzer anmelden darf

Sie können die gültigen Anmeldezeiten nur für alle gültigen Anmelderechner und nicht für jeden dieser Rechner einzeln festlegen.

Bedenken Sie auch Folgendes: Je restriktiver Sie die gültigen Anmeldezeiten und Anmeldecomputer für die Benutzer handhaben, desto geringer wird auch die Wahrscheinlichkeit, dass ein Konto zu Unrecht benutzt werden kann.

Die tägliche Arbeit mit Benutzerkonten

Zur täglichen Arbeit mit Konten zählen neben dem eben beschriebenen Erstellen und Konfigurieren noch weitere Tätigkeiten. Zu den weiteren administrativen Aufgaben gehören auch das Aktivieren bzw. Deaktivieren von Konten, Umbenennen von Konten sowie das Entsperren von Konten.

Um ein aktives Konto zu deaktivieren oder ein deaktiviertes Konto zu aktivieren, wählen Sie aus dem Kontextmenü des Benutzers den Eintrag KONTO DEAKTIVIEREN bzw. KONTO AKTIVIEREN. Sie sollten ein Konto so lange deaktiviert lassen, bis es benötigt wird. Haben Sie beispielsweise Mitte des Monats bereits die Benutzerkonten für Mitarbeiter eingerichtet, die erst im nächsten Monat ihre Tätigkeit aufnehmen, so sollten diese Konten auch erst am 1. des Folgemonats aktiviert werden, um eventuellen Missbrauch zu verhindern. Deaktivierte Konten sind immer mit dem Symbol des weißen Kreuzchens im roten Kreis gesondert gekennzeichnet.

Auch für das Umbenennen von Konten wählen Sie den entsprechenden Eintrag aus dem Kontextmenü. Das Umbenennen eines Kontos ist sinnvoll, wenn ein neuer Mitarbeiter die Einstellungen seines Vorgängers bis auf den Namen übernehmen soll.

Soll ein Benutzer gelöscht werden, verwenden Sie den Kontextmenüeintrag BENUTZER ENTFERNEN.

Schließlich finden Sie im Kontextmenü noch den Eintrag KENNWORT ÄNDERN. Auch wenn Sie bei den Kennwortoptionen die Passwortvergabe durch den Benutzer eingestellt haben (siehe Tabelle 8.4), können Sie als Administrator jederzeit das Kennwort eines Benutzers zurücksetzen, falls dieser sich sein Kennwort nicht merken konnte und sich deshalb nicht mehr anmelden kann. Um ein Kennwort wieder zurückzusetzen, wählen Sie den oben genannten Eintrag aus dem Kontextmenü, geben das neue Kennwort ein und bestätigen es. Sie können auf diese Weise auch ein leeres Kennwort vergeben. Teilen Sie dieses vorläufige Kennwort dem ausgesperrten Benutzer mit und bitten ihn, sich künftig sein Kennwort besser zu merken. Er kann nun, wenn die Option aktiviert ist, das vom Administrator vergebene Kennwort bei der Anmeldung ändern.

8.2.5 Verwalten von Benutzerprofilen

In diesem Kapitel werden Ihnen die Grundlagen von Benutzerprofilen und Basisverzeichnissen nahegebracht. In einem Benutzerprofil werden diverse Ordner mit Daten und Konfigurationseinstellungen eines Benutzers gespeichert. Mit Benutzerprofilen kann die Konsistenz der Benutzereinstellungen sichergestellt werden. Bei einem Basisverzeichnis handelt es sich um einen alternativen Ordner zum Speicherort EIGENE DATEIEN. Zunächst lernen Sie die verschiedenen Arten von Benutzerprofilen kennen. Danach erfahren Sie, wie Benutzerprofile und Basisverzeichnisse eingerichtet und konfiguriert werden.

Arten von Benutzerprofilen

Ein Benutzerprofil umfasst alle persönlichen Einstellungen und Dateien eines Benutzers. Man spricht auch von den Desktop-Einstellungen auf dem lokalen Computer. Ein neues Benutzerprofil wird automatisch erstellt, sobald sich ein neuer Benutzer das erste Mal an einem Computer anmeldet. Bei der Installation werden standardmäßig die Profile für die folgenden Benutzer angelegt: für den Kontonamen des Benutzers, der bei der Installation angegeben wird, DEFAULT USER und ALL USERS. Durch den Einsatz von Profilen können mehrere Benutzer an einem Computer arbeiten, wobei jeder seine persönlichen Einstellungen bekommt und sich seine Änderungen nicht auf die Einstellungen der anderen Benutzer auswirken. Angenommen, Benutzer 1 möchte auf seinem Desktop große Icons verwenden und wählt diese Option. Bei der nächsten Anmeldung erhält ausschließlich Benutzer 1 die großen Icons, während Benutzer 2 weiterhin die herkömmlichen Windows-Icons behält. In einem Profil sind immer die Einstellungen und Daten enthalten, die beim letzten erfolgreichen Herunterfahren des Computers eingestellt und vorhanden waren. Das Profil beinhaltet also eine Momentaufnahme vom letzten Zustand vor dem Herunterfahren. Wird der Computer nicht ordnungsgemäß heruntergefahren, kann auch das Benutzerprofil Schaden nehmen, indem möglicherweise nicht alle Änderungen in das Profil eingetragen werden.

Jedes Profil beinhaltet dieselben Inhalte, nur hinsichtlich des Speicherortes und der Änderungsmöglichkeiten unterscheiden sie sich. Die lokalen Benutzerprofile befinden sich im Verzeichnis %SYSTEM%\DOKUMENTE UND EINSTELLUNGEN\%BENUTZERANMELDENAME%, z.B. C:\Dokumente und Einstellungen\Administrator. Wurde der Computer von Windows NT auf Windows 2000/XP aktualisiert, so befindet sich das Profil in %SYSTEMROOT%\PROFILES\%BENUTZERANMELDENAME%. Servergespeicherte Profile befinden sich in einer Netzwerkfreigabe auf einem Server. Ein Profil enthält die persönlichen Ord-

ner, individuelle Einstellungen, z.B. die Bildschirmauflösung, das Farbschema, Ansichtsoptionen im Windows-Explorer, Favoriten usw. Diese Informationen befinden sich in den folgenden Ordnern des Profils:

Ordner	Inhalt
Anwendungsdaten1	Hier werden persönliche Einstellungen zu Applikationen gespeichert, beispielsweise die Office-Benutzerwörterbücher oder Office-Vorlagen. Alle Windows 2000/XP-konformen Applikationen legen dort die persönlichen Einstellungen ab anstatt direkt im Programmverzeichnis.
Cookies	Hier befinden sich Informationen über besuchte Internet-Seiten.
Desktop	Hier werden alle Elemente des aktuellen Desktops wie Verknüpfungen oder auf dem Desktop gespeicherte Daten abgelegt.
Druckumgebung1	Hier befinden sich Verknüpfungen zu Objekten des Druckerordners.
Eigene Dateien	Eigene Dateien wird als das Standardverzeichnis für persönliche Dokumente benutzt. Microsoft-Applikationen, wie z.B. das Office-Paket, geben auch diesen Pfad vor. Darin enthalten ist auch der Ordner EIGENE BILDER. Er ist der Speicherort für alle Grafikelemente des Benutzers.
Favoriten	Hier befinden sich die Verknüpfungen zu den als Favoriten gewählten Internetseiten.
Lokale Einstellungen1	Dieser Ordner beinhaltet vier weitere Ordner: ANWENDUNGSDATEN, z.B. Outlook-Archive, TEMP für alle temporär verwendeten Dateien, TEMPORARY INTERNET FILES für zwischengespeicherte Internetdaten und VERLAUF für eine Übersicht über besuchte Internetseiten.
Netzwerkumgebung1	Hier befinden sich Verknüpfungen zu Netzwerkelementen wie aktuell verbundenen Netzlaufwerken.
Recent1	In diesem Ordner wird eine Liste der zuletzt geöffneten Dokumente und Ordner gepflegt.
Send to1	Hier befinden sich die Verknüpfungen zu Elementen, die Sie im Kontextmenüs eines Objekts unter SENDEN AN finden.
Startmenü	Hier befinden sich die Verknüpfungen zu allen Einträgen und Elementen des Startmenüs.
Vorlagen	Hier befinden sich Vorlagen für Dokumenttypen, die auf dem Computer geöffnet werden können.
NTUSER.DAT11	Diese Datei speichert Registry-Einstellungen wie Monitorauflösung, bevorzugtes Farbschema, Ansichtsoptionen des Explorers und der Ordner. Ist die *NTUSER.DAT* beschädigt oder fehlt sie, wird für den Benutzer ein neues Profil angelegt, obwohl die Verknüpfungen noch alle in den oben beschriebenen Ordnern vorhanden sind.

Tabelle 8.5: Die Inhalte eines Benutzerprofils

Die mit 1 gekennzeichneten Ordner sind nur sichtbar, wenn Sie im Windows-Explorer unter EXTRAS/ORDNEROPTIONEN/ANSICHT die Option ALLE DATEIEN UND ORDNER ANZEIGEN gewählt haben. Standardmäßig werden diese versteckten Objekte nicht angezeigt.

Es gibt insgesamt drei Arten von Benutzerprofilen. Es handelt sich um lokale, servergespeicherte sowie verbindliche Benutzerprofile. Die folgende Tabelle gibt eine Übersicht über diese verschiedenen Typen.

Benutzerprofil	Beschreibung
Lokal	Diese Art von Profilen wird angelegt, sobald sich ein neuer Benutzer das erste Mal an einem Computer anmeldet. Die in diesem Profil gespeicherten Einstellungen sind ausschließlich für den lokalen Computer gültig.
Servergespeichert	Die servergespeicherten Profile werden nicht lokal, sondern auf einem Server abgelegt. Sie sind stets verfügbar. Dabei ist es gleichgültig, von welchem Rechner im Netzwerk aus sich der Benutzer anmeldet, er bekommt immer seine persönlichen Einstellungen. Nimmt der Benutzer Änderungen vor, werden diese auch auf dem Server gespeichert. Ein servergespeichertes Profil muss vom Administrator eingerichtet werden.
Verbindlich	Auch dieses Profil wird auf einem Server gespeichert. Es ist somit auch immer verfügbar, egal an welchem Rechner sich der Benutzer anmeldet. Allerdings werden in diesem Profil seine Änderungen nicht gespeichert. Der Benutzer bekommt immer wieder die Einstellungen, die der Administrator einmal für ihn oder eine ganze Benutzergruppe festgelegt hat.

Tabelle 8.6: Die drei Arten von Benutzerprofilen

Ein lokales Profil muss im Gegensatz zu servergespeicherten und verbindlichen Profilen nicht explizit eingerichtet werden. Es wird automatisch bei jeder Anmeldung eines neues Benutzers eingerichtet. Hierzu werden die Grundeinstellungen des Ordners DEFAULT USER in DOKUMENTE UND EINSTELLUNGEN benutzt und mit einem neuen Namen versehen.

Checkliste zum Einrichten von Benutzerprofilen

Die folgende Checkliste gibt Ihnen einen Überblick über die erforderlichen Schritte, die Sie zur Einrichtung und Konfiguration servergespeicherter Benutzerprofile bis hin zum Festlegen von Kontingentgrenzen für Benutzerprofile durchführen sollten. Da diese Schritte hier nicht chronologisch beschrieben werden, sondern in den jeweiligen Gesamtkontext eines Kapitels eingegliedert sind, werden die jeweils relevanten Kapitel angegeben.

1. Wählen Sie einen Dateiserver aus, und erstellen Sie auf diesem einen oder mehrere freigegebene Ordner, in dem/denen Sie die Benutzerprofile speichern möchten. Durch die Verwendung eines zentralen Speicherorts wird Ihnen auch die Datensicherung erleichtert.

2. Richten Sie die servergespeicherten Benutzerprofile ein. Überlegen Sie sich, für welche Anwendergruppen welche Einstellungen sinnvoll sein können.
3. Spezifizieren Sie die Benutzerordner, für die Sie Ordnerumleitungen einrichten möchten. Diese umgeleiteten Ordner stellen sich für die Benutzer wie lokale Ordner dar und belasten im Gegensatz zu Ordnern, die im servergespeicherten Profil liegen, nicht das Netzwerk.
4. Aktivieren Sie bei Bedarf die Option, Dateien und Ordner offline verfügbar zu machen. Damit kann einem Benutzer auch dann Zugriff auf die Daten gewährt werden, wenn er nicht am Netzwerk angemeldet ist.
5. Legen Sie über Datenträgerkontingente Beschränkungen fest, wie groß die Inhalte der Benutzerprofile maximal sein dürfen.
6. Erstellen Sie einen Plan, welche Optionen von Gruppenrichtlinien und anderen Konfigurationseinstellungen Sie als standardmäßige oder erweiterte Funktionen definieren möchten. Teilen Sie Ihre Angestellten in Gruppen ein, die auf deren Funktion basieren, und weisen Sie dann den Gruppen standardmäßige oder erweiterte Optionen zu.

Einrichten eines servergespeicherten Profils

Das servergespeicherte Profil wird auf einem Server im Netzwerk abgelegt und ist somit immer verfügbar. Die persönlichen Einstellungen sind für den Benutzer an jedem Computer verfügbar, an dem er sich anmeldet, und nicht auf einen lokalen Rechner begrenzt. Bei der Anmeldung an einem Computer kopiert Windows die Daten des Profils auf den Clientcomputer. Bei der ersten Anmeldung wird das Profil komplett kopiert, bei späteren Anmeldungen wird geprüft, ob Änderungen an dem Profil vorgenommen sind. Ist dies der Fall, werden ausschließlich die Änderungen auf den Client kopiert. Die Änderungen, die der Client während seiner Sitzung am Profil vorgenommen hat, werden während des Abmeldevorgangs auf den Server geschrieben. Der ideale Speicherort für die Profile ist ein Dateiserver, von dem regelmäßig Backups erstellt werden. Legen Sie die Profile nicht auf dem Domänencontroller ab, da beim Kopieren von Profilen verstärkt Netzwerkressourcen belegt werden, wodurch die Leistung des Domänencontrollers herabgesetzt werden kann.

Sie können ein servergespeichertes Profil nicht nur für einen einzelnen Benutzer, sondern auch für eine komplette Benutzergruppe einrichten. Dies ist sinnvoll, wenn z.B. alle Mitglieder einer Gruppe mit denselben Aufgaben dieselben Einstellungen erhalten sollen. Die Benutzer erhalten nur die Einträge und Verknüpfungen, die sie für ihre Arbeit benötigen. Auch die benötigten Netzwerkressourcen, wie z.B. ein bestimmtes Laufwerk für Daten und ein bestimmter Drucker, können ihnen gleich automatisch zugeteilt werden. Dabei handelt es sich um verbindliche, servergespeicherte Benutzerprofile.

Um ein neues servergespeichertes Benutzerprofil für einen Benutzer einzurichten, führen Sie die folgenden Schritte aus:

1. Richten Sie auf dem Dateiserver einen neuen Ordner ein und geben diesen frei. Wählen Sie als Freigabenamen beispielsweise PROFILE.
2. Wählen Sie das gewünschte Benutzerobjekt, und öffnen Sie über dessen Eigenschaften die Registerkarte PROFIL. Geben Sie hier im Feld PROFILPFAD einen Pfad im folgenden Format an: \\Servername\Freigabename\Anmeldename, also etwa \\Borussia\Profile\pmustermann.

Benutzen Sie statt des Anmeldenamens die Variable *%username%*. Windows kann diese Variable durch den Namen des Benutzerkontos ersetzen. Sie sparen sich dadurch Arbeit und können die Profile leichter kopieren. Meldet sich der Benutzer zum ersten Mal an, wird automatisch der Profilordner mit seinem Anmeldenamen eingerichtet.

Um ein servergespeichertes Profil für eine Gruppe von Benutzern einzurichten, führen Sie die folgenden Schritte aus. Man spricht in diesem Fall auch von einem standardmäßigen, servergespeicherten Benutzerprofil.

1. Erstellen Sie in der Serververwaltung unter BENUTZER ein neues Benutzerkonto, das als Profilvorlage dienen soll. Vergeben Sie für diesen Benutzer einen Benutzeranmeldenamen wie z.B. VORLAGE.
2. Melden Sie sich mit diesem Vorlagennamen an und nehmen alle Einstellungen und Änderungen am Desktop vor. Melden Sie sich dann wieder als Administrator an.
3. Richten Sie auf dem Dateiserver einen neuen Ordner ein und geben diesen frei. Wählen Sie als Freigabenamen beispielsweise PROFILE. In diesem Ordner werden alle Benutzerprofile angelegt.
4. Kopieren Sie von dem Rechner, an dem Sie eben die Änderungen am Profil vorgenommen haben, aus dem Verzeichnis %System%\Dokumente und Einstellungen\Benutzername den Profilordner in die Freigabe auf dem Dateiserver. Dies geschieht auf folgende Weise:

- Öffnen Sie in der Systemsteuerung den Eintrag SYSTEM.
- Wählen Sie die Registerkarte BENUTZERPROFILE. Sie sehen hier eine Liste aller Benutzer, die sich bereits an diesem Computer angemeldet hatten (siehe Abbildung 8.21).

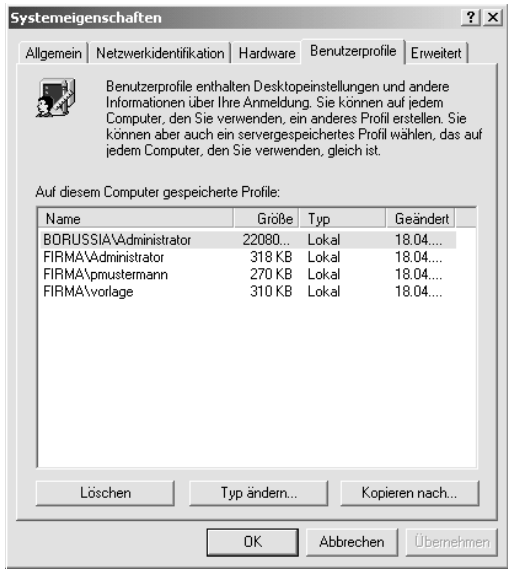


Abbildung 8.21: Die auf einem Computer vorhandenen lokalen Benutzerprofile

- Sie sehen in der Liste auch das Vorlagenprofil mit dem Namen FIRMA\VORLAGE. Markieren Sie dieses Profil und klicken auf die Schaltfläche KOPIEREN NACH.
  - Geben Sie hier den Pfad zu der im zweiten Schritt erstellten Freigabe auf dem Dateiserver an und geben einen Ordner für den Benutzer an, der das Profil erhalten soll, z.B. \\Borussia\Profile\pmustermann (siehe Abbildung 8.22). Nach dem Kopiervorgang befinden sich im Ordner PMUSTERMANN alle Ordner mit den zugehörigen Einstellungen aus %System%\Dokumente und Einstellungen\Vorlage.

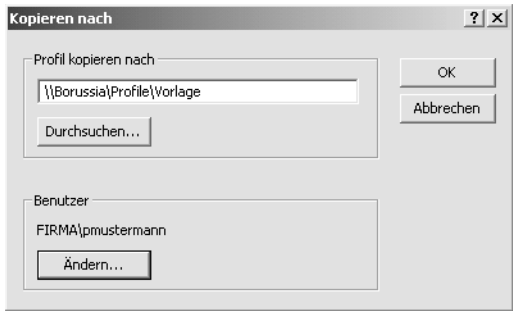


Abbildung 8.22: Das Kopieren des Benutzerprofils auf den Dateiserver

- Um nun die Benutzer hinzuzufügen, die dieses Profil benutzen sollen, klicken Sie auf die Schaltfläche ÄNDERN. Sie erhalten eine Liste aller vorhandenen Benutzer und Gruppen und können die gewünschten Objekte auswählen. Bestätigen Sie dann mit OK.

5. Legen Sie abschließend in den Kontoeigenschaften für alle Benutzer den Profilpfad entsprechend fest, in unserem Beispiel also \\Borussia\Profile\%username%.

Künftig werden alle Benutzer, die Sie eben für die Verwendung dieses Benutzerprofils ausgewählt haben, dieses Profil als Standardprofil bei der Anmeldung erhalten. Ihre Änderungen werden in ihrem jeweiligen Ordner \%username% gespeichert.

Die Vorteile servergespeicherter Profile bestehen darin, dass sich ein Benutzer von jedem beliebigen Computer im Netzwerk aus anmelden kann und dabei immer seine persönlichen Einstellungen bekommt. Ein Nachteil besteht in dem dadurch verursachten Netzwerkverkehr. Sie sollten auch keine servergespeicherten Benutzerprofile für die Benutzer einrichten, die über langsame RAS-Verbindungen wie z.B. eine Telefonleitung auf das Netzwerk zugreifen.

Einrichten eines verbindlichen Profils

Bei einem verbindlichen Profil hat der Benutzer nicht die Möglichkeit, dauerhaft Änderungen an seinem Desktop vorzunehmen. Er kann nur temporär Einstellungen ändern. Diese werden aber nicht gespeichert und stehen damit bei der nächsten Anmeldung nicht mehr zur Verfügung. Mit dieser Methode haben Sie als Administrator die volle Kontrolle über die Desktop-Einstellungen Ihrer Benutzer.

Ein verbindliches Profil ist schreibgeschützt. Um ein verbindliches Profil einzurichten, führen Sie die folgenden Schritte aus:

1. In dem Profilordner jedes Benutzers befindet sich die Datei *NTUSER.DAT*. Standardmäßig ist diese Datei versteckt. Um sie anzuzeigen, wählen Sie im Windows-Explorer unter EXTRAS/ORDNEROPTIONEN/ANSICHT die Option ALLE DATEIEN UND ORDNER ANZEIGEN. In dieser Datei werden die Desktop-Einstellungen des Benutzers gespeichert.
2. Um diese Datei mit einem Schreibschutz zu versehen, muss sie umbenannt werden. Geben Sie ihr den neuen Namen *NTUSER.MAN*. Die Dateiendung *.MAN* steht für mandatory (verbindlich). Nun kann der Benutzer seine Desktop-Einstellungen nur für die Zeit seiner Arbeit ändern. Bei der nächsten Anmeldung des Benutzers werden die Änderungen nicht übernommen

Einrichten von Basisverzeichnissen

Ein Basisverzeichnis ist ein alternativer Ordner anstatt des Ordners EIGENE DATEIEN für persönliche Dokumente. Das Basisverzeichnis ist kein Bestandteil eines Benutzerprofils. Auf ein Basisverzeichnis kann ein Benutzer mit jedem beliebigen Microsoft-Betriebssystem angefangen von MS DOS bis hin zu Windows XP zugreifen. Sie können die Basisverzeichnisse aller Benutzer zentralisiert auf einem Dateiserver anlegen, was die Verwaltung und Sicherung der Daten erleichtert, oder jedem Benutzer lokal ein Basisverzeichnis zuweisen.

Um ein Basisverzeichnis einzurichten, führen Sie die folgenden Schritte aus:

1. Wenn Sie sich für ein serverbasiertes Basisverzeichnis entscheiden, müssen Sie auf einem Dateiserver eine Freigabe erstellen, in der sämtliche Basisverzeichnisse gespeichert werden sollen. Wählen Sie für die Zugriffsberechtigungen der Freigabe nur die Gruppe BENUTZER und entfernen die Gruppe JEDER.
2. Öffnen Sie nun die Registerkarte PROFIL in den Kontoeigenschaften des Benutzers (siehe Abbildung 8.23).

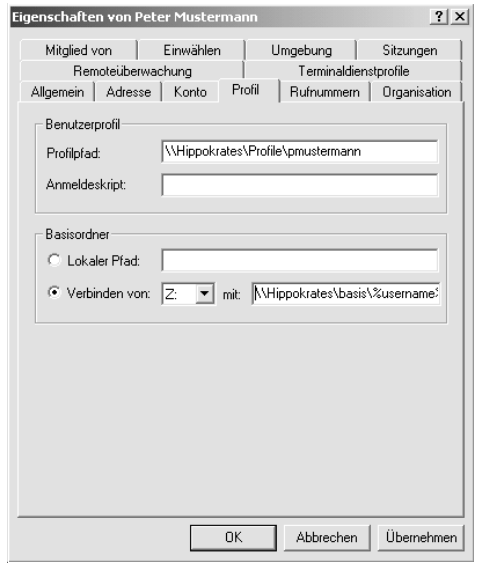


Abbildung 8.23: Das Basisverzeichnis für einen Benutzer festlegen

3. Da Sie sich für ein servergespeichertes Basisverzeichnis entschieden haben, markieren Sie die Checkbox VERBINDEN VON und wählen einen Laufwerksbuchstaben aus. Sie sollten für alle Benutzer denselben unbelegten Buchstaben, etwa Z, verwenden. Geben Sie dann den Pfad im Format \\SERVERNAME\FREIGABE\BENUTZERNAME an. Anstatt des Benutzernamens können Sie auch hier wieder die Variable *%username%* verwenden.

   Wenn Sie einen lokalen Pfad als Basisverzeichnis verwenden möchten, markieren Sie die Checkbox LOKALER PFAD und geben den Pfad ein. Ein lokaler Pfad ist nur sinnvoll, wenn sich der Benutzer nur von einem Computer aus anmeldet. Versucht er die Anmeldung von einem anderen Computer im Netzwerk aus, wird der lokale Pfad selbstverständlich nicht gefunden. Sie müssen in diesem Fall auch auf jedem lokalen Rechner separat für die Datensicherung des Basisverzeichnisses sorgen. In den meisten Fällen ist ein servergespeichertes Basisverzeichnis die bessere Lösung.

8.2.6 Umleiten des Ordners Eigene Dateien

Der Ordner Eigene Dateien stellt den standardmäßigen Speicherort für die Dokumente des Benutzers dar, in dem Applikationen wie beispielsweise Word oder Excel die Dateien speichern und öffnen. Über die Ordnerumleitung können die folgenden fünf Komponenten umgeleitet werden:

- Ordner EIGENE DATEIEN
- Ordner EIGENE BILDER
- Ordner ANWENDUNGSDATEN
- Ordner DESKTOP
- Ordner STARTMENÜ (diese Option ist nur für Terminalserver-Benutzer verfügbar)

Um die Umleitung des Ordners Eigene Dateien vorzunehmen, führen Sie die folgenden Schritte durch:

1. In der Serververwaltung öffnen Sie den Eintrag BENUTZER und klicken in der rechten Fensterhälfte auf den Link WEITERLEITUNG DES ORDNERS „EIGENE DATEIEN“ KONFIGURIEREN.
2. Im Fenster UMLEITEN VON CLIENTDOKUMENTEN (siehe Abbildung 8.24) können Sie drei verschiedene Arten der Umleitung konfigurieren.

Standardmäßig ist die erste Option aktiviert. Diese bewirkt, dass die Inhalte des Ordners Eigene Dateien an den Standardbenutzerordner des SBS-Benutzers umgeleitet werden. Markieren Sie die Option DIE ORDNER „EIGENE DATEIEN“ AN EINEN NETZWERKORDNER UMLEITEN, wählen Sie über DURCHSUCHEN einen beliebigen Netzwerkordner aus. Über die dritte Option wird die Ordnerumleitung außer Kraft gesetzt. Bestätigen Sie Ihre Auswahl mit OK.

Alternativ zu diesem Verfahren können Sie die Ordnerumleitung auch über eine Gruppenrichtlinie konfigurieren. Weitere Hinweise dazu finden Sie in Kapitel 8.6.22.

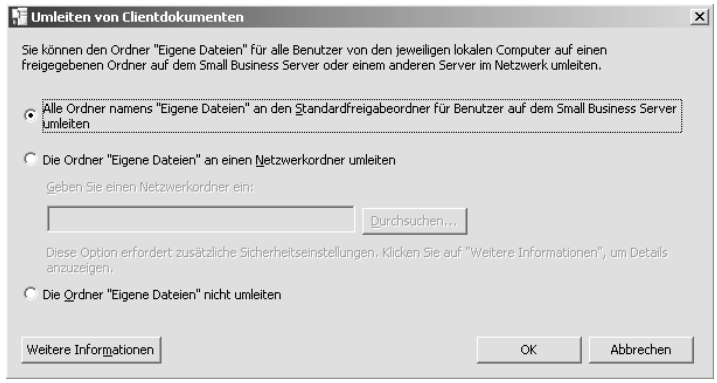


Abbildung 8.24: Die Weiterleitung des Ordners Eigene Dateien einrichten

8.2.7 Postfach- und Datenträgerkontingenteinstellungen ändern

Um den Benutzern nur eine bestimmte Menge an Speicherplatz bereitzustellen, können Sie sowohl für die Postfächer als auch für den Datenspeicher von Benutzerdaten auf dem Server Grenzen festlegen. Für die Postfächer können die Grenzwerte für jeden Benutzer separat oder für alle festgelegt werden, ein Datenträgerkontingent gilt für alle Benutzer.

Die Postfachgröße für einen bestimmten Benutzer festlegen

1. Um die Postfachgröße für einen bestimmten Benutzer zu ändern, wählen Sie dessen Eigenschaften in der Serververwaltung unter BENUTZER.
2. Wechseln Sie auf die Registerkarte EXCHANGE – ALLGEMEIN. Klicken Sie dort auf SPEICHERWERTGRENZE.
3. Im Fenster SPEICHERWERTGRENZE (siehe Abbildung 8.25) deaktivieren Sie die Checkbox STANDARDWERTE FÜR POSTFACHSPEICHER VERWENDEN.

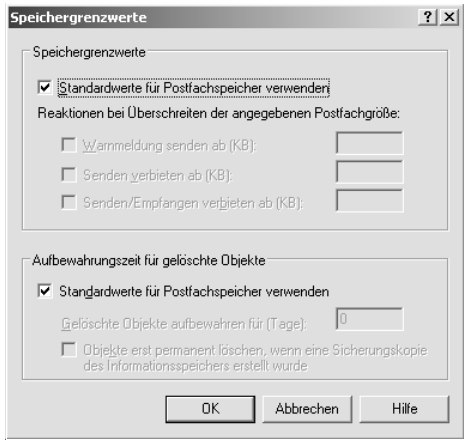


Abbildung 8.25: Die Speichergrenzwerte für die Postfachgröße eines Benutzers festlegen

4. Um die neuen Werte zu bestimmen, legen Sie die gewünschten Werte unter WARNMELDUNG SENDEN AB (KB), SENDEN VERBIETEN AB (KB) sowie SENDEN/EMPFANGEN VERBIETEN AB (KB) fest und klicken auf OK.

   Zusätzlich können Sie auf dieser Registerkarte auch festlegen, wie viele Tage unter Outlook gelöschte Objekte noch auf dem Exchange Server aufbewahrt werden sollen.

Die Postfachgröße für alle Benutzer festlegen

Sollen die Postfachbeschränkungen für alle Benutzer der SBS-Domäne gelten, so führen Sie die folgenden Schritte durch:

1. Öffnen Sie in der Serververwaltung den Eintrag ERWEITERTE VERWALTUNG und doppelklicken EXCHANGE-DOMÄNE.
2. Doppelklicken Sie dann auf SERVER, den Namen Ihres Servers und ERSTE SPEICHERGRUPPE. Wählen Sie unter POSTFACHSPEICHER den Eintrag EIGENSCHAFTEN aus dem Kontextmenü.
3. Wechseln Sie auf die Registerkarte GRENZWERTE (siehe Abbildung 8.26) und nehmen in den Feldern WARNMELDUNG SENDEN AB (KB), SENDEN VERBIETEN AB (KB), SENDEN UND EMPFANGEN VERBIETEN AB (KB), GELÖSCHTE OBJEKTE AUFBEWAHREN FÜR (TAGE) sowie GELÖSCHTE POSTFÄCHER AUFBEWAHREN FÜR (TAGE) die gewünschten Einstellungen vor.

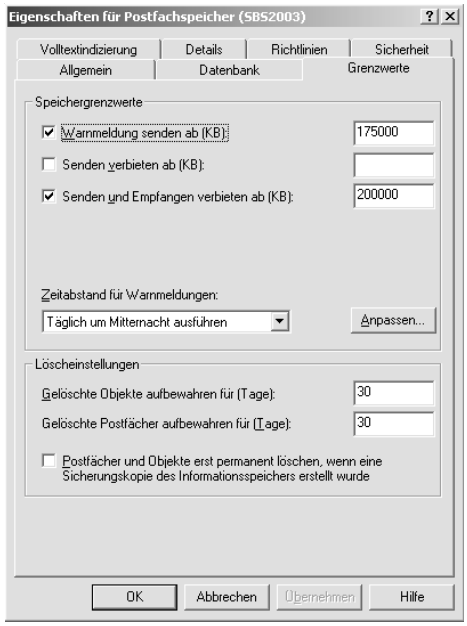


Abbildung 8.26: Die Speichergrenzwerte für die Postfachgröße aller Benutzer festlegen

   Die Standardwerte für WARNMELDUNG SENDEN AB liegt bei 175 MB und für SENDEN UND EMPFANGEN VERBIETEN AB bei 200 MB.

4. Über ANPASSEN können Sie die Intervalle oder den Zeitplan für das Senden von Warnmeldungen konfigurieren. Klicken Sie dann auf OK.

Einrichten von Datenträgerkontingenten

Mit Hilfe von Datenträgerkontingenten können Sie festlegen, wie viel Speicherplatz ein Benutzer auf einem bestimmten Laufwerk belegen darf. Damit können Sie sicherstellen, dass der vorhandene Speicherplatz gleichmäßig unter allen Benutzern aufgeteilt wird.

Datenträgerkontingente können Sie auf Laufwerken aktivieren, auf denen sich die Benutzerprofile oder Basisverzeichnisse der Benutzer befinden. Sie können eine Maximalgröße des Benutzerordners und Schwellenwerte für Warnmeldungen konfigurieren, die eine entsprechende Warnung ausgeben, wenn das Kontingent bald erschöpft ist. Ist das Limit des Kontingents erreicht, kann der Benutzer keine weiteren Daten in seinem Benutzerordner speichern. Damit können Sie sicherstellen, dass ein Benutzer nicht beliebig viele, möglicherweise nie benutzte Daten in seinem Ordner anlegen kann und damit zu viel Festplattenplatz auf dem Server verschwendet wird. Er wird so gezwungen, seine Datenbestände regelmäßig zu überprüfen. Bei Datenträgerkontingenten wird die Größe des Benutzerordners nach den Dateien berechnet, für die der jeweilige Benutzer der Besitzer ist.

Sie müssen die Datenträgerkontingente einrichten, bevor die Benutzer auf den Datenträger zugreifen. Wenn bereits vor Aktivierung der Datenträgerkontingente Benutzer Daten auf dem Datenträger speichern, greifen die Kontingenteinstellungen nicht mehr für die Benutzer, sondern ausschließlich für die Benutzer, die nach der Kontingentaktivierung das erste Mal auf den Datenträger zugreifen.

Datenträgerkontingente können Sie lediglich auf Datenträgern einrichten, die mit NTFS formatiert sind. Um für eine Netzwerkfreigabe die Kontingenteinstellung durchzusetzen, müssen Sie das Rootverzeichnis des entsprechenden Laufwerks freigeben.

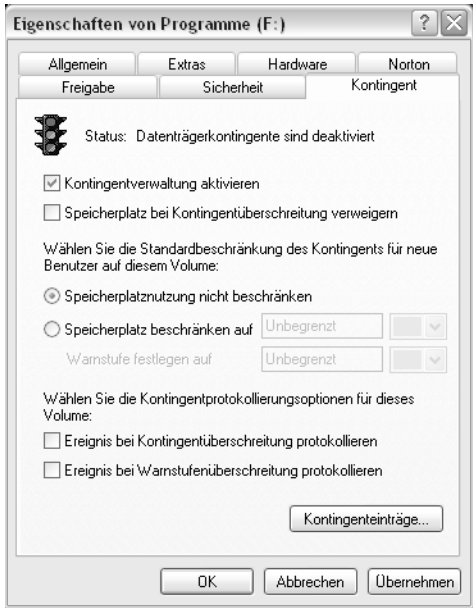


Abbildung 8.27: Die Konfiguration eines Datenträgerkontingents

Sie finden die Einstellungen zu Datenträgerkontingenten in den Eigenschaften eines Laufwerks auf der Registerkarte KONTINGENT. Um ein Datenträgerkontingent zu aktivieren, nehmen Sie auf der Registerkarte KONTINGENT die folgenden Einstellungen vor (siehe Abbildung 8.27):

1. Standardmäßig sind die Datenträgerkontingente deaktiviert. Um ein Kontingent zu aktivieren, markieren Sie die Checkbox KONTINGENTVERWALTUNG AKTIVIEREN.
2. Um die Anwendung von Kontingenten effektiv durchzusetzen, sollten Sie auch die zweite Checkbox SPEICHERPLATZ BEI KONTINGENTÜBERSCHREITUNG VERWEIGERN aktivieren. Somit ist sichergestellt, dass der Benutzer keine weiteren Daten ablegen kann, wenn die Grenze erreicht ist. Anderenfalls würde – je nach weiterer Konfiguration – nur eine Ereignisprotokollierung auftreten, aber der Benutzer könnte weiter Daten speichern.
3. Markieren Sie dann den Eintrag SPEICHERPLATZ BESCHRÄNKEN AUF und geben den gewünschten Wert ein.

Achten Sie darauf, dass Sie die korrekte Maßeinheit angegeben haben. Standardmäßig wird Kilobyte (KB) gesetzt. So könnte bei einer Konfiguration von beispielsweise 1000 KB schnell ein Problem auftreten.

4. Im Feld WARNSTUFE FESTLEGEN AUF bestimmen Sie, ab wann der Benutzer eine Meldung erhalten soll, dass sein Speicherplatz allmählich knapp wird. Sie sollten als Warnwert ca. 75% des Gesamtkontingents bestimmen.
5. Schließlich können Sie über die beiden unteren Checkboxen bestimmen, ob automatisch ein Eintrag ins Ereignisprotokoll erfolgen soll, wenn entweder das Kontingent erschöpft ist oder der Warnwert erreicht ist – oder in beiden Fällen. Standardmäßig ist die Protokollierung deaktiviert. Klicken Sie dann auf OK.

8.3 Verwalten von Benutzervorlagen

In diesem Kapitel werden Ihnen die Arbeitsschritte rund um die Benutzervorlagen vorgestellt. Dazu zählen das Hinzufügen, Importieren und Exportieren von Vorlagen. Benutzervorlagen sind lediglich unter dem SBS 2003 vorhanden. Der Windows Server 2003 kennt keine Entsprechung dazu.

Standardmäßig verfügt der SBS 2003 über die vier Benutzervorlagen *Administrator Template*, *Mobile User Template*, *Power User Template* sowie *User Template*.

- USER TEMPLATE: In dieser Vorlage ist der Zugriff auf das Internet, E-Mail, Netzwerkdrucker, Faxgeräte und freigegebene Ordner gestattet. Diese Vorlage sollte für normale Benutzerkonten angewendet werden.
- MOBILE USER TEMPLATE: In dieser Vorlage sind alle Berechtigungen des User Templates enthalten. Zusätzlich kann eine Verbindung auf den SBS 2003 per VPN-Zugriff oder DFÜ-Zugriff hergestellt werden.

- POWER USER TEMPLATE: Diese Vorlage beinhaltet alle Berechtigungen des Mobile User Templates. Weiterhin können Benutzer, die auf dieser Vorlage basieren, Benutzer, Gruppen, Drucker, Faxe und freigegebene Ordner verwalten. Sie können auch eine Remote-Verbindung mit dem Server herstellen. Eine lokale Anmeldung am Server ist jedoch nicht möglich.
- ADMINISTRATOR TEMPLATE: Diese Vorlage verfügt über einen uneingeschränkten Zugriff für die Server- und Domänenverwaltung.

Benutzervorlagen bieten den Vorteil, dass in ihnen bereits eine große Anzahl vorkonfigurierter Einstellungen, z.B. bezüglich Berechtigungen, vorgenommen ist. Beim Erstellen eines neuen Benutzers müssen Sie eine der Vorlagen auswählen. Damit erhält der Benutzer automatisch alle Einstellungen, die für diese Vorlage gültig sind.

8.3.1 Hinzufügen neuer Benutzervorlagen

Um eine neue Benutzervorlage zu erstellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie in der Serververwaltung aus dem Kontextmenü von BENUTZERVORLAGEN den Eintrag VORLAGE HINZUFÜGEN.
2. Klicken Sie zunächst auf WEITER und geben dann im Fenster VORLAGENKONTENINFORMATIONEN einen Namen und optional eine Beschreibung für die Vorlage an (siehe Abbildung 8.28).

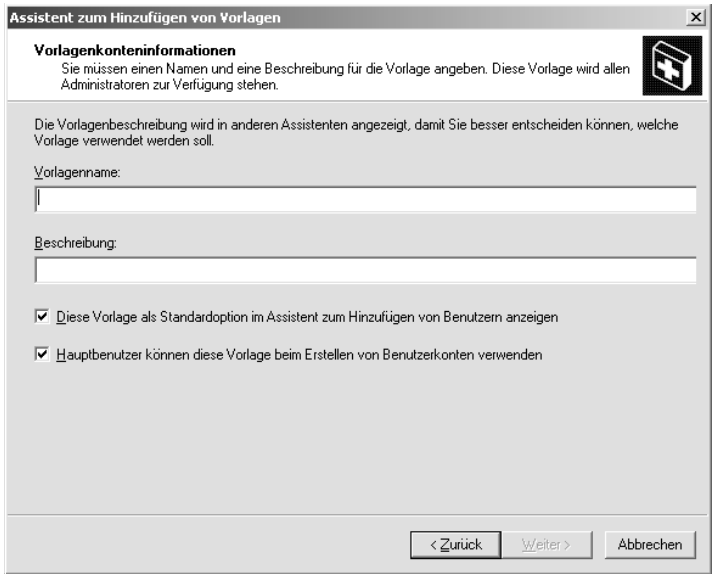


Abbildung 8.28: Das Erstellen einer neuen Benutzervorlage

Zusätzlich können Sie über die entsprechenden Checkboxen festlegen, ob die neue Vorlage beim Anlegen neuer Benutzer standardmäßig im Assistenten angezeigt werden soll und ob Hauptbenutzer diese Vorlage verwenden dürfen. Klicken Sie dann auf WEITER.

3. Als Nächstes können Sie Sicherheitsgruppen-Mitgliedschaften für die Benutzer über HINZUFÜGEN auswählen, die mit der Benutzervorlage erstellt werden. Klicken Sie dann auf WEITER.
4. Danach können Sie ebenso Verteilergruppen auswählen. Klicken Sie erneut auf WEITER.
5. Im nächsten Schritt erfolgt die Auswahl der Sitegruppen für die SharePoint Services. Eine Beschreibung der einzelnen Sitegruppen haben Sie bereits in Kapitel 5.2.2 gesehen. Markieren Sie die gewünschte(n) Gruppe(n) und klicken auf WEITER.
6. Weiterhin können Sie die Adressinformationen für die Benutzer festlegen, die mit der Vorlage erstellt werden. Klicken Sie dann auf WEITER.
7. Im nächsten Schritt können Sie eine Speicherplatzbegrenzung für den Benutzer festlegen. Diese Kontingenteinstellung gilt für das Laufwerk auf dem SBS 2003, das den Benutzerordner beherbergt. Standardmäßig liegt die Größenbeschränkung bei 1024 MB und der Warnwert bei 900 MB. Möchten Sie kein Kontingent festlegen, markieren Sie stattdessen die Checkbox KEINE SPEICHERPLATZBEGRENZUNG. Klicken Sie dann auf WEITER. Danach können Sie den Assistenten fertig stellen.

8.3.2 Import und Export von Vorlagen

Sie können sowohl die vordefinierten als auch selbst erstellte Vorlagen über die Import- und Exportfunktion zwischen mehreren SBS 2003-Servern austauschen.

Export

1. Um den Export zu starten, wählen Sie aus dem Kontextmenü der Vorlage VORLAGEN EXPORTIEREN.
2. Klicken Sie im Assistenten auf WEITER. Im Fenster VORLAGENAUSWAHL sehen Sie links alle vorhandenen Vorlagen. Markieren Sie die gewünschten und klicken auf HINZUFÜGEN. Klicken Sie dann auf WEITER.
3. Geben Sie dann den Pfad und Dateinamen an, wo die Vorlagen gespeichert werden sollen. Die Vorlagen werden als XML-Datei exportiert. Klicken Sie auf WEITER und beenden den Assistenten.

Import

1. Zum Import wählen Sie den Kontextmenüeintrag VORLAGEN IMPORTIEREN.
2. Klicken Sie im Assistenten auf WEITER. Im Fenster IMPORTPFAD wählen Sie die zu importierende XML-Datei aus. Klicken Sie dann auf WEITER.
3. Im Fenster VORLAGENAUSWAHL wählen Sie die zu importierende(n) Vorlage(n) aus. Diese Auswahl ist sinnvoll, wenn in der XML-Datei mehrere Vorlagen gespeichert sind, aber nicht alle importiert werden sollen. Klicken Sie dann auf WEITER und beenden den Assistenten.

8.4 Verwalten von Sicherheitsgruppen und Verteilergruppen

In diesem Kapitel lernen Sie nun grundlegende Dinge zum Thema Benutzergruppen. Um sich die Verwaltung der Benutzer zu vereinfachen, können Sie Benutzer, die in einem Unternehmen ähnliche Aufgaben ausführen, zu Benutzergruppen zusammenfassen.

8.4.1 Grundlegendes zu Gruppen

Eine Benutzergruppe ist zunächst einmal nichts anderes als eine Zusammenfassung von mehreren Benutzerkonten. Sie vereinfachen die Benutzerverwaltung durch die Einrichtung von Gruppen enorm, da Sie nun nicht mehr jedem einzelnen Benutzer Zugriffsrechte auf Ressourcen zuweisen, sondern in nur einem Arbeitsschritt einer Gruppe und damit allen darin enthaltenen Benutzern die entsprechenden Rechte geben oder verweigern.

Es ist möglich, dass ein Benutzer Mitglied mehrerer Gruppen ist oder eine Gruppe Mitglied einer anderen Gruppe. Zu einer Gruppe können Sie Benutzerkonten, Computerkonten, andere Gruppen und Kontakte hinzufügen.

8.4.2 Gruppentypen und Gruppenbereiche

Die Gruppen werden in zwei verschiedene Typen und drei Gruppenbereiche unterschieden. Zunächst einmal gibt es die beiden Gruppentypen *Sicherheitsgruppe* und *Verteilergruppe*. Die wichtigere von beiden ist die Sicherheitsgruppe. In einer Verteilergruppe werden Benutzer ausschließlich für Prozesse zusammengefasst, die nichts mit Zugriffsrechten und Sicherheit zu tun haben. Ein klassisches Beispiel ist eine Verteilerliste zum Massenversand von E-Mails. Nur die Sicherheitsgruppen dienen der Zusammenfassung von Benutzern für die Vereinfachung der Vergabe von Zugriffsrechten. Sie besitzen die Grundfunktionalität der Verteilergruppen, nämlich das Zusammenfassen von mehreren Benutzern für eine bestimmte Funktion, sowie zusätzlich die Möglichkeit, den Zugriff auf Ressourcen zu steuern. In unserem Kontext sind ausschließlich die Sicherheitsgruppen relevant. Wenn also künftig von Gruppen die Rede ist, sind damit nur die Sicherheitsgruppen gemeint.

In der Serververwaltung finden Sie für beide Gruppentypen jeweils einen Eintrag, um diese zu verwalten.

Die Sicherheitsgruppen werden in drei Gruppenbereiche unterteilt. Dies sind globale Gruppen, domänenübergreifende lokale Gruppen sowie universelle Gruppen. Beim Erstellen einer Gruppe müssen Sie einen dieser drei Bereich auswählen. Diese Gruppen können Sie für eine Domäne einrichten. Unabhängig von diesen drei Gruppenbereichen gibt es die lokalen Gruppen, die Sie auf Windows 2000/XP Professional-Computern sowie Mitgliedservern in der Domäne einrichten. Diese Gruppen sind lediglich auf dem lokalen Computer verfügbar und dürfen nicht mit domänenübergreifenden lokalen Gruppen verwechselt werden.

Die drei Gruppenbereiche haben die folgenden Eigenschaften bezüglich der Mitgliedschaft ihrer Gruppenmitglieder und des Zugriffs auf die Netzwerkressourcen:

Gruppenbereich	Mitgliedschaft	Ressourcenzugriff
Global	Mitglieder der lokalen Domäne	Auf Ressourcen beliebiger Domänen
Domänenübergreifend lokal	Mitglieder aus einer beliebigen Domäne	Auf Ressourcen der lokalen Domäne
Universell. Universelle sind nicht im gemischten Betriebsmodus des Active Directory verfügbar.	Mitglieder aus einer beliebigen Domäne	Auf Ressourcen beliebiger Domänen

Tabelle 8.7: Eigenschaften der drei Gruppenbereiche

Sie sehen also, dass die globalen Gruppen hinsichtlich der Gruppenmitgliedschaft eingeschränkt sind, während die domänenübergreifenden lokalen Gruppen hinsichtlich des Ressourcenzugriffs beschränkt sind. Die Nichteinschränkung gilt jeweils für die andere Komponente. Nur bei einer universellen Gruppe gibt es keinerlei Einschränkungen.

8.4.3 Standardmäßig vorhandene Gruppen

Es gibt mehrere standardmäßig vorhandene Gruppen unter SBS 2003. Dabei wird wieder unterschieden in Domänencontroller und Windows-Clients bzw. Mitgliedserver. Domänencontroller können drei Arten von Gruppen beinhalten, nämlich integrierte, vordefinierte und besondere Gruppen. Auf allen übrigen Computern können Sie lediglich vordefinierte lokale Gruppen einrichten. Die folgenden Tabellen geben Ihnen eine Übersicht über die standardmäßigen Mitglieder dieser Gruppen und deren Einsatzmöglichkeiten und Berechtigungen.

Integrierte Gruppen

Integrierte Gruppen gehören zu dem Gruppenbereich domänenübergreifend lokal. Sie befinden sich im Container BUILTIN der SBS-Domäne. Diesen Gruppen sind bereits feste Berechtigungen zugeteilt, die sie für die Arbeit im Active Directory benötigen. Es gibt insgesamt 16 dieser Gruppen.

Integrierte Gruppe	Beschreibung	Standardmäßige Mitglieder
Administratoren	Konto, um alle Verwaltungsaufgaben in der Domäne durchzuführen	Domänen-Admins und Organisations-Admins
Benutzer	Benutzer können die Aufgaben durchführen, für die ihnen die Rechte erteilt sind.	Domänenbenutzer und authentifizierte Benutzer
Druck-Operatoren	Konto zum Einrichten und Verwalten von Netzwerkdruckern auf Domänencontrollern	

Integrierte Gruppe	Beschreibung	Standardmäßige Mitglieder
Gäste	Mitglieder können nur die ihnen erlaubten Aufgaben ausführen	Gast, IWAM_Computername, IUSR_Computername und TsInternetUser
Konten-Operatoren	Konto zum Einrichten und Verwalten von Benutzerkonten und Gruppen	
Leistungsprotokollbenutzer	Die Benutzer verfügen über Remote-Zugriff, um die Planung der Leistungsindikator-Protokollierung durchzuführen.	Netzwerkdienst
Netzwerk-Konfigurationsoperatoren	Diese Benutzer verfügen für einige Netzwerkkonfigurationen über administrative Berechtigungen.	
Prä-Windows 2000 kompatibler Zugriff	Zur Gewährleistung der Abwärtskompatibilität wird allen Benutzern und Gruppen Lesezugriff gewährt	NT-Systemgruppe Jeder
Remote-Desktop-Benutzer	Diese Benutzer dürfen sich remote anmelden.	Remote-Operatoren
Replikations-Operator	Konto zur Unterstützung der Active Directory-Replikation	
Server-Operatoren	Konto zum Sichern und Wiederherstellen sowie gemeinsamen Zugriff auf Ressourcen des Servers	
Sicherungs-Operatoren	Konto zum Sichern und Wiederherstellen aller Domänencontroller über Windows-Backup.	
Systemmonitorbenutzer	Die Mitglieder verfügen über Remote-Uugriff für die Überwachung des Computers.	
Terminalserver-Lizenzserver	Diese Gruppe ist nur vorhanden, wenn ein Terminalserver konfiguriert ist.	
Windows-Authentifizierungsgruppe	Die Mitglieder haben Zugriff auf das (berechnete) Attribut tokenGroupsGlobalAndUniversal.	Domänencontroller der Organisation

Tabelle 8.8: Die 16 integrierten Gruppen des SBS 2003

Globale Gruppen

Weiterhin gibt es vordefinierte Gruppen, die dem Gruppenbereich global angehören. Diese Gruppen befinden sich im Container USERS der SBS-Domäne. Zu diesen Gruppen können neue Mitglieder hinzugefügt werden, und diese globalen Gruppen können zu

domänenübergreifenden lokalen Gruppen hinzugefügt werden. Es gibt die folgenden integrierten Gruppen:

Vordefinierte Gruppe	Beschreibung	Standardmäßige Mitglieder
Domänen-Admins	Sie können auf jedem Computer in der Domäne administrative Aufgabe ausführen.	Administratoren
Domänen-Benutzer	Alle Benutzer werden dieser Gruppe hinzugefügt	Administrator, Krbtgt, IWAM_Computername, IUSR_Computername und TsInternetUser
Domänen-Gäste	Alle Gäste werden automatisch dieser Gruppe hinzugefügt	Gast
Organisations-Admins	Konto für Verwaltungsaufgaben im gesamten Netzwerk	Administrator

Tabelle 8.9: Die vordefinierten Gruppen des SBS 2003

Sofern Sie weitere Dienste installiert haben, sind weitere vordefinierte Gruppen vorhanden, so beispielsweise DHCP-Administratoren und -Benutzer, DNS-Admins, RAS- und IAS-Server, Schema-Admins usw.

Gruppen besonderer Identität

Die Gruppen mit besonderer Identität befinden sich auf jedem Windows-Computer mit Windows 2000 und höher, unabhängig davon, ob es sich um einen Domänencontroller handelt oder nicht. Zu diesen Gruppen können Sie jedoch weder Mitglieder hinzufügen noch diese Gruppen Mitglied anderer Gruppen werden lassen. Es handelt sich um Zweckgruppen, die Benutzer temporär enthalten. Die Gruppen werden nicht durch die Person definiert, die auf einen Computer oder eine Ressource zugreift, sondern dadurch, wie der Zugriff erfolgt. Deshalb finden Sie diese Gruppen auch in keinem Container. Die folgende Tabelle zeigt Ihnen die Gruppen besonderer Identität.

Besondere Gruppe	Beschreibung
Anonyme Anmeldung	Umfasst alle Benutzer, die nicht vom SBS 2003 authentifiziert werden konnten
Authentifizierte Benutzer	Fasst alle Benutzer zusammen, die über ein gültiges Domänenkonto verfügen. Sie sollten statt der Gruppe lieber jedem in dieser Gruppe Zugriffsrechte erteilen.
Ersteller-Besitzer	Das Benutzerkonto des Benutzers, der die Ressource ursprünglich erstellt oder später in Besitz genommen hat.
Interaktiv	Das Benutzerkonto des Benutzers, der sich an einem Rechner physisch anmeldet.

Besondere Gruppe	Beschreibung
Jeder	Umfasst alle Benutzer, die auf den Computer zugreifen. Darin ist auch das Gastkonto enthalten. Standardmäßig hat diese Gruppe Vollzugriff auf alle Ressourcen.
Netzwerk	Umfasst alle Benutzer, die aktuell auf eine beliebige freigegebene Ressource zugreifen.
Wählverbindung	Alle aktuellen Benutzer einer DFÜ-Verbindung

Tabelle 8.10: Die Gruppen mit besonderer Identität des SBS 2003

Auf jedem Computer ab Windows 2000, der kein Domänencontroller ist, gibt es vordefinierte lokale Gruppen. Die Mitglieder dieser Gruppen können ihre Aufgaben nur auf dem lokalen System ausführen. Diese Gruppenkonten sind nicht in der Domäne gültig. Die folgenden Gruppen sind vordefinierte lokale Gruppen: Administratoren, Benutzer, Gäste, Hauptbenutzer, Replikations-Operator und Sicherungs-Operatoren. Bis auf die Gruppe Hauptbenutzer gelten für diese Konten dieselben Beschreibungen der Tabelle 8.8. Lediglich Hauptbenutzer sind nur in lokalen Gruppen vorhanden. Sie können neue lokale Konten erstellen und ändern sowie die Freigabe von Ressourcen vornehmen.

8.4.4 Einrichten und Bearbeiten von Gruppen und Gruppeneigenschaften

In diesem Kapitel wird beschrieben, wie Sie eine neue Gruppe auf dem SBS 2003 erstellen und deren Eigenschaften konfigurieren.

Erstellen einer neuen Gruppe

Um eine neue Gruppe zu erstellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie in der Serververwaltung aus dem Kontextmenü von SICHERHEITSGRUPPEN den Eintrag SICHERHEITSGRUPPE HINZUFÜGEN.
2. Im Assistenten klicken Sie auf WEITER und geben dann unter SICHERHEITSGRUPPENNAME den Namen und optional eine Beschreibung für die Gruppe an. Klicken Sie dann auf WEITER.
3. Im Fenster GRUPPENMITGLIEDSCHAFT sehen Sie links alle auf dem SBS 2003 vorhandenen Benutzer, Gruppen und Vorlagen. Markieren Sie die gewünschten Einträge und klicken auf HINZUFÜGEN. Fahren Sie dann mit WEITER fort. Um den Assistenten zu beenden, klicken Sie auf FERTIG STELLEN.

Lokale Gruppen erstellen Sie auf Clientcomputern und Mitgliedservern über STARTMENÜ/PROGRAMME/VERWALTUNG/COMPUTERVERWALTUNG/LOKALE BENUTZER UND GRUPPEN.

Mitgliedschaftslisten bearbeiten

Um zu der neu erstellten Gruppe Mitglieder hinzuzufügen, wählen Sie aus dem Kontextmenü der Gruppe EIGENSCHAFTEN und dort die Registerkarte MITGLIEDER. Klicken Sie auf die Schaltfläche HINZUFÜGEN. Sie können nun weitere Mitglieder für diese

Gruppe auswählen. Umgekehrt können Sie auch die Gruppe als Mitglied anderer Gruppen hinzufügen, indem Sie die Registerkarte MITGLIED VON wählen und dort über HINZUFÜGEN die gewünschte Gruppe auswählen.

Löschen von Gruppen

Um eine Gruppe wieder zu löschen, wählen Sie den Eintrag SICHERHEITSGRUPPE ENTFERNEN aus deren Kontextmenü. Eine Gruppe kann nur gelöscht werden, wenn keines der Mitglieder sie als primäre Gruppe definiert hat. Durch das Löschen der Gruppe löschen Sie nicht die Benutzerkonten der Mitglieder. Da beim Löschen der Gruppe jedoch die SID gelöscht wird, werden auch alle mit der Gruppe verknüpften Berechtigungen entfernt. Das Neuerstellen einer gleichnamigen Gruppe übernimmt nicht die Einstellungen der alten Gruppe. Eine Gruppe kann erst gelöscht werden, wenn keiner der Mitglieder diese Gruppe mehr als primäre Gruppe definiert hat.

Ändern von Gruppeneigenschaften

Auch die Eigenschaften des Gruppenbereichs und Gruppentyps können Sie ändern. Sobald Sie z.B. den Betriebsmodus in einheitlich umsetzen, können Sie auch die Gruppen in universelle Gruppen umwandeln. Eine globale Gruppe kann jedoch nicht in eine universelle Gruppe umgewandelt werden, wenn sie noch Mitglied einer anderen globalen Gruppe ist. Auch eine domänenübergreifende Gruppe kann nicht in eine universelle Gruppe umgewandelt werden, solange sie noch Mitglied einer anderen domänenübergreifenden Gruppe ist. Bei universellen Gruppen kann nicht mehr der Gruppentyp geändert werden. Wird Active Directory im gemischten Modus ausgeführt, ist die Option universelle Gruppe nicht anwählbar. Sie können auch keine globale Gruppe in eine domänenübergreifende Gruppe und umgekehrt umwandeln.

Um eine der Eigenschaften zu ändern, öffnen Sie die Eigenschaften der Gruppe. Nehmen Sie auf der Registerkarte ALLGEMEIN die gewünschten Änderungen vor (siehe Abbildung 8.29).

Abbildung 8.29: Das Ändern der Gruppeneigenschaften

8.5 Verwaltung von Clientcomputern und Servercomputern

Für die Verwaltung der Clients und Server stehen Ihnen in der Serververwaltung die beiden Einträge CLIENTCOMPUTER und SERVERCOMPUTER zur Verfügung.

In der Active Directory-Struktur werden die neuen Clientcomputer im Container MYBUSINESS/SBSCOMPUTERS angelegt, die Server im Container MYBUSINESS/SBSSERVERS.

Im Gegensatz zum Windows Server 2003 ist das Erstellen von Computern unter dem SBS 2003 eng an das Erstellen von Benutzern und auch an das Zuweisen von Applikationen geknüpft.

8.5.1 Clientcomputer

Um einen neuen Clientcomputer zu erstellen , führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü von Clientcomputer den Eintrag CLIENTCOMPUTER EINRICHTEN.
2. Geben Sie dort einen Namen für den Computer ein und klicken auf HINZUFÜGEN. Auf diese Art können Sie auch mehrere neue Computer erstellen. Klicken Sie dann auf WEITER.
3. Danach können Sie aus den Clientanwendungen des SBS 2003 auswählen, welche auf dem Computer installiert werden sollen (siehe Abbildung 8.30). Klicken Sie hier auf WEITER.

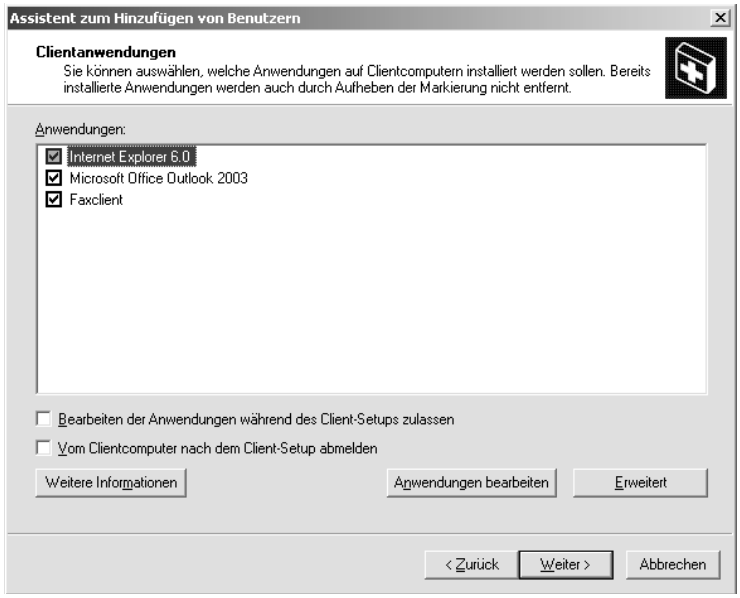


Abbildung 8.30: Hinzufügen von Client-Applikationen zum Computer

Die genaue Durchführung dieser Option wurde bereits in Kapitel 2.7.7 im Zuge der Aufgabenliste nach der Installation beschrieben. Weitere Hinweise finden Sie dort.

Hinzufügen von Anwendungen

Nachdem Sie einen oder mehrere Clientcomputer erstellt haben, können Sie auch nachträglich noch Anwendungen zu diesem Computer hinzufügen. Verwenden Sie dazu den Link CLIENTCOMPUTERN ANWENDUNGEN HINZUFÜGEN.

Sie wählen zunächst alle Clientcomputer über HINZUFÜGEN aus. Danach erhalten Sie wiederum das Fenster CLIENTANWENDUNGEN (siehe Abbildung 8.30).

Einstellungen des Clientcomputers

Um einen schnellen Überblick über die Einstellungen der einzelnen Clientcomputer zu erhalten, klicken Sie auf den Link COMPUTEREINSTELLUNGEN ANZEIGEN. Sie finden dort alle verfügbaren Clientcomputer aufgelistet. Wenn Sie einen der Computer doppelklicken, können Sie dessen Konfigurationseinstellungen in den Bereichen ZUGEWIESENE ANWENDUNGEN, CLIENT-SETUP-EINSTELLUNGEN sowie CLIENT-SETUP-KONFIGURATIONSOPTIONEN (siehe Abbildung 8.31) betrachten.

Abbildung 8.31: Die verschiedenen Einstellungen eines Clientcomputers anzeigen

Weitere Verwaltungsoptionen

Sobald Sie einen der verfügbaren Clientcomputer angeklickt haben, erhalten Sie einige weitere Links zur Verwaltung. Sie haben außer den eben beschriebenen Optionen noch die Möglichkeit, die Ereignisprotokolle des Rechners anzeigen zu lassen, die Computerverwaltung des Clients aufzurufen, eine Verbindung zu diesem Computer über die Terminaldienste herzustellen und Remote-Unterstützung anzubieten sowie den Computer aus dem Netzwerk zu entfernen. Dieselben Funktionen können Sie auch über das Kontextmenü des Computers aufrufen.

8.5.2 Servercomputer

Unter dem Link SERVERCOMPUTER haben Sie lediglich die Möglichkeit, einen Servercomputer einzurichten.

1. Zunächst geben Sie den Namen für den Server ein und klicken dann auf WEITER.
2. Als Nächstes legen Sie fest, ob der neue Server eine feste IP-Adresse verwenden oder ob diese per DHCP zugewiesen werden soll. Klicken Sie dann auf WEITER. Danach können Sie den Assistenten fertig stellen.

Sobald Sie den Server doppelklicken, erhalten Sie wie auch beim Clientcomputer einige weitere Links. Sie können die Computerverwaltung aufrufen, eine Verbindung über die Terminaldienste herstellen, die Ereignisprotokolle und Dienste des Servers betrachten und diesen aus dem Netzwerk entfernen. Auch hier können Sie dieselben Funktionen auch über das Kontextmenü aufrufen.

8.6 Gruppenrichtlinienverwaltung

In diesem Kapitel lernen Sie die Gruppenrichtlinien kennen. Sie sind unter Active Directory das zentrale Werkzeug zur Steuerung der Konfiguration von Benutzern und Computern. Gruppenrichtlinien können auf den Ebenen von Standorten, Domänen und Organisationseinheiten angewendet werden. Ein Gruppenrichtlinienobjekt gibt für einen Benutzer eine Ansammlung von Regeln des Unternehmens in Bezug auf verfügbare Ressourcen, Zugriffsrechte und Konfiguration der Ressourcen wieder. Über eine Gruppenrichtlinie werden die Desktop-Einstellungen eines Benutzers konfiguriert. Sie können ihm über diese Richtlinie beispielsweise Software zuweisen oder bestimmen, welche Objekte er im Startmenü sehen darf und welche nicht. Unter Windows NT stand Ihnen – wenn auch nicht in diesem Umfang – dafür die Systemrichtlinie zur Verfügung. Gruppenrichtlinien sind ein Bestandteil der IntelliMirror-Technologie. IntelliMirror ist der Oberbegriff für die Steuerung der Client-Desktops unter Windows 2000/XP/2003. Für jeden Client bestimmen Sie Richtlinien, die auf seiner Funktion, seinem Standort und seinen Gruppenmitgliedschaften basieren. Der Benutzer erhält überall seine in den Gruppenrichtlinien definierten Einstellungen, egal an welchem Computer er sich anmeldet. IntelliMirror umfasst die folgenden Funktionen: Verwaltung von Benutzerdaten und -einstellungen sowie Zuweisung, Installation und Konfiguration von Software.

Unter Windows Server 2003 wurde die Administration der Gruppenrichtlinien durch die Bereitstellung der GPMC (Group Policy Management Console) entschieden vereinfacht.

In diesem Kapitel wird bei sämtlichen Konfigurationsschritten davon ausgegangen, dass die GPMC installiert ist. Ist dies nicht der Fall, weichen die Optionen teilweise entschieden voneinander ab.

8.6.1 Die Windows NT-Systemrichtlinie und Windows 2003-Gruppenrichtlinie

Unter Windows NT konnten über den Systemrichtlinien-Editor in der Registry gespeicherte Benutzer- und Computerkonfigurationen festgelegt werden. Sie konnten eine Systemrichtlinie definieren, über welche die Arbeitsumgebung eines Benutzers gesteuert werden konnte. Diese Konfigurationseinstellungen konnten dann auf seinen Computer angewendet werden.

In der NT-Systemrichtlinie gab es insgesamt 72 Optionen zur Richtlinieneinstellung. Der Windows Server 2003 und somit auch der SBS 2003 verfügen über mehr als 700 Gruppenrichtlinien. Diese ergeben sich durch erweiterte Features des Betriebssystems wie den Remote-Desktop, die Software Restriction Rules oder beziehen sich auf den Windows Media Player bzw. das Startmenü. Über die NT-Systemrichtlinie konnte nur eine Richtlinie von einem Benutzer oder Computer in der Domäne verarbeitet werden, während unter Windows 2003 mehrere Gruppenrichtlinienobjekte in verschiedenen Leveln der Active Directory-Hierarchie mit Containern verbunden werden können.

Insgesamt umfasst die Windows 2003-Gruppenrichtlinie vier administrative Vorlagen. Administrative Vorlagen sind Textdateien, welche die entsprechenden Werte für die geänderten Registry-Schlüssel oder auch die Standardwerte enthalten. Für jeden Wert ist auch die entsprechende Stelle der Registry angegeben, an der die Werte stehen. Die beiden Dateien system.adm und inetres.adm werden automatisch in die Gruppenrichtlinie installiert. Sie schreiben die Einstellungen in vier reservierte Bereiche der Registry. Dabei handelt es sich um folgende Schlüssel:

```
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
```

Dabei handelt es sich um die Dateien *Conf.adm* (Einstellungen für NetMeeting), *Inetres.adm* (Internet Explorer), *System.adm* (Systemeinstellungen) und *Wmplayer.adm* (Media Player).

Sobald eine Gruppenrichtlinie geändert wird, werden die entsprechenden Bereiche in der Registry erst gelöscht und dann komplett neu geschrieben. Änderungen an diesen Bereichen sind nur mit Administratorrechten durchführbar. Diese administrativen Vorlagen des lokalen Gruppenrichtlinienobjekts befinden sich im Verzeichnis %SYSTEMROOT%\SYSTEM32\GROUPPOLICY. Sie können manuell editiert werden. Auch das Erstellen eigener adm-Dateien ist möglich.

Die drei anderen administrativen Vorlagen können optional in die Gruppenrichtlinien installiert werden. Sie sollten aber besser nur im Systemrichtlinien-Editor (poledit.exe) zur Verwaltung älterer Windows-Versionen herangezogen werden. Benutzen Sie diese drei Vorlagen nicht zur Verwaltung von 2000- oder XP-Clients, da die Einstellungen der Systemrichtlinie dauerhaft in der Registry wirksam bleiben können. Es handelt sich um die Dateien *winnt.adm*, *windows.adm* sowie *common.adm*. Über die *winnt.adm* werden Optionen für die Benutzeroberfläche von Windows NT, über die *windows.adm* Optionen für Windows 9x und über *common.adm* gemeinsame Benutzeroberflächen-Optionen für Windows NT und 9x gesteuert.

8.6.2 Was bedeuten GPO, GPC und GPT?

Zunächst einmal sollen die drei geheimnisvollen Abkürzungen aufgeschlüsselt werden, die Ihnen im Laufe dieses Kapitels immer wieder begegnen werden. GPO bedeutet Gruppenrichtlinienobjekt (Group Policy Object), ein GPC ist ein Gruppenrichtliniencontainer (Group Policy Container), und GPT heißt Gruppenrichtlinienvorlage (Group Policy Template). Nachdem Sie nun die Abkürzungen kennen gelernt haben, sollen diese Begriffe mit Leben gefüllt werden.

Ein GPO besteht aus einer Reihe von einzelnen Gruppenrichtlinien, die Sie einem Benutzer oder Computer zuweisen können. Alle Einstellungen und Daten einer Gruppenrichtlinie werden in einem GPO gespeichert. Sobald Sie ein GPO für einen Benutzer oder Computer implementiert haben, enthält dieses ein GPC und ein GPT. Im GPC befinden sich die GPO-Informationen wie Version oder Status (aktiviert oder deaktiviert). Das GPC enthält Untercontainer für die Richtlinien für Computer und Benutzer. Im GPC werden alle Eigenschaften der Richtlinie gespeichert, die nicht häufigen Änderungen unterworfen sind, also quasi die Beschreibung der Richtlinie. Im GPT werden die Einstellungen für die Richtlinie gespeichert. Dazu zählen z.B. Skripte oder Sicherheitseinstellungen. Diese Daten können sich häufiger ändern. Die Ordnerstruktur des GPT wird beim Erstellen des GPO angelegt. Sie finden die GPT-Daten für domänenbasierte Gruppenrichtlinienobjekte im Verzeichnis %SYSTEMROOT%\SYSVOL\[DOMÄNENNAME]\POLICIES\[GUID DES JEWEILIGEN GPO]. Zusätzlich sind im Verzeichnis \USER\SCRIPTS\ bzw. \MACHINE\SCRIPTS\ von SYSVOL die Anmelde- und Abmeldeskripte für das GPO gespeichert.

Auf jedem Windows 2000/XP-Computer befindet sich auch ein lokales GPO – unabhängig davon, ob der Computer Mitglied einer Domäne ist oder nicht. Dieses finden Sie im Verzeichnis %SYSTEMROOT%\SYSTEM32\GROUPPOLICY. Einige der Funktionen wie z.B. Softwareverteilung oder Ordnerumleitung sind in den lokalen GPOs im Gegensatz zu domänenbasierten GPOs nicht verfügbar.

8.6.3 Verarbeiten und Vererben von Gruppenrichtlinien

Auf Domänenebene können GPOs auf Standorte, Domänen und Organisationseinheiten angewendet werden. Wenn sich ein Computer nicht in einer Domäne befindet, ist für ihn nur das lokale GPO gültig. Befindet er sich jedoch in einer Domäne, können die Einstellungen des lokalen GPOs durch die der Domäne überschrieben werden. Gruppenrichtlinien für Computer, die Mitglieder in Active Directory sind, werden in dieser Gültigkeitsreihenfolge abgearbeitet:

1. Lokales GPO
2. GPO des Standorts
3. GPO der Domäne
4. GPO der Organisationseinheit

Als Erstes werden also die Einstellungen des lokalen GPO geprüft. Dann werden die Einstellungen des GPOs für den Standort abgearbeitet. Ist eine Richtlinie nur auf Standortebene definiert, wird sie zu den bestehenden Richtlinieneinstellungen des lokalen GPOs addiert. Ist auf der Standortebene eine vom lokalen GPO abweichende Einstellung

getroffen, so überschreibt das GPO des Standorts das lokale GPO. In dieser Weise werden alle GPOs bis zur Ebene der Organisationseinheit abgearbeitet. Wenn Sie eine Hierarchie von OUs und Unter-OUs eingerichtet haben, werden die OU-GPOs bis zu der untersten OU abgearbeitet. Man spricht hierbei auch von der LSDOU-Reihenfolge (Lokal – Standort – Domäne – Organisationseinheit).

Ein einzelnes GPO kann mit mehreren Containern wie Standorten, Domänen und Organisationseinheiten verbunden sein. Andererseits kann aber auch einer dieser Container mehrere GPOs beinhalten. Selbstverständlich kann auch ein GPO in nur einem Container angewendet werden.

In Abbildung 8.32 sehen Sie, dass der Container Domäne mit zwei verschiedenen GPOs, nämlich GPO 1 und 2, verknüpft ist, während andererseits dasselbe GPO, nämlich GPO 3, mit zwei verschiedenen Containern verknüpft ist, nämlich Organisationseinheit 1 und 2. Der einzelne Container-Standort ist mit nur einem GPO, nämlich GPO 4, verbunden.

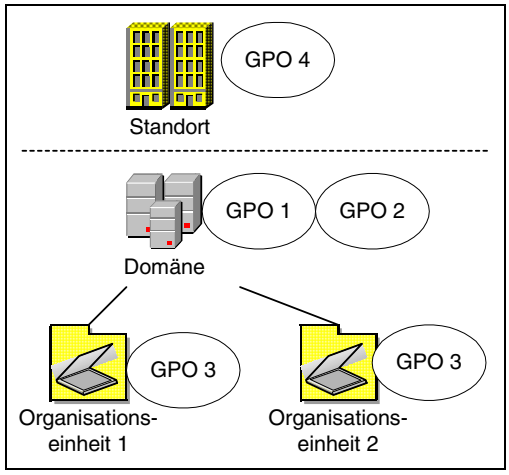


Abbildung 8.32: Die Verknüpfungsmöglichkeiten von GPOs

Das eben beschriebene Modell geht davon aus, dass pro Hierarchieebene jeweils nur ein Container vorhanden ist, also beispielsweise nur eine Organisationseinheit ohne weitere OU-Untercontainer. Befinden sich aber in einem Container weitere Container (eine OU ist durch weitere OUs strukturiert), so gilt auch für Gruppenrichtlinien der standardmäßige Weg der Vererbung: Der übergeordnete Container vererbt die konfigurierten Richtlinien an alle Benutzer und Computer der untergeordneten Container. Dies gilt jedoch nur für Richtlinien, die entweder aktiviert oder deaktiviert sind. Die nicht konfigurierten Richtlinien werden nicht weiter vererbt.

Haben Sie jedoch in einem untergeordneten Container einige spezielle Richtlinien konfiguriert, so werden diese vorrangig vor den vom übergeordneten Container geerbten behandelt. Sind im über- und untergeordneten Ordner mehrere Richtlinien konfiguriert, die sich nicht widersprechen, so werden diese addiert. Widersprechen sich jedoch die Einträge in der Richtlinie des über- und untergeordneten Containers, so werden die Einstellungen des untergeordneten Containers verwendet, die des übergeordneten Containers werden in diesem Fall nicht vererbt.

Wenn in einem untergeordneten Container eine bestimmte Richtlinie nicht konfiguriert ist, sondern nur in dem übergeordneten Container, so wird daraus die Einstellung übernommen.

8.6.4 Inhalte eines GPOs

Jedes GPO ist in die Bereiche Computerkonfiguration und Benutzerkonfiguration unterteilt. In der Computerkonfiguration werden nur maschinenbezogene Einstellungen getroffen. Sie werden bei jedem Start des Computers angewendet. Dabei ist es gleichgültig, welcher Benutzer sich an dem Computer anmeldet. Umgekehrt bezieht sich die Benutzerkonfiguration nur auf den Benutzer. Dabei spielt es keine Rolle, an welchem Computer sich der Benutzer anmeldet. In beiden Konfigurationsbereichen befinden sich die Untercontainer SOFTWAREEINSTELLUNGEN, WINDOWS-EINSTELLUNGEN und ADMINISTRATIVE VORLAGEN.

Softwareeinstellungen

In beiden Konfigurationen befindet sich standardmäßig nur der Eintrag SOFTWAREINSTALLATION. Über diesen Punkt können neue Pakete für die Softwareverteilung erstellt und konfiguriert werden (siehe Kapitel Abbildung 8.7).

Windows-Einstellungen

Unter den WINDOWS-EINSTELLUNGEN finden Sie für beide Konfigurationen die Knoten SKRIPTS sowie SICHERHEITSEINSTELLUNGEN. Zusätzlich sind in der Benutzerkonfiguration noch Internet Explorer-Wartung, Remote-Installationsdienste sowie Ordnerumleitung vorhanden. Die folgende Tabelle zeigt Ihnen die Bedeutung der einzelnen Knoten.

Knoten	Beschreibung
Skripts	Hier können Sie Skripte für das An- und Abmelden von Benutzern sowie das Starten und Herunterfahren des Rechners definieren. Es sind Skripte in Form von Stapelverarbeitungen (.cmd/.bat) oder auch Visual Basic-, Java- oder Perl-Skripte möglich. Wenn mehrere Skripte eingesetzt werden, kann auch deren Reihenfolge bestimmt werden. Beim Starten eines Rechners wird erst das Startskript und bei der Benutzeranmeldung das Anmeldeskript verarbeitet. Beim Herunterfahren wird zunächst das Abmeldeskript und dann das Skript zum Herunterfahren abgearbeitet. Standardmäßig darf die Verarbeitung der Skripte maximal zehn Minuten in Anspruch nehmen. Dieser Wert kann jedoch bei Bedarf heraufgesetzt werden.
Sicherheitseinstellungen	Hier können Sie detaillierte Sicherheitseinstellungen für die Maschinen oder Benutzer einstellen. Dazu zählen Kontorichtlinien (Kennwort und Kontensperrung), das Zuweisen von Benutzerrechten oder Überwachungsrichtlinien. Weiterhin können Sie hier die Startoptionen für Windows-Systemdienste festlegen, für bestimmte Registry-Schlüssel und Dateien Sicherheitseinstellungen konfigurieren sowie die Richtlinien öffentlicher Schlüssel festlegen.

Knoten	Beschreibung
Internet Explorer-Wartung	Hier können Sie den Internet Explorer für die Client-Computer konfigurieren. Dazu zählen beispielsweise ein geändertes Logo, angepasste Symbolleisten, vordefinierte Verbindungen wie Proxy-Einstellungen usw., Links, die automatisch hinzugefügt werden, oder auch das Anpassen des Sicherheitsfilters.
Remote-Installationsdienste	Hier können Sie bestimmen, ob automatische oder benutzerdefinierte Remote-Installationen gestattet werden oder nicht, ob nach der Installation ein Neustart durchgeführt werden soll oder nicht.
Ordnerumleitung	Über die Ordnerumleitung können einige Windows-Ordner wie Eigene Dateien oder Startmenü vom standardmäßigen Benutzerprofil an eine zentrale Stelle im Netzwerk umgeleitet werden. Weitere Hinweise dazu finden Sie in Kapitel 8.x.

Tabelle 8.11: Die Windows-Einstellungen in einem GPO

Die mmc-Knoten SOFTWAREEINSTELLUNGEN (Zuweisung, Installation etc.), REMOTE-INSTALLATION sowie ORDNERUMLEITUNG sind nur verfügbar, wenn eine Domäne mit Active Directory eingerichtet worden ist.

Administrative Vorlagen

Unter der Computer- und Softwarekonfiguration finden Sie jeweils den Knoten ADMINISTRATIVE VORLAGEN. Hier können Sie die Einstellungen konfigurieren, die auf den Bereichen HKEY_LOCAL_MACHINE (Computerkonfiguration) sowie HKEY_CURRENT_USER (Benutzerkonfiguration) der Registry beruhen. Die Computerkonfiguration bezieht sich auf die folgenden Bereiche: Windows-Komponenten, System, Netzwerk und Drucker. Die administrativen Vorlagen der Benutzerkonfiguration umfassen zusätzlich die Bereiche Startmenü und Taskleiste, Desktop sowie Systemsteuerung. Dafür fehlt dort der Bereich Drucker. In den einzelnen Bereichen können Sie folgende Einstellungen vornehmen:

Knoten	Beschreibung
Windows-Komponenten	In der Computerkonfiguration können Sie Einstellungen für die Windows-Komponenten NetMeeting, Internet Explorer, Taskplaner und Windows Installer vornehmen. In der Benutzerkonfiguration sind zusätzlich Einstellungen am Windows Explorer und an der mmc möglich.
System	Für die Computerkonfiguration sind die Bereiche Anmeldung, Datenträgerkontingente, DNS-Client, Gruppenrichtlinien und Windows-Dateischutz verfügbar, für die Benutzerkonfiguration An-/Abmeldung sowie Gruppenrichtlinien.
Netzwerk	Hier legen Sie die Einstellungen für Offline-Dateien und Netzwerk- und DFÜ-Verbindungen fest wie z.B. die Verfügbarkeit des Netzwerkverbindungsassistenten oder das (De-)Aktivieren von LAN-Verbindungen.

Knoten	Beschreibung
Drucker	Hier werden Druckereinstellungen wie z.B. die Veröffentlichung im Active Directory vorgenommen.
Startmenü und Taskleiste	Hier können Sie das Startmenü individuell definieren. Es können bestimmte Programmgruppen oder Menüeinträge entfernt oder auch Kontextmenüs der Taskleiste deaktiviert werden.
Desktop	Es können Einstellungen für den Active Desktop wie z.B. das Hintergrundbild oder das Hinzufügen von Objekten vorgenommen werden. Auch für den Suchdialog des Active Directory können Größe oder Filter gesetzt werden.
Systemsteuerung	Hier können die Menüpunkte Software, Anzeige, Drucker und Ländereinstellungen näher konfiguriert werden. Die übrigen Elemente der Systemsteuerung können wahlweise auch ausgeblendet werden.

Tabelle 8.12: Die administrativen Vorlagen eines GPO

Jede einzelne Richtlinie der Benutzerkonfiguration (jedoch nicht alle in der Computerkonfiguration) verfügt in den Eigenschaften über zwei Registerkarten. Auf der Registerkarte RICHTLINIE können Sie die richtlinienspezifischen Einstellungen treffen und die Richtlinie aktivieren oder deaktivieren. Auf der Registerkarte ERKLÄRUNG finden Sie die Funktion der jeweiligen Richtlinie sowie die Einstellungen präzise erläutert, die Sie konfigurieren können. Da diese Erklärungen sehr eingängig sind, wird an dieser Stelle darauf verzichtet, alle Richtlinien im Detail zu beschreiben.

Jede Richtlinie kann einen von drei möglichen Werten haben. Entweder ist sie *nicht konfiguriert*, d.h., es wurde kein Wert festgelegt, oder aber es wurde ein Wert festgelegt, sodass die Richtlinie auf *aktiviert* oder *deaktiviert* gesetzt werden kann. Um einen Wert zu setzen oder die Richtlinie zu deaktivieren, wählen Sie die entsprechende Checkbox in den Eigenschaften der Richtlinie.

Wenn Sie eine bestimmte Anzahl von Richtlinien in den administrativen Vorlagen konfiguriert haben und ausschließlich diese im Blickpunkt haben möchten, so sollten Sie eine andere Ansichtsoption wählen. Standardmäßig werden alle Richtlinien angezeigt, egal ob sie konfiguriert sind oder nicht. Markieren Sie den Knoten ADMINISTRATIVE VORLAGEN in der Computer- bzw. Benutzerkonfiguration und wählen aus dem Menü ANSICHT den Punkt NUR KONFIGURIERTE RICHTLINIEN ANZEIGEN. Dadurch werden alle nicht konfigurierten Richtlinien ausgeblendet, und es bleiben nur die aktivierten und deaktivierten übrig.

8.6.5 Abarbeiten der Gruppenrichtlinien für Computer und Benutzer

Sobald ein Computer, für den Gruppenrichtlinien konfiguriert sind, hochgefahren wird und er den RPC-(Remote Procedure Call-)Dienst gestartet hat, werden zunächst die für die Computerkonfiguration definierten Gruppenrichtlinien angefordert. Ist der Computer kein Mitglied der Domäne, wird nur das lokale GPO abgearbeitet. Sind für den Computer mehrere GPOs auf einer Ebene, z.B. Standort, definiert, werden sie der Reihenfolge der definierten Liste nach abgearbeitet. Dabei wird die Reihenfolge lokal, Standort,

Domäne und OU eingehalten. Anschließend werden die Startskripte für den Computer abgearbeitet. Die Abarbeitung der maschinenbezogenen Richtlinien erfolgt, während das Fenster COMPUTEREINSTELLUNGEN WERDEN ÜBERNOMMEN beim Startvorgang angezeigt wird.

Dann erscheint das Fenster für die Benutzeranmeldung. Nachdem sich der Benutzer erfolgreich verifiziert hat, wird zunächst sein Benutzerprofil geladen. Dann werden die Gruppenrichtlinienobjekte in derselben Reihenfolge wie die der Computerkonfiguration abgearbeitet. Schließlich werden noch die Anmeldeskripte für den Benutzer ausgeführt. All dies geschieht im Hintergrund, während das Fenster BENUTZERDEFINIERTE EINSTELLUNGEN WERDEN GELADEN angezeigt wird.

Dies ist die standardmäßige Reihenfolge des Abarbeitens. Jedoch können für diese Reihenfolge auch Ausnahmen definiert werden. Die drei Ausnahmemöglichkeiten lauten KEIN VORRANG, DEAKTIVIERT und LOOPBACK. Die beiden ersten Optionen können Sie aktivieren (siehe Abbildung 8.33), indem Sie auf der Registerkarte GRUPPENRICHTLINIE auf OPTIONEN klicken.

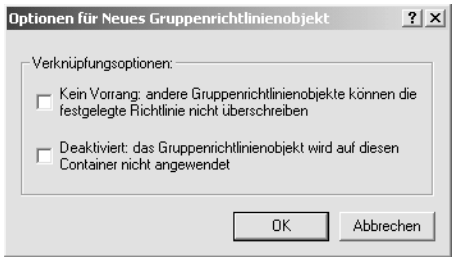


Abbildung 8.33: Verknüpfungsoptionen für ein GPO

Diese beiden Optionen haben folgende Bedeutung:

KEIN VORRANG: Diese Option bewirkt, dass keine Eigenschaft der Richtlinien dieses GPO überschrieben und damit außer Kraft gesetzt werden kann. Die Durchsetzung der mit KEIN VORRANG markierten Richtlinie wird erzwungen. Sind mehrere GPOs mit dieser Option markiert, so gilt diese Einstellung für das in der Hierarchie höchste Objekt. Sind also ein GPO auf Domänen- und eines auf OU-Ebene auf KEIN VORRANG gesetzt, so gilt die Option für das ranghöhere OU-GPO.

DEAKTIVIERT: Mit der Deaktivierung werden die Einstellungen am GPO am jeweiligen Container nicht durchgesetzt. Das Deaktivieren ist nur wirksam, wenn das GPO nicht auf KEIN VORRANG gesetzt ist.

Eine weitere Option zur Steuerung der GPO-Verarbeitung ist die Option LOOPBACK. Um diese Option anzuwenden, öffnen Sie den folgenden Pfad: GPO/COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM/GRUPPENRICHTLINIEN. Dort finden Sie die Richtlinie LOOPBACK-VERARBEITUNGSMODUS FÜR BENUTZERGRUPPENRICHTLINIE.

Die Loopback-Funktion ist für Computer sinnvoll, an denen die Benutzerrichtlinie je nach Computer geändert werden muss – unabhängig vom Benutzer. Hierzu zählen etwa Laboratorien oder Unterrichtsräume. Standardmäßig werden alle Benutzereinstellungen aus der GPO-Liste von Standort, Domäne und OU abgerufen, und zwar unter den Verer-

bungsbedingungen, wie sie vom Administrator konfiguriert sind. Um dieses Verhalten zu ändern, bieten sich beim Aktivieren dieser Richtlinie die Möglichkeiten ERSETZEN und ZUSAMMENFÜHREN.

ERSETZEN: Wenn Sie diese Option wählen, wird statt der GPO-Liste für den Benutzer die GPO-Liste für den Computer verwendet. Die Richtlinieneinträge der Computer ersetzen vollständig die Einträge des Benutzers, die normalerweise verwendet werden würden.

ZUSAMMENFÜHREN: In diesem Fall werden sowohl die GPO-Liste des Computers als auch die GPO-Liste des Benutzers bei der Anmeldung verwendet. Allerdings wird die GPO-Liste des Computers an die Benutzerliste angehängt und somit als zweite bearbeitet. Treten nun Konflikte zwischen den Einstellungen der beiden Listen auf, so überschreiben die Computereinstellungen die des Benutzers, da die Computer GPO-Liste als zweite verarbeitet wird.

8.6.6 Spezielle Optionen für Gruppenrichtlinien

Neben der Reihenfolge des Abarbeitens können Sie auch noch einige spezielle Einstellungen für die Richtlinien der Benutzer- und Computerkonfiguration treffen. Dazu zählen etwa das Aktualisierungsintervall oder synchrone bzw. asynchrone Anwendung des GPO. Sie erreichen diese Optionen über GRUPPENRICHTLINIE/COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM/GRUPPENRICHTLINIEN.

Computerkonfiguration

In der Computerkonfiguration stehen Ihnen die folgenden wichtigsten Optionen zur Verfügung:

- HINTERGRUNDAKTUALISIERUNG DER GRUPPENRICHTLINIE DEAKTIVIEREN: Ist diese Richtlinie aktiviert, werden die Richtlinien für die Computer- und Benutzerkonfiguration nicht im laufenden Betrieb des Computers aktualisiert, sondern erst wenn sich der Benutzer abgemeldet hat. Ist die Richtlinie deaktiviert, werden die Richtlinien in einem definierbaren Intervall aktualisiert.
- GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR COMPUTER: Sie können das Intervall festlegen, wie oft die Richtlinien für die Computerkonfiguration im Hintergrund während des laufenden Betriebes auf dem Computer aktualisiert werden soll. Es ist ein Wert zwischen 0 bis 64.800 Minuten (= 45 Tage) möglich. Damit nicht alle Clients gleichzeitig ihre Aktualisierung durchführen, ist eine Verzögerung des Intervalls konfigurierbar. Der Standardwert liegt bei 30 Minuten, kann aber bis auf 24 Stunden ausgedehnt werden. Wenn im Hintergrund eine Richtlinie der Computerkonfiguration aktualisiert wird, kann der Benutzer dies u.U. bemerken, wenn sich der Desktop aktualisiert oder geöffnete Menüs geschlossen werden. Über die Richtlinie GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR DOMÄNENCONTROLLER können dieselben Einstellungen auch für die Domänencontroller getroffen werden.
- GRUPPENRICHTLINIEN FÜR COMPUTER ASYNCHRON BEIM STARTEN ANWENDEN (nur Windows 2000): Bleibt diese Richtlinie deaktiviert, kann die Benutzeranmeldung erst erfolgen, wenn alle Gruppenrichtlinien der Computerkonfiguration aktualisiert worden sind. Vordem erhalten Sie nicht das Dialogfeld zur Windows-Anmeldung. Dies ist das standardmäßige und sichere Windows 2000-Startverfahren. Ist die Richtlinie

aktiviert, kann die Anmeldung bereits erfolgen, wenn noch nicht alle Richtlinien aktualisiert sind.

- GRUPPENRICHTLINIEN FÜR BENUTZER ASYNCHRON BEI DER ANMELDUNG ANWENDEN (nur Windows 2000): Bleibt diese Richtlinie deaktiviert, wird der Desktop für den Benutzer erst verfügbar, wenn alle Gruppenrichtlinien der Benutzerkonfiguration aktualisiert worden sind. Auch dies ist das sichere Windows-Standardverfahren. Wird die Richtlinie aktiviert, ist der Desktop bereits verfügbar, wenn noch nicht alle Richtlinien abgearbeitet sind. Startet der Benutzer bereits in dieser Zeit eine Applikation, an der Änderungen vorgenommen worden sind, so kann dies zu erheblichen Problemen führen.

Die eben beschriebenen Verarbeitungsmethoden werden standardmäßig nur unter Windows 2000 synchron durchgeführt. Windows XP Professional hingegen wartet standardmäßig beim Starten und Anmelden nicht ab, bis das Netzwerk vollständig gestartet ist. Meldet sich ein bekannter Benutzer am System an, werden gecachte Daten benutzt, was den Startvorgang deutlich beschleunigt. Die Gruppenrichtlinien werden somit asynchron verarbeitet, sobald das Netzwerk vollständig verfügbar ist. Nur wenn sich ein Benutzer neu an einem Rechner unter Windows XP anmeldet, werden die GPOs synchron verarbeitet.

Weiterhin können Sie z.B. für Registry, Internet Explorer, Ordnerumleitung, Datenträgerkontingente, Skripte oder Softwareinstallation Optionen wie Hintergrundaktualisierung, Erkennen von langsamen Verbindungen oder die Aktualisierung ohne Änderungen konfigurieren.

8.6.7 Mehrere Anmeldungen unter Windows XP, bis ein GPO wirksam wird

Wie gerade erwähnt, erfolgt die schnelle Benutzeranmeldung unter Windows XP durch das Cachen der letzten Benutzeranmeldung. Sind nun in der Zwischenzeit Änderungen an den Benutzereinstellungen – z.B. eine neue Ordnerumleitung – vorgenommen worden, so können diese Einstellungen bei der asynchronen Richtlinienverarbeitung beim erstmaligen Einloggen des Benutzers nicht übernommen werden. Nachdem aber alle Richtlinien abgearbeitet sind, werden die Änderungen den gecachten Daten hinzugefügt und somit die Login-Einstellungen aktualisiert. Dabei wird für den nächsten Anmeldevorgang die asynchrone Verarbeitung deaktiviert, damit die Änderungen umgesetzt werden können. Der Benutzer erhält also erst bei seiner zweiten Anmeldung nach der Änderung der Richtlinie die entsprechenden Einstellungen.

Ebenso verhält es sich, wenn einem Benutzer über die Softwareinstallation neue Software zugewiesen wurde. Bei der asynchronen Verarbeitung kann die Software nicht installiert werden, wenn für den Benutzer bereits der Desktop verfügbar ist. Stattdessen wird nicht der Benutzer, sondern der Computer darüber informiert, dass eine neue Software zu installieren ist. Bei der nächsten Anmeldung des Benutzers sorgt dann der Computer für die synchrone Richtlinienverarbeitung des Benutzers, sodass die Software installiert werden kann.

Diese Verhaltensweisen gelten selbstverständlich auch für Windows 2000, sofern dort das asynchrone Verarbeiten der Richtlinieneinstellungen aktiviert ist.

Um unter Windows XP wie unter Windows 2000 standardmäßig alle Änderungen bei einem Startvorgang und Einloggen wirksam werden zu lassen, müssen Sie unter COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM/ANMELDUNG die Richtlinie BEIM NEUSTART DES COMPUTERS UND BEI DER ANMELDUNG IMMER AUF DAS NETZWERK WARTEN aktivieren.

8.6.8 Implementierungsstrategie für Gruppenrichtlinien

Vor dem Erstellen der Gruppenrichtlinien sollten Sie sich auch einige Gedanken über die Planung der Gruppenrichtlinientypen sowie die Implementierung und Zuweisung machen. Beginnen Sie also nicht damit, planlos GPOs zu erstellen, die auf die Benutzer und Computer losgelassen werden.

Dieses Kapitel zeigt Ihnen einige Entwürfe und Hinweise zur Implementierung der Gruppenrichtlinien. Viele dieser einzelnen Entwürfe sind miteinander kombinierbar.

Anzahl der GPOs pro Benutzer und Computer

Entscheiden Sie, wie viele GPOs insgesamt erstellt und wie diese auf den verschiedenen Hierarchieebenen angewendet werden sollen. Im Modell der dezentralen GPOs wird pro Benutzer bzw. Computer nur ein einziges GPO auf OU-Basis angewendet, das eine Reihe von Richtlinieneinstellungen beinhaltet. Auf Domänen- und Standortbasis wird kein zentrales GPO definiert. Befinden sich innerhalb einer Organisationseinheit nun Benutzer oder Computer, die nicht dasselbe GPO verwenden können, so werden die Benutzer/Computer mit identischen Sicherheitsanforderungen innerhalb der OU zu einer Unter-OU innerhalb des Containers zusammengefasst. Dieses Modell bietet zwar den Vorteil, dass bei der Anmeldung nur ein GPO abzuarbeiten ist und diese somit schnell erfolgt. Jedoch erhöht sich der Verwaltungsaufwand, da Benutzer/Computer mit identischen Sicherheitsanforderungen in Unter-OUs zusammengefasst werden müssen.

Es ist umgekehrt auch möglich, für eine Domäne oder einen Standort ein zentrales GPO zu erstellen, das die Grundanforderungen an alle Benutzer erfüllt. Denkbar wären hierfür Optionen für die Benutzerkonten und Passwörter. Neben diesem globalen GPO können Sie spezifische GPOs für die einzelnen Organisationseinheiten einrichten. Dieses Verfahren ist sinnvoll, wenn die OUs nach funktionellen Aspekten eingerichtet worden sind. So werden alle Mitglieder einer OU Finanzen innerhalb dieser OU über nahezu identische GPO-Einstellungen verfügen, aber über komplett andere als die Mitglieder der OU Vertrieb. Dabei wird eine bestimmte Richtlinieneinstellung nach Möglichkeit nur in einem GPO vorhanden sein. Sind nun an dieser Richtlinie Änderungen erforderlich, so müssen Sie nur ein einziges GPO bearbeiten und nicht wie im eben beschriebenen Modell alle GPOs, die diese Richtlinie enthalten. Dieses Modell ist sinnvoll, wenn das Unternehmen über verschiedene Organisationseinheiten verfügt, die jeweils andere Sicherheitsaspekte zu bedenken haben. Allerdings können nun auch die Anmeldezeiten der Clients zunehmen, da sie eine Reihe von GPOs mit jeweils nur wenigen Richtlinien abzuarbeiten haben. Dafür ist der Verwaltungsaufwand geringer.

Anzahl der Richtlinien pro GPO

In diesem Zusammenhang ist das Definieren verschiedener Richtlinientypen erforderlich. Sie können GPOs erstellen, in denen entweder nur die Richtlinien der Benutzer- oder Computerkonfiguration enthalten sind. Die Anmeldezeit verlängert sich hierbei ein wenig, da zwei verschiedene GPOs abzuarbeiten sind. Jedoch eignet sich diese Einteilung zur schnellen Fehlersuche. Wird davon ausgegangen, dass der Fehler in dem GPO der Richtlinien der Benutzerkonfiguration liegt, so sollte sich unter einem anderen Benutzerkonto testweise angemeldet werden, dem keine Richtlinien zugewiesen sind. Ist damit der Fehler behoben, liegt er in der Benutzerkonfiguration, andernfalls in der Computerkonfiguration.

Eine weitere Möglichkeit zur Definition von Richtlinientypen besteht darin, den Bereich der Richtlinien festzulegen, die in einem GPO enthalten sein sollen. Sie können beispielsweise ein GPO anlegen, in dem sich nur die Richtlinien zur Softwareinstallation befinden, ein weiteres, das nur Richtlinien zur Anmeldung enthält usw. Selbstverständlich kann ein GPO auch Richtlinien aus verschiedenen Bereichen enthalten. Je mehr Richtlinien in einem GPO enthalten sind, desto geringer wird die Anmeldezeit der Clients, desto höher wird umgekehrt aber auch der administrative Aufwand beim Bearbeiten der Richtlinieneinstellungen.

Verwalten der GPOs

Durch die Delegierung der Verwaltung ist es möglich, dass die Administratoren auf OU-Ebene bestimmte domänenweite GPOs außer Kraft setzen. Bei anderen GPOs kann ihnen diese Möglichkeit auch entzogen werden. Sollen bestimmte Sicherheitseinstellungen eines domänenweiten GPOs nicht die Einstellungen des OU-GPO überschreiben, so sollte das OU-GPO mit der Option KEIN VORRANG versehen werden. Dieses Verfahren kann für unternehmensweite Konto- oder Passwortrichtlinien angewendet werden.

Um einem Administrator die Möglichkeit zu geben, OU-spezifische Einstellungen in seiner OU durchzusetzen und nicht ausschließlich domänenweite Richtlinien zu übernehmen, kann er mit der entsprechenden Berechtigung die Option RICHTLINIENVERERBUNG DEAKTIVIEREN für die gewünschte Organisationseinheit festlegen. Es kann jedoch nur die Vererbung der Gruppenrichtlinien deaktiviert werden, bei denen nicht die Option KEIN VORRANG ausgewählt ist.

8.6.9 Spezielle An- und Abmeldeskripte

Über die Gruppenrichtlinie können Sie Computern und Benutzern Skripte zum Starten und Herunterfahren bzw. für die An- und Abmeldung zuweisen. Das Login-Skript für einen Computer wird beim Start des Rechners ausgeführt, das für einen Benutzer, sobald er sich anmeldet. Die An- und Abmeldeskripte befinden sich im Verzeichnis SYSVOL\USER\SCRIPTS.

Diese Skripte können nur für Windows 2000- und XP-Clients ausgeführt werden. Ältere Windows-Clients besitzen nicht die Möglichkeit, diese Skripte aus dem Active Directory auszulesen und auszuführen. Für diese alten Clients müssen Sie die herkömmlichen Start- und Anmeldeskripte verwenden.

Im Gegensatz zu den altbekannten An- und Abmeldeskripten unter Windows NT, die meist als Batchdatei erstellt worden sind, können Sie nun auch Skripte in VBScript oder JScript erstellen. Sie können beispielsweise ein Skript erstellen, das beim Start die Gruppenmitgliedschaft eines Benutzers prüft. Es kann ermitteln, ob der Benutzer z.B. ein Mitglied der Gruppe Buchhalter in der Domäne *firma.de* ist. Mit Hilfe eines solchen Skriptes ist es möglich, Gruppenmitgliedern beim Start bestimmte Laufwerke oder Drucker zuzuweisen. Eine umfangreiche Referenz zu den Skriptsprachen finden Sie unter *www.microsoft.com/scripting*.

Über ein Skript können Sie das Anmeldeverhalten der Benutzer steuern. Bei der Anmeldung kann über ein Skript der Name des Benutzers abgefragt und geprüft werden, ob es sich um einen gültigen Active Directory-Benutzer handelt. Ist dies der Fall, wird weiter geprüft, ob er Mitglied einer im Skript definierten Benutzergruppe ist. Ist dies der Fall, werden weitere Optionen wie z.B. das Zumappen bestimmter Laufwerke und Drucker durchgeführt.

Das Skript wird als Textdatei geschrieben und unter der Dateiendung .vbs bei einem VBScript oder .js bei einem JavaScript gespeichert. Sie sollten ein Skript jedoch niemals per Doppelklick öffnen, da es automatisch startet und unvorhergesehene Aktionen auslösen könnte. Zum Bearbeiten öffnen Sie das Skript mit einem beliebigen Texteditor.

Ein praktisches Beispiel für den Einsatz eines An- und Abmeldeskripts ergibt sich aus folgender Situation: Wenn sich ein Administrator auch an einem beliebigen Arbeitsplatz unter Windows 2000 oder XP Professional anmelden und von dort aus den Server verwalten möchte, müssen ihm zu diesem Zweck seine Administrationswerkzeuge zur Verfügung stehen, aber nur so lange, wie der Administrator selbst auf dem Rechner angemeldet ist. Wenn sich hinterher ein anderer Benutzer dort anmeldet, dürfen für ihn diese Werkzeuge nicht mehr zur Verfügung stehen. Die Gefahr ist zu groß, dass der nachfolgende unversierte Benutzer diese als Spielzeug missbraucht. Unter Windows NT hätten Sie für sich als Administrator auf jedem Nicht-Server-Arbeitsplatz die Admin-Tools installieren und vor dem Verlassen des Arbeitsplatzes wieder deinstallieren müssen. Dieses zeitaufwändige Verfahren ist ab Windows 2000 nicht mehr notwendig. Bei der Anmeldung als Administrator werden die entsprechenden Programme installiert, über ein Abmeldeskript wird die Deinstallation der Programme durchgeführt.

Die Anzahl der Möglichkeiten für den Einsatz von An- und Abmeldeskripten und auch von Skripten zum Starten/Herunterfahren des Rechners ist vielfältig. Ein entscheidender Vorteil gegenüber Windows NT besteht darin, dass Sie nicht mehr nur ein, sondern eine beliebige Anzahl von Skripten für einen Computer oder Benutzer implementieren können. Angenommen, sämtliche Computer verfügen über ein standardisiertes Startskript. Nun soll jedoch auf allen Rechnern eine neue **.dll* oder ein bestimmter Registry-Schlüssel installiert werden. Diese Installation können Sie über ein zweites Startskript steuern. Ist die neue **.dll* oder der Schlüssel auf allen Computern installiert, kann dieses zweite Skript wieder entfernt werden.

Skripte eignen sich auch gut, wenn Benutzern nur für einen bestimmten Zeitraum standardmäßig nicht zugewiesene Operationen erlaubt werden sollen. Soll eine Gruppe von Benutzern beispielsweise eine Schulung zum Thema Internet Explorer erhalten, können Sie über ein zweites Anmeldeskript den Benutzern für die Dauer der Schulung erweiterte Berechtigungen zuteilen und ansonsten zugewiesene Einschränkungen wie z.B.

Browser-Menüs, Auto-Vervollständigen oder Filtereinstellungen aufheben. Ist die Schulung abgeschlossen, wird das zweite Skript wieder entfernt, und den Benutzern stehen nur noch die eingeschränkten Funktionalitäten zur Verfügung.

8.6.10 Die Group Policy Management Console (GPMC)

Die Group Policy Management Console (GPMC) ist eine neue mmc, in der sämtliche Einstellungen bezüglich der Gruppenrichtlinien zentral vorgenommen werden können. Dazu zählen Backup und Wiederherstellung an einem beliebigen Ort im Netzwerk sowie Im- und Export von GPOs und Sicherheitseinstellungen. Ferner werden HTML-Reports über die GPO-Einstellungen sowie die Auswirkungen von GPO-Einstellungen ausgegeben. Auch die Verwaltung der Sicherheitsaspekte wird in der GPMC simplifiziert. Zusätzlich besteht die Möglichkeit, WMI-Filter anzuwenden. Mit Hilfe von WMI-Filtern werden Anfragen an eine WMI-Datenbank auf einem Zielcomputer gesendet. Diese Datenbank wertet dies dann als wahr oder falsch aus. Sämtliche Operationen, die Sie über die GUI der GPMC vornehmen können, können auch skriptgesteuert erfolgen. Jedoch kann die Einstellung an den GPOs nicht via Skript vorgenommen werden.

Diese Zentralisierung stellt eine deutliche Verbesserung gegenüber der ursprünglichen Art der Gruppenrichtlinienverwaltung dar. Zum einen war die Verknüpfung eines GPO mit einer Reihe von Benutzergruppen zwar möglich, aber unübersichtlich. Man konnte sehr schnell den Überblick verlieren, an welchen Stellen das GPO verwendet wird. Auch die Anwendung von mehreren GPOs auf den verschiedenen Ebenen Standort, Domäne und OU konnte schnell kompliziert werden. Aufgrund von Vererbung der verschiedenen Richtlinien und Priorisierung von GPOs derselben Ebene war es sicher nicht immer ohne Probleme möglich, die genauen Auswirkungen der GPOs zu erkennen.

Ohne die GPMC musste ein Administrator eine Reihe von Werkzeugen zur Erstellung und Verwaltung von Gruppenrichtlinien aufrufen. In der GPMC sind jedoch die folgenden Programme enthalten: die mmcs ACTIVE DIRECTORY-BENUTZER UND -COMPUTER sowie ACTIVE DIRECTORY-STANDORTE UND -DIENSTE, RSoP (Resultant Set of Policy), der Delegierungs-Assistent sowie der ACL-Editor (Access Control List). Diese Funktionalitäten sind nun über einen zentralen Aufruf erreichbar. Sobald jedoch die GPMC installiert ist, kann die Administration der GPOs nicht mehr wie gewohnt durchgeführt werden. Wollen Sie den Gruppenrichtlinieneditor beispielsweise über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER aufrufen, so erhalten Sie die Meldung, dass Sie zur Verwaltung die GPMC benutzen mögen. Die Registerkarte GRUPPENRICHTLINIE in den Eigenschaften von Domänen oder Organisationseinheiten ist nicht länger verfügbar. Sie können darüber nur noch die GPMC öffnen.

Die GPMC ist bereits in den SBS 2003 integriert. Sie können diese Konsole über die Serververwaltung aufrufen.

Zusätzlich zum direkten Aufruf vom SBS 2003 aus kann die GPMC auch auf einem anderen Computer zur Remote-Verwaltung installiert werden. Dabei muss es sich um einen Computer mit Windows XP Professional oder Windows Server 2003 handeln. Im Falle von Windows XP müssen zusätzlich die folgenden Komponenten installiert sein:

- Windows XP SP1 sowie
- Microsoft .NET Framework

Zusätzlich wird das Post SP1-Hotfix Q326469 benötigt. Dies ist in der GPMC enthalten und wird während der Installation der GPMC mit installiert. Für die Verwendung auf einem anderen Computer kann die GPMC auch unter

https://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=F39E9D60-7E41-4947-82F5-3330F37ADFEB

downgeloadet werden. Sie finden die GPMC auch auf der mitgelieferten CD.

Neben den genannten neuen Kern-Features können mit der GPMC auch in weiteren Bereichen Verwaltungsaufgaben durchgeführt und simplifiziert werden. Tabelle 8.13 gibt Ihnen einen Überblick über weitere Features der GPMC.

Feature	Beschreibung
Neue Gruppenrichtlinieneinstellungen	Der Windows Server 2003 enthält über 150 zusätzliche GPO-Einstellungen gegenüber Windows 2000. Diese beziehen sich u.a. auf die Bereiche Terminal Server, DNS, Fehler-Reporting oder Roaming Profiles.
Webansicht der administrativen Vorlagen	Sobald eine bestimmte Richtlinieneinstellung gewählt wird, zeigt die Webansicht detaillierte Informationen zu den Einstellungen sowie dem Zweck der Einstellungen. Die Webansicht ist auch für die Registerkarte ERKLÄRUNG jeder Einstellung verfügbar.
GPO-Modeling	Das GPO-Modeling bietet die Möglichkeit, Richtlinieneinstellungen, Sicherheit und Applikationen in einem „Was-wenn-Szenario“ zu untersuchen. Diese Funktion ist bei einer Umstrukturierung oder Expansion sehr hilfreich. Bevor eine Änderung durchgeführt wird, können zahlreiche Tests ausgeführt werden, um die Konsequenzen für einen Benutzer oder eine Gruppe abzusehen.
DNS-Client	Die DNS-Client-Einstellungen auf dem SBS 2003 wie z.B. die dynamische Registrierung der DNS-Records oder die Übernahme des primären DNS-Suffix können vereinfacht über die Gruppenrichtlinie eingestellt werden.
Netzwerkverbindungen	Über die Gruppenrichtlinie kann die GUI zur Einstellung der Netzwerkverbindungen nur bestimmten Benutzern verfügbar bzw. nicht verfügbar gemacht werden.
Softwareinstallation bei der Anmeldung	Bei der Softwareverteilung besteht nun die Möglichkeit, dem Benutzer zugewiesene Software vollständig bei seiner Anmeldung zu installieren und nicht erst bei Bedarf.
Software Support-URL	Für jedes installierte Softwarepaket kann der Benutzer über die Systemsteuerung – Software – Hinzufügen/Entfernen eine URL aufrufen, über die er direkt auf die Supportseite des Herstellers gelangt. Dies entlastet den firmeninternen Support und das Helpdesk.

Feature	Beschreibung
WMI-Filter	Über WMI (Windows Management Instrumentation) werden Hard- und Software-Inventory-Daten sowie weitere Konfigurationseinstellungen aus der Registry, dem Dateisystem, Treibern, Active Directory, Windows Installer, SNMP, Netzwerk, SQL und Exchange ausgelesen. Beim WMI-Filtering kann festgelegt werden, ob ein GPO auf einem WMI-Filter beruhen soll. Ein WMI-Filter ist eine Abfrage der WMI-Daten. Über diesen Filter können Sie festlegen, auf welche Benutzer und Computer ein GPO angewendet werden soll. Diese Funktion ist sinnvoll, wenn an alle Benutzer einer OU ein bestimmtes Softwarepaket verteilt werden soll, wofür jedoch genügend Festplattenkapazität zur Verfügung stehen muss. Sie können in diesem Fall einen WMI-Filter verwenden, der die Applikation lediglich bei den Benutzern installiert, die über mindestens 500 MB freien Festplattenplatz verfügen.

Tabelle 8.13: Weitere Features der GPMC

8.6.11 Die Administration über die GPMC

Nach der Installation der GPMC befindet sich im STARTMENÜ/VERWALTUNG der neue Eintrag GRUPPENRICHTLINIENVERWALTUNG. Beim Start dieser mmc werden Sie aufgefordert, sich mit einem gültigen Domänenbenutzerkonto anzumelden, sofern der Verwaltungscomputer lediglich Mitglied einer Arbeitsgruppe ist. Abbildung 8.34 zeigt eine Übersicht über die GPMC.

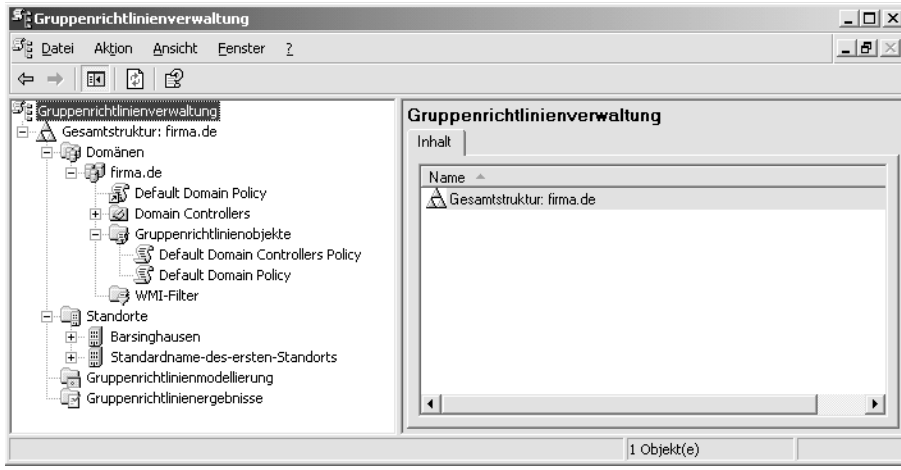


Abbildung 8.34: Die Group Policy Management Console (GPMC)

In der mmc wird die Hierarchie des Netzwerks von der obersten Ebene der Gesamtstruktur über Domänen, Standorte und OUs bis hin zu den einzelnen GPOs abgebildet. Standardmäßig werden dort keine Standorte und weiteren Domänen außer der aktuel-

len angezeigt. Um weitere Objekte der mmc hinzuzufügen, wählen Sie aus dem Kontextmenü von DOMÄNEN bzw. STANDORTE den Eintrag DOMÄNEN ANZEIGEN bzw. STANDORTE ANZEIGEN. Aus der Liste wählen Sie die Standorte bzw. Domänen aus, die in der mmc angezeigt werden sollen.

8.6.12 Erstellen, Löschen und Verknüpfen von GPOs

Um in der GPMC ein neues GPO zu erstellen, wählen Sie eine Domäne und klicken dort auf GRUPPENRICHTLINIENOBJEKTE. Aus dem Kontextmenü wählen Sie NEU und vergeben einen Namen für das neue GPO. Soll das neue GPO zugleich mit der Domäne verknüpft werden, so wählen Sie GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN. Soll ein bestehendes GPO mit einer Domäne, einem Standort oder einer OU verknüpft werden, so wählen Sie aus dem jeweiligen Kontextmenü den Eintrag VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN.

Nachdem das Objekt erstellt ist, wählen Sie aus dessen Kontextmenü BEARBEITEN. Es öffnet sich der Gruppenrichtlinienobjekt-Editor, mit dem Sie alle Einstellungen bearbeiten können, wie in Kapitel Abbildung 8.6.4 beschrieben. Bedenken Sie, dass sich die Änderungen an einem bestehenden GPO auf sämtliche Container auswirken, mit denen das GPO verknüpft ist. Bei Änderungen gibt die GPMC jeweils eine Warnmeldung aus, die Sie an diese Tatsache erinnert.

Jedes GPO verfügt über insgesamt vier Registerkarten. Unter BEREICH (siehe Abbildung 8.35) sehen Sie, mit welchen Standorten, Domänen und OUs das GPO verknüpft ist, für welche Benutzergruppen das GPO angewendet wird und mit welchen WMI-Filtern es verknüpft ist.

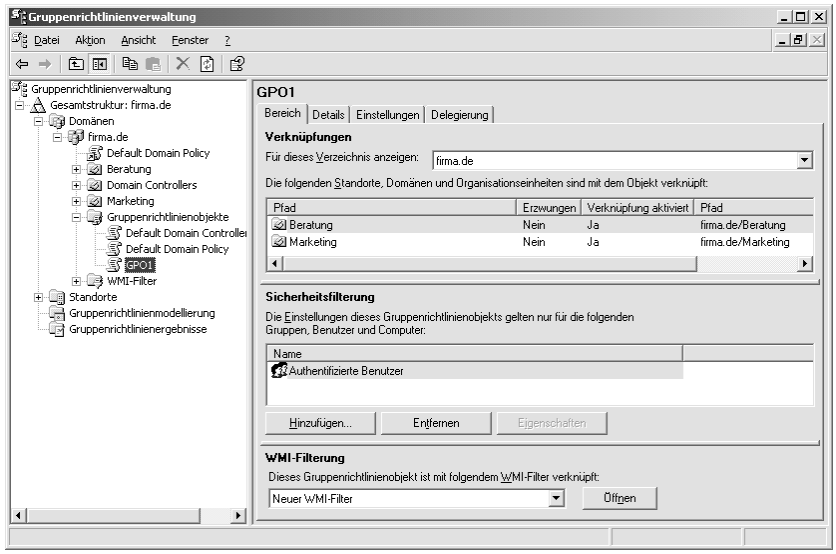


Abbildung 8.35: Die Registerkarte Bereich eines GPO

Die Registerkarte DETAILS gibt Auskunft über Erstell- und Änderungsdatum, die GUID, den Besitzer, die Domäne sowie den Objektstatus.

Die Registerkarte EINSTELLUNGEN (siehe Abbildung 8.36) zeigt, welche Bereiche des GPO konfiguriert worden sind. Für die Computer- und Benutzerkonfiguration finden Sie eine übersichtliche Auflistung der Richtlinien, die aktiviert oder deaktiviert sind. Nicht konfigurierte Einstellungen werden nicht angezeigt.

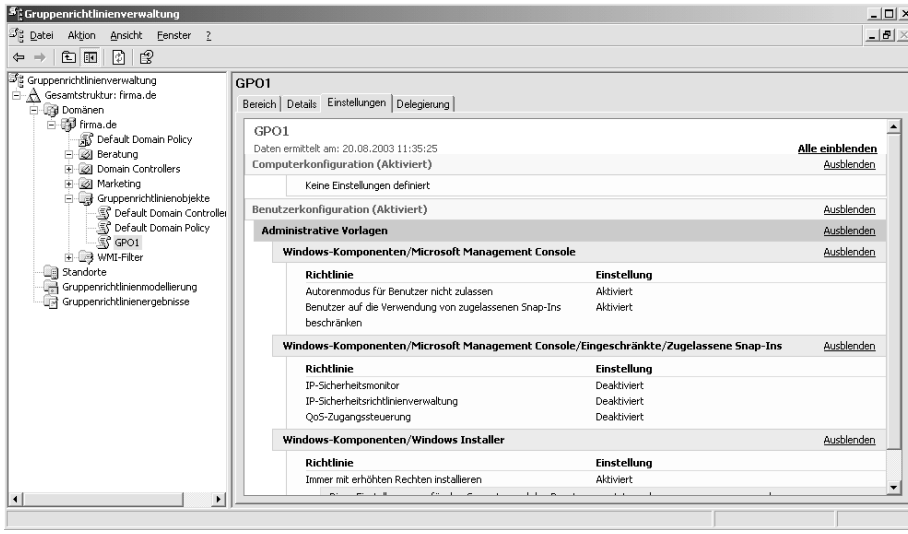


Abbildung 8.36: Die Registerkarte Einstellungen eines GPO

Die vierte Registerkarte DELEGIERUNG zeigt an, welche Benutzer und Gruppen welche Berechtigungen für das GPO besitzen. Über die Einträge im Kontextmenü der Gruppen und Benutzer können die Berechtigungen auch modifiziert werden.

Bevor Sie ein GPO löschen, sollten Sie auf dessen Registerkarte BEREICH prüfen, ob noch domänenübergreifende Verknüpfungen bestehen. Wählen Sie dazu aus der Drop-down-Liste VERKNÜPFUNGEN FÜR DIESES VERZEICHNIS ANZEIGEN DEN EINTRAG [GESAMTSTRUKTUR]. Nun können Sie alle bestehenden Verknüpfungen löschen, bevor das GPO selbst endgültig gelöscht wird. Die beiden GPOs *Default Domain Controllers Policy* und *Default Domain Policy* können nicht gelöscht werden.

Über den Kontextmenüeintrag STATUS DER GRUPPENRICHTLINIE jedes GPO können Sie den Status der Richtlinien festlegen. Sie können das GPO aktivieren, separat die Einstellungen der Benutzerkonfiguration oder Computerkonfiguration oder das gesamte GPO deaktivieren.

8.6.13 Backup von GPOs

Beim Backup eines GPO werden sämtliche Bestandteile des GPO gesichert, die im Active Directory selbst sowie der Dateistruktur im Ordner SYSVOL enthalten sind. Dazu zählen die GUID des GPO sowie die Domäne, die Einstellungen des GPO, die Zugriffsberechtigungen für das GPO sowie der Verweis auf möglicherweise verknüpfte WMI-Filter. Die WMI-Filter selbst werden beim Backup eines GPO jedoch nicht gesichert. Dasselbe gilt auch für IPSec-Richtlinien, die auf eine GPO angewendet werden können. Dies liegt

darin begründet, dass beispielsweise für einen WMI-Filter andere Berechtigungen gelten als für das GPO selbst. Es wäre also möglich, dass einem Administrator beim Backup oder Wiederherstellen eines GPO nicht die erforderlichen Berechtigungen für einen WMI-Filter oder eine IPSec-Richtlinie zur Verfügung stehen. Zusätzlich würde es unnötig sein, WMI-Filter oder IPSec-Richtlinien zusammen mit jedem GPO zu speichern, wenn diese mit mehreren GPOs verknüpft sind. Für das Backup der WMI-Filter selbst verwenden Sie in der GPMC die Export- und Importfunktion des WMI-Filters selbst (siehe Kapitel Abbildung 8.6.21). Ein Backup der IPSec-Richtlinien führen Sie über die Import- und Exportfunktion des Snap-in IP-SICHERHEITSRICHTLINIEN IN DEM JEWEILIGEN GPO SELBST DURCH.

Beim Backup eines GPO wird ein XML-basierter Bericht erstellt. Dieser Bericht enthält einen Zeitstempel, optional eine Beschreibung sowie die GPO-Einstellungen. Jeder Backup-Vorgang wird durch eine eindeutige Nummer gekennzeichnet. So ist es möglich, mehrere Sicherungen desselben GPO an demselben Speicherort abzulegen. Die XML-basierten Backup-Berichte können über die GPMC als HTML betrachtet werden.

Damit ein Backup durchgeführt werden kann, muss für das GPO die Berechtigung Lesen bestehen. Für den Speicherort des Backups muss Schreibzugriff vorhanden sein. Um ein Backup eines GPO anzulegen, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des gewünschten GPO den Eintrag SICHERN.
2. Sie erhalten das Fenster GRUPPENRICHTLINIENOBJEKT SICHERN (siehe Abbildung 8.37). Über die Schaltfläche DURCHSUCHEN legen Sie den Speicherort fest. In das Textfeld BESCHREIBUNG können Sie optional einen Kommentar angeben. Klicken Sie dann auf SICHERN.

Abbildung 8.37: Die Sicherung eines GPO durchführen

Während des Sicherungsvorgangs werden Sie über den Status sowie den Erfolg oder Misserfolg informiert.

Wollen Sie mehrere GPOs gleichzeitig sichern, so klicken Sie in der GPMC auf den Knoten GRUPPENRICHTLINIENOBJEKTE. Auf der Registerkarte INHALT markieren Sie nun ein GPO oder mehrere. Wollen Sie mehrere GPOs markieren, halten Sie dabei die Taste Strg gedrückt. Sie erhalten dasselbe Dialogfeld wie in Abbildung 8.37 dargestellt. Es werden dann alle gewählten GPOs gesichert.

Wollen Sie sämtliche vorhandenen GPOs sichern, so wählen Sie aus dem Kontextmenü des Knotens GRUPPENRICHTLINIENOBJEKTE den Eintrag ALLE SICHERN. Sie erhalten ebenfalls dasselbe Dialogfeld wie in Abbildung 8.37 dargestellt. Es werden dann alle vorhandenen GPOs gesichert.

Für die Sicherung der GPOs können Sie auch Skripte verwenden. Sie können entweder eigene Skripte schreiben oder ein vordefiniertes Skript benutzen. Die vordefinierten Skripte befinden sich im Verzeichnis GPMC\SCRIPTS. Mit Hilfe des Skripts *BackupGPO.wsf* können Sie die Sicherung eines GPO durchführen, das Skript *BackupAllGPO.wsf* führt eine Sicherung sämtlicher GPOs durch.

Verwalten mehrerer Backups

Außer der Erstellung von Sicherungen ist über die GPMC auch die Verwaltung der Backups möglich. Um das Dialogfenster zur Backup-Verwaltung aufzurufen, wählen Sie entweder aus dem Kontextmenü des DOMÄNEN-Containers oder des Containers GRUPPENRICHTLINIENOBJEKTE den Eintrag SICHERUNGEN VERWALTEN. Im ersten Fall werden alle gesicherten GPOs der kompletten Gesamtstruktur angezeigt, im zweiten Fall lediglich die GPOs der aktuellen Domäne. Die Verwaltungsmöglichkeiten sind in beiden Fällen dieselben (siehe Abbildung 8.38).

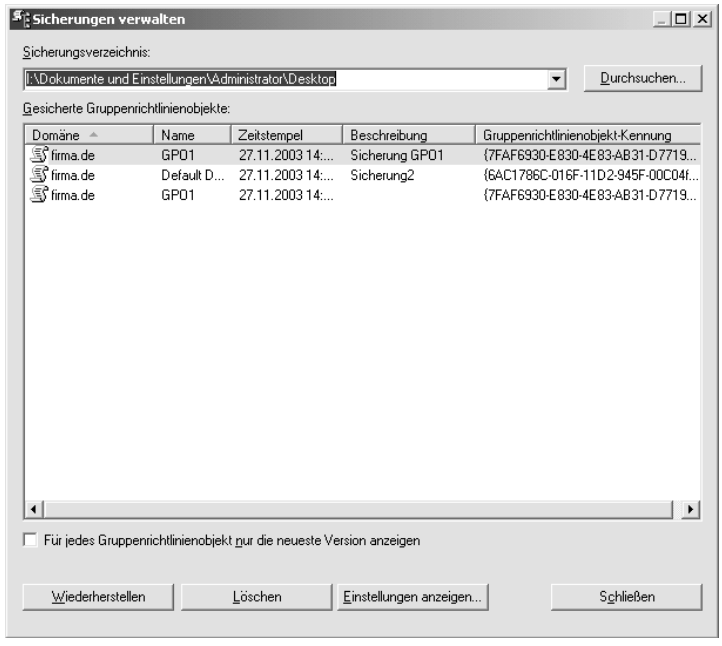


Abbildung 8.38: Die Verwaltung mehrerer gesicherter GPOs

Im Fenster SICHERUNGEN VERWALTEN sehen Sie unter SICHERUNGSVERZEICHNIS den Pfad zu der Lokation, in der sich die angezeigten Sicherungen der GPOs befinden. Zu jedem gesicherten Objekt wird der Name der Domäne, der Name des GPO, der Zeitpunkt des Backups, eine optionale Beschreibung sowie die eindeutige GUID des GPO angegeben. Sofern Sie die Checkbox FÜR JEDES GRUPPENRICHTLINIENOBJEKT NUR DIE NEUESTE VERSION ANZEIGEN aktivieren, wird für ein GPO, das mehrmals gesichert wurde, lediglich der Eintrag angezeigt, der den neuesten Zeitstempel trägt.

Im unteren Bereich befinden sich drei Schaltflächen, über die Sie ein gesichertes GPO wieder herstellen oder löschen können. Jede dieser beiden Aktionen muss vor ihrer Durchführung separat bestätigt werden. Auch das Anzeigen der GPO-Einstellungen ist möglich. Hierzu öffnet sich der standardmäßige Webbrowser des Benutzers und zeigt die Einstellungen als html-Seite an.

Die Verwaltung mehrerer Sicherungen kann auch skriptgesteuert erfolgen. Verwenden Sie hierzu das Beispielskript *QueryBackupLocation.wsf*, das sich im Verzeichnis GPMC\SCRIPTS befindet.

8.6.14 Wiederherstellung von GPOs

Die Wiederherstellung eines GPO darf nicht mit dem Import oder Kopieren eines GPO (siehe Kapitel Abbildung 8.6.15) verwechselt werden. Beim Wiederherstellen wird das GPO auf einen früheren Status zurückgesetzt. Dies kann erforderlich werden, wenn ein GPO wieder auf einen funktionierenden älteren Status gebracht werden soll (Rollback) oder wenn ein GPO versehentlich gelöscht worden ist. Bei der Wiederherstellung behält das GPO seine ursprüngliche GUID. Ersetzt werden die Einstellungen des GPO, seine Berechtigungen sowie die verknüpften WMI-Filter. Sind beim Löschen eines GPOs auch seine Verknüpfungen gelöscht worden, so müssen diese manuell wiederhergestellt werden. Dieser Prozess ist nicht Bestandteil der GPO-Wiederherstellung. Um die Verknüpfungen schneller wiederherstellen zu können, sehen Sie sich den Sicherungsbericht des GPOs an, in dem alle Verknüpfungen des GPOs innerhalb der Domäne aufgeführt sind.

Ein gesichertes GPO kann nicht wiederhergestellt werden, wenn zwischenzeitlich die Domäne umbenannt worden ist. Sie sollten also grundsätzlich sämtliche GPOs sichern, sobald eine Domäne umbenannt worden ist.

Wiederherstellen vorhandener GPOs

Um ein vorhandenes GPO mit seinen ursprünglichen Einstellungen wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü des GPOs den Eintrag VON SICHERUNG WIEDER HERSTELLEN. Damit wird der Wiederherstellungs-Assistent gestartet.
2. Geben Sie zunächst den Ordner an, in dem sich die Sicherungen der GPOs befinden. Sie können auch über die Schaltfläche DURCHSUCHEN nach einem Ordner suchen. Klicken Sie dann auf WEITER.

3. Nachdem Sie einen Sicherungsordner ausgewählt haben, werden nun alle Sicherungen des GPO angezeigt, die sich in diesem Ordner befinden (siehe Abbildung 8.39). Zur besseren Orientierung wird für jede Sicherung der Zeitstempel sowie die optionale Beschreibung angezeigt. Über die Schaltfläche EINSTELLUNGEN ANZEIGEN können Sie die Details des GPO betrachten. Markieren Sie dann die gewünschte Sicherung und klicken auf WEITER.

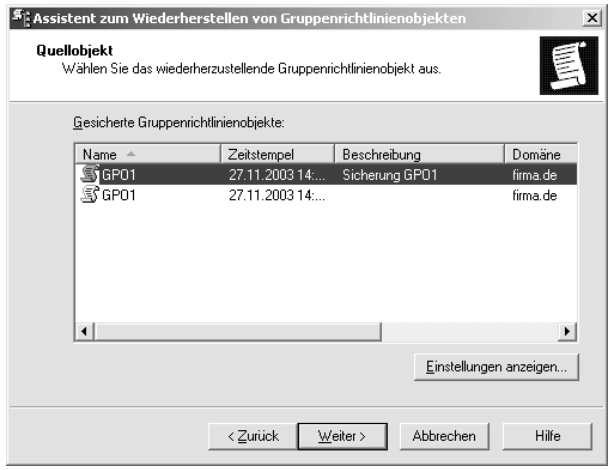


Abbildung 8.39: Die Auswahl des wiederherzustellenden GPO

4. Sie erhalten eine Zusammenfassung über die gewählten Schritte. Klicken Sie hier auf FERTIG STELLEN. Damit wird das gesicherte GPO mit seinen Einstellungen wiederhergestellt und überschreibt die aktuellen Werte des GPO. Die Versionsnummer des GPO wird dabei um einen Wert erhöht. Dies ist erforderlich, damit die Clients, auf die das GPO angewendet wird, das wiederhergestellte GPO übernehmen.

   Um ein GPO wiederherstellen zu können, müssen Sie über Berechtigungen verfügen, die ein Löschen, Ändern der Sicherheitseinstellungen sowie Bearbeiten der Einstellungen zulassen. Zudem müssen Sie über Lesezugriff auf das Quellverzeichnis des gesicherten GPO verfügen. Es ist jedoch nicht die Berechtigung zum Erstellen von GPOs erforderlich.

Wiederherstellen bereits gelöschter GPOs

Um ein versehentlich gelöschtes GPO wiederherzustellen, öffnen Sie das Fenster SICHERUNGEN VERWALTEN (siehe Abbildung 8.38). Markieren Sie dort den gewünschten Eintrag und klicken auf die Schaltfläche WIEDERHERSTELLEN. Wenn Sie ein bereits gelöschtes GPO wiederherstellen, wird die Versionsnummer des gesicherten GPOs beibehalten. Das wiederhergestellte GPO trägt also dieselbe Versionsnummer wie das gesicherte GPO. Um ein gelöschtes GPO wiederherstellen zu können, müssen Sie über die Berechtigung verfügen, GPOs in der Domäne erstellen zu dürfen. Die Person, die das GPO wiederherstellt, wird zudem zum neuen Ersteller-Besitzer des GPO.

Skriptgesteuerte Wiederherstellung von GPOs

Um ein GPO skriptgesteuert wiederherzustellen, können Sie entweder ein eigenes Skript schreiben oder auf die vordefinierten Skripte im Verzeichnis GPMC\SCRIPTS zugreifen. Verwenden Sie das Skript *RestoreGPO.wsf*, um ein einzelnes GPO wiederherzustellen, und das Skript *RestoreAllGPOs.wsf*, um sämtliche GPOs wiederherzustellen.

Wiederherstellen von GPOs mit Einstellungen zur Softwareinstallation

Beim Wiederherstellen von GPOs ist denjenigen GPOs besondere Beachtung zu schenken, die Einstellungen zur Softwareinstallation (siehe Kapitel Abbildung 8.7) enthalten. Dies gilt, wenn ein solches GPO gelöscht wurde und wieder hergestellt werden soll. Dabei können zwei verschiedene Probleme auftreten.

1. Sofern GPO-übergreifende Beziehungen bestehen, die eine Applikation in dem wiederhergestellten GPO updaten, werden diese nach der Wiederherstellung nicht beibehalten. Die Applikation des wiederhergestellten GPO verliert also ihr Update. In diesen GPO-übergreifenden Beziehungen ist festgelegt, dass eine Applikation eine andere updaten soll, wobei die beiden Applikationen nicht über dasselbe GPO verteilt werden. Die Beziehungen bleiben jedoch bestehen, wenn die Applikationen im wiederhergestellten GPO ihrerseits Applikationen anderer GPOs updaten soll.
2. Sofern der Clientcomputer noch nicht darüber informiert ist, dass ein GPO gelöscht wurde – dies ist der Fall, wenn seit dem Löschen noch kein Neustart des Computers oder keine neue Anmeldung des Benutzers erfolgt ist – und an ihn Applikationen verteilt wurden, welche die Option ANWENDUNGEN DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGEN besitzen, so werden veröffentlichte Applikationen (siehe Kapitel Abbildung 8.7.3), die bereits installiert sind, beim nächsten Einloggen gelöscht, und zugewiesene Applikationen werden vor einer Neuinstallation zunächst deinstalliert.

Normalerweise wird bei der Option ANWENDUNGEN DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGEN die Anwendung deinstalliert, wenn das betreffende GPO nicht mehr auf den Computer oder Benutzer angewendet wird.

Dieses ungewünschte Verhalten liegt darin begründet, dass bei der Wiederherstellung dem Active Directory-Objekt, das die entsprechende Applikation repräsentiert, eine neue GUID zugewiesen wird. Da sich die GUID der bereits vorhandenen Applikation von der neu zugewiesenen GUID unterscheidet, wird die Applikation von Windows als zwei verschiedene Applikationen angesehen. Eine Lösung dieses Problems kann nur darin bestehen, bei der Wiederherstellung des GPOs die ursprüngliche GUID der Applikation zu benutzen. Da jedoch die GUIDs vom Active Directory vergeben werden, kommt hier ein neues Feature des Windows Server 2003 zum Tragen. Hierbei handelt es sich um die sog. Tombstone-Reanimierung (Tombstone re-animation). Tombstones sind Objekte im Active Directory, die zwar gelöscht sind, aber noch nicht endgültig aus dem Verzeichnis entfernt worden sind. Standardmäßig werden alle gelöschten Objekte erst nach 60 Tagen endgültig entfernt.

Die Tombstone-Reanimierung wird beim Wiederherstellen von GPOs automatisch von der GPMC ausgeführt. Diese Reanimierung kann erfolgreich durchgeführt werden, wenn die folgenden drei Punkte erfüllt sind:

- Die GPMC arbeitet mit einem Domänencontroller, auf dem Windows Server 2003 ausgeführt wird.
- Der Zeitraum zwischen dem Löschen und Wiederherstellen des GPO darf nicht das definierte Tombstone-Intervall überschreiten. Standardmäßig liegt dieser Zeitraum bei 60 Tagen.
- Der Benutzer, der die Wiederherstellung durchführt, muss über die Berechtigung zur Tombstone-Reanimierung verfügen. Standardmäßig besitzen nur die Domänen- und Organisationsadministratoren diese Berechtigung. Sie kann jedoch über den ACL-Editor jeder anderen Person zugewiesen werden.

Schlägt die Tombstone-Reanimierung fehl, wird der Applikation eine neue GUID zugewiesen und sie somit als neue Applikation identifiziert, sodass die oben beschriebenen Probleme auftreten.

8.6.15 Kopieren von GPOs

Ob GPOs zwischen zwei Domänen kopiert werden sollen oder ein Import des GPO von einer Domäne in die andere durchgeführt werden soll, ist davon abhängig, ob zwischen den Domänen eine Vertrauensstellung besteht oder nicht. Ist dies der Fall, können die GPOs kopiert werden, andernfalls ist ein Import durchzuführen (siehe Kapitel 8.6.16). Man spricht im zweiten Fall auch von Migration der GPOs. Da im Umfeld des SBS 2003 keine Vertrauensstellung zu einer anderen Domäne bestehen kann, entfällt hier die Möglichkeit, GPOs zu kopieren. Ein Kopieren von GPOs ist somit auch nicht von der Testumgebung in die produktive Umgebung möglich.

8.6.16 Import und Export von GPOs

Deshalb kann unter dem SBS 2003 nur der Import und Export von GPOs verwendet werden. Der Importvorgang von GPOs wird auch als Migration bezeichnet. Beim Migrieren von GPOs sind verschiedene Dinge zu bedenken, da die Daten sehr komplex sind, an verschiedenen Stellen gespeichert werden und einige dieser Daten domänenspezifisch sind. Damit diese domänenspezifischen Daten ebenfalls korrekt migriert werden können, verwendet die GPMC Migrationstabellen (siehe Kapitel 8.6.18). In diesen Tabellen können die domänenbezogenen Daten mit den neuen Werten für das GPO eingetragen werden.

Bei dem Import werden die Einstellungen eines GPO in ein vorhandenes GPO transferiert. Als Quelle dient die Sicherung des GPO. Wie beim Kopieren kann sich das Ziel-GPO entweder in derselben Domäne, in einer anderen Domäne derselben Gesamtstruktur oder sogar in einer anderen Domäne einer anderen Gesamtstruktur befinden. Allerdings muss in diesem Fall keine Vertrauensstellung zwischen den Domänen bestehen. Es muss lediglich von der Zieldomäne aus Zugriff auf den Speicherort der GPOs in der Quelldomäne bestehen. Das Ziel-GPO, in das die Einstellungen transferiert werden, behält seine Sicherheitseinstellungen sowie Verknüpfungen mit seinen WMI-Filtern.

Um ein GPO zu importieren, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des GPO den Eintrag EINSTELLUNGEN IMPORTIEREN. Damit wird ein Assistent gestartet.
2. Da die aktuellen Einstellungen des GPO beim Import überschrieben werden, können Sie diese sichern. Wollen Sie eine Sicherung durchführen, klicken Sie auf die Schaltfläche SICHERN. Sie können dann einen Speicherort angeben. Klicken Sie danach auf WEITER.
3. Als Nächstes wählen Sie den Sicherungsordner aus, in dem sich das zu importierende GPO befindet. Sind dort mehrere GPOs vorhanden, so wählen Sie das gewünschte aus. Klicken Sie dann auf WEITER.
4. Nun wird die ausgewählte Sicherung überprüft, ob sich in dieser UNC-Pfade oder Sicherheitsprincipals befinden, die übertragen werden müssen (siehe Abbildung 8.40). Ist dies der Fall, kommen die Migrationstabellen zum Zuge. Andernfalls klicken Sie auf WEITER. Sie erhalten eine Zusammenfassung. Klicken Sie hier auf FERTIG STELLEN.

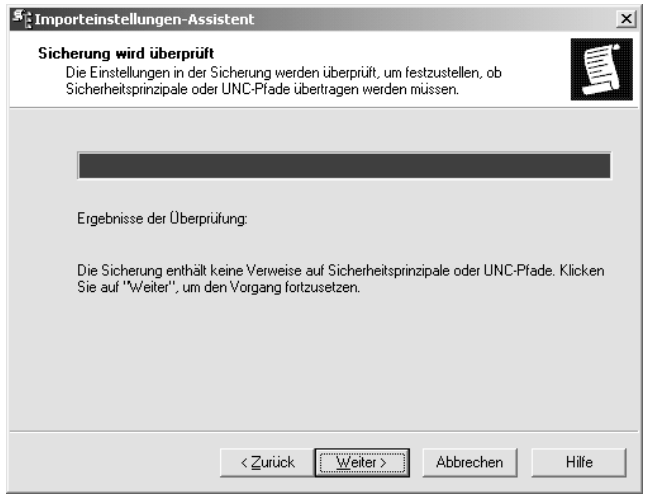


Abbildung 8.40: Überprüfen der GPO-Sicherung auf Sicherheitsprincipals und UNC-Pfade hin

Auch ein skriptgesteuerter Import ist möglich. Hierzu finden Sie im Ordner GPMC\SCRIPTS das Skript ImportGPO.wsf, um ein GPO zu importieren, sowie das Skript ImportAllGPOs.wsf, um sämtliche GPOs zu importieren.

8.6.17 Erstellen von HTML-Berichten

Um einen HTML-Bericht für ein GPO zu erstellen, wählen Sie zunächst aus der OU oder der Domäne das gewünschte GPO. Im Detailbereich klicken Sie nun auf die Registerkarte EINSTELLUNGEN.

Aus dem Kontextmenü des Einstellungsberichts wählen Sie nun DRUCKEN oder BERICHT SPEICHERN. Berichte werden im HTML-Format gespeichert und können im Internet Explorer angezeigt werden. Hierzu ist entweder der Internet Explorer in der Version 6

oder der Netscape Navigator in der Version 7 erforderlich. Über EIN-/AUSBLENDEN können Sie auswählen, welche Informationen über die GPOs der Bericht enthalten soll. Ist im Internet Explorer eine erhöhte Sicherheitskonfiguration aktiviert, so müssen Sie beim Anzeigen der Berichte jeweils eine Bestätigung ausführen, da ein Skript ausgeführt wird. Um diese Bestätigung zu umgehen, fügen Sie zur Liste vertrauenswürdiger Sites im Internet Explorer den Eintrag *about:security_mmc.exe* hinzu.

8.6.18 Migrationstabellen

Migrationstabellen werden beim Kopieren und Importieren von GPOs zwischen zwei verschiedenen Domänen benutzt. In diesen Tabellen sind die domänenspezifischen Daten der GPOs eingetragen. Zu verschiedenen Datentypen wie z.B. UNC-Pfaden oder globalen Gruppen ist jeweils der Wert der Quelle und des Ziels eingetragen. Mit Hilfe dieser Tabellen können die Werte des Quell-GPOs während des Kopier- oder Importvorgangs so konvertiert werden, dass sie für das Ziel-GPO nutzbar sind. Der Aufbau einer Migrationstabelle sieht folgendermaßen aus:

Datentyp	Wert der Quelle	Wert des Ziels
UNC-Pfad	\\Server1\Freigabe1	\\Server2\Freigabe2
Globale Gruppe	Domäne1\Gruppe1	Domäne2\Gruppe2

Tabelle 8.14: Aufbau einer Migrationstabelle

Angenommen, Sie möchten ein GPO von Domäne1 nach Domäne2 migrieren. In Domäne1 befindet sich die Sicherheitsgruppe Gruppe1. In Domäne2 gibt es hingegen nur die Gruppe2. Für diese Gruppe sind jedoch identische Sicherheitseinstellungen konfiguriert, sodass auch Gruppe2 das GPO benutzen soll. Wird für den Kopiervorgang keine Migrationstabelle verwendet, so beziehen sich die Sicherheitseinstellungen in Domäne2 auf Gruppe1, obwohl diese Gruppe in der Domäne nicht vorhanden ist. Die Sicherheitseinstellungen können also für Gruppe2 nicht greifen. Dieses Problem lässt sich auch dann nicht lösen, wenn in Domäne2 ebenfalls eine Gruppe1 vorhanden wäre. Der Grund dafür liegt darin, dass neben dem Namen der Gruppe auch deren eindeutige SID gespeichert wird – und die SIDs für eine Gruppe1 in Domäne1 und Domäne2 können nicht identisch sein. Bei lokalen Domänengruppen besitzt die Gruppe ohnehin nur Gültigkeit in der Quelldomäne und in keiner externen Domäne. Für Verweise auf die folgenden Bereiche von Sicherheitseinstellungen können die Migrationstabellen angepasst werden:

- Zuweisen von Benutzerrechten
- Eingeschränkte Gruppen
- Systemdienste
- Dateisystem
- Registry

Auch im GPO vorhandene UNC-Pfade bereiten Probleme, wenn die Werte nicht in einer Migrationstabelle angepasst werden. Dies gilt, wenn UNC-Pfade – z.B. Pfade zu den persönlichen Ordnern von Benutzern – nur in Domäne1 verfügbar sind, da sich Domäne2 in

einem anderen Netzwerksegment befindet. Diese umgeleiteten Ordner sind für die Benutzer in der Domäne2 nicht mehr erreichbar. UNC-Pfade können für die folgenden Bereiche über die Migrationstabellen angepasst werden:

- Einstellungen für die Ordnerumleitung
- Einstellungen für die Softwareinstallation, z.B. Softwareverteilungspunkte
- Verweise auf Skripte (z.B. An- und Abmeldeskripte), die außerhalb des GPO gespeichert sind. Die Skripte selbst werden nur dann zusammen mit dem GPO kopiert, wenn sie innerhalb des Quell-GPO gespeichert sind.

Mit dem Einsatz von Migrationstabellen werden die eben beschriebenen Probleme bereits während des Import- oder Kopiervorgangs behoben. Es wird automatisch im GPO nach Einstellungen gesucht, die z.B. den Wert \\Domäne1\Freigabe1 oder Domäne1\Gruppe1 enthalten. Diese Werte werden automatisch durch die Einträge \\Domäne2\Freigabe2 oder Domäne2\Gruppe2 ersetzt. Somit ist die Funktionsfähigkeit des GPO in der Zieldomäne gewährleistet.

Anwenden von Migrationstabellen

Sobald beim Kopieren oder Importieren (siehe Abbildung 8.40) eines GPO festgestellt wird, dass sich in diesem Verweise auf UNC-Pfade oder Bereiche der genannten Sicherheitseinstellungen befinden, wird eine Migrationstabelle verwendet. Für deren Einsatz gibt es drei verschiedene Optionen:

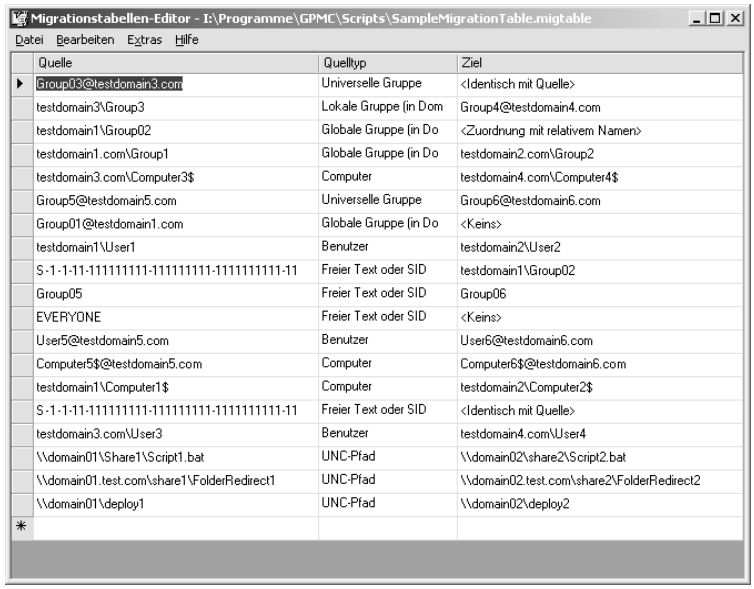
1. KEINE MIGRATIONSTABELLE VERWENDEN: In diesem Fall werden sämtliche Verweise – so wie sie sind – in das Ziel-GPO kopiert. Dann kann eine Funktionsfähigkeit des GPO in der Zieldomäne nicht gewährleistet werden.
2. EINE MIGRATIONSTABELLE VERWENDEN: Mit dieser Option werden alle Verweise des Quell-GPO auf die Werte umgesetzt, die für das Ziel-GPO in der Migrationstabelle festgelegt sind. Sind für einige Einträge keine Werte für die Zieldomäne angegeben, so werden die Werte des Quell-GPO übernommen.
3. EINE MIGRATIONSTABELLE EXKLUSIV VERWENDEN: Um diese Option nutzen zu können, müssen für alle Verweise des Quell-GPO Werte für das Ziel-GPO in der Migrationstabelle eingetragen sein. Ist dies nicht der Fall, wird der Kopier- bzw. Importvorgang nicht fortgesetzt. Mit dieser Option können Sie also immer sicherstellen, dass für alle Verweise der Wert umgesetzt wird.

Aufbau der Migrationstabellen

Bei den Migrationstabellen handelt es sich um XML-Dateien. Sie tragen die Dateierweiterung *.migtable*. In der GPMC ist der Migrationstabellen-Editor integriert. Die Anpassungen müssen also nicht in der XML-Datei vorgenommen werden. Um den Migrationstabellen-Editor zu öffnen, verwenden Sie eine der folgenden Möglichkeiten:

- Wählen Sie aus dem Kontextmenü des Containers GRUPPENRICHTLINIENOBJEKTE den Eintrag MIGRATIONSTABELLEN-EDITOR ÖFFNEN.
- Wählen Sie aus dem Kontextmenü des Containers DOMÄNEN den Eintrag MIGRATIONSTABELLEN-EDITOR ÖFFNEN.
- STARTEN SIE DAS PROGRAMM *mtedit.exe* IM GPMC-INSTALLATIONSVERZEICHNIS.
- Doppelklicken Sie eine bestehende .migtable-Datei.

Im Verzeichnis GPMC\Script befindet sich eine Beispieldatei einer Migrationstabelle. Öffnen Sie die Datei *SampleMigrationTable.migtable* mit dem Migrationstabellen-Editor (siehe Abbildung 8.41) oder einem Texteditor wie Notepad, um den XML-Code zu betrachten (siehe Listing 8.1).



Quelle	Quelltyp	Ziel
Group03@testdomain3.com	Universelle Gruppe	<Identisch mit Quelle>
testdomain3\Group3	Lokale Gruppe (in Dom	Group4@testdomain4.com
testdomain1\Group02	Globale Gruppe (in Do	<Zuordnung mit relativem Namen>
testdomain1.com\Group1	Globale Gruppe (in Do	testdomain2.com\Group2
testdomain3.com\Computer3$	Computer	testdomain4.com\Computer4$
Group5@testdomain5.com	Universelle Gruppe	Group6@testdomain6.com
Group01@testdomain1.com	Globale Gruppe (in Do	<Keins>
testdomain1\User1	Benutzer	testdomain2\User2
S-1-1-11-11111111-11111111-1111111111-11	Freier Text oder SID	testdomain1\Group02
Group05	Freier Text oder SID	Group06
EVERYONE	Freier Text oder SID	<Keins>
User5@testdomain5.com	Benutzer	User6@testdomain6.com
Computer5$@testdomain5.com	Computer	Computer6$@testdomain6.com
testdomain1\Computer1$	Computer	testdomain2\Computer2$
S-1-1-11-11111111-11111111-1111111111-11	Freier Text oder SID	<Identisch mit Quelle>
testdomain3.com\User3	Benutzer	testdomain4.com\User4
\\domain01\Share1\Script1.bat	UNC-Pfad	\\domain02\share2\Script2.bat
\\domain01.test.com\share1\FolderRedirect1	UNC-Pfad	\\domain02.test.com\share2\FolderRedirect2
\\domain01\deploy1	UNC-Pfad	\\domain02\deploy2

Abbildung 8.41: Der Aufbau einer Migrationstabelle im Migrationstabellen-Editor

Das folgende Listing zeigt den XML-Code einer Migrationstabelle. Als Beispiel wurde der Code für die Tabelle 8.14 verwendet.

```
<?xml version="1.0" encoding="utf-16"?>
<MigrationTable   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://
www.microsoft.com/GroupPolicy/GPOOperations/MigrationTable">
   <Mapping>
      <Type>GlobalGroup</Type>
      <Source>Domäne1\Gruppe1</Source>
      <Destination>Domäne2\Gruppe2</Destination>
   </Mapping>
   <Mapping>
      <Type>UNCPath</Type>
      <Source>\\Server1\Freigabe1</Source>
      <Destination>\\Server2\Freigabe2</Destination>
   </Mapping>
</MigrationTable>
```

Listing 8.1: XML-Code einer Migrationstabelle

In jeder Migrationstabelle befindet sich mindestens ein Eintrag. Für jeden dieser Einträge sind drei Angaben in den jeweiligen Spalten vorhanden: Quelle, Quelltyp und Ziel (siehe Abbildung 8.41).

Die Spalte QUELLE gibt den Namen der Quelle an, z.B. einen Gruppennamen oder UNC-Pfad, auf den im Quell-GPO verwiesen wird. Der Namenstyp, z.B. Benutzername, muss im Quell-GPO und mit dem in der Migrationstabelle angegebenen Ziel-GPO identisch sein. Die Namen können in einem der folgenden Formate angegeben werden:

- User Principal Name (UPN), z.B. user1@domäne.de
- DNS-Name, z.B. domäne.de\user1
- SAM, z.B. Domäne\user1
- Freier Text, z.B. user1. Unter QUELLTYP muss FREIER TEXT ODER SID eingetragen werden.
- SID, z.B. S-1-11-111111111-111111111-1111111111-1112. Unter QUELLTYP muss FREIER TEXT ODER SID eingetragen werden.

Der QUELLTYP bezeichnet die domänenspezifische Information des Quell-GPO. In die Migrationstabelle können die folgenden Quelltypen eingetragen werden:

- Benutzer
- Computer
- Lokale Domänengruppe
- Globale Domänengruppe
- Universelle Gruppe
- UNC-Pfad
- Freier Text oder SID (Diese Kategorie wird nur für Sicherheitsprincipals benutzt, die als pure SID oder Text vorliegen.)

In der Spalte ZIEL wird angegeben, wie der Name des Benutzers, der Gruppe, der UNC-Pfad usw. bei der Transferierung in das Ziel-GPO behandelt werden soll. Hierzu stehen vier Optionen zur Verfügung:

- Der Zielname entspricht dem Quellnamen: In diesem Fall wird im Ziel-GPO derselbe Verweis wie im Quell-GPO verwendet. Denselben Effekt erreichen Sie, wenn Sie gar keinen Wert angeben.
- <KEINS>: Hiermit wird der Benutzer, Computer oder die Gruppe aus dem GPO gelöscht. Diese Option kann jedoch nicht für UNC-Pfade benutzt werden.
- <ZUORDNUNG MIT RELATIVEM NAMEN>: Hierdurch wird z.B. aus dem Verweis Domäne1\Gruppe1 automatisch der Verweis Domäne2\Gruppe1. Anstelle der Domäne des Quell-GPO wird der Domänenname des Ziel-GPO gesetzt. Der Name des Benutzers, der Gruppe oder des Computers bleibt erhalten. Diese Option kann jedoch nicht für UNC-Pfade benutzt werden.
- Der Zielname wird explizit angegeben: In diesem Fall wird der Name des Quell-GPO durch den angegebenen Namen im Ziel-GPO ersetzt.

Erstellen einer Migrationstabelle

Für die Erstellung einer Migrationstabelle bietet Ihnen der Editor die Möglichkeit, die Tabelle automatisch mit den Werten eines GPO oder einer GPO-Sicherung auszufüllen.

1. Öffnen Sie zunächst eine leere Migrationstabelle, indem Sie aus dem Kontextmenü des Containers DOMÄNE oder GRUPPENRICHTLINIENOBJEKTE den Eintrag MIGRATIONSTABELLEN-EDITOR ÖFFNEN wählen.
2. Sie erhalten eine leere Tabelle mit den drei beschriebenen Spalten Quelle, Quelltyp und Ziel. Wählen Sie aus dem Menü EXTRAS den Eintrag VON GRUPPENRICHTLINIENOBJEKT AUFFÜLLEN oder VON SICHERUNG AUFFÜLLEN.
3. Wählen Sie dann das GPO oder die Sicherung des GPO aus, deren Verweise auf Sicherheitsprincipals und UNC-Pfade automatisch in die Tabelle in die Spalte QUELLE und QUELLTYP geschrieben werden sollen.
4. Für die Spalte ZIEL können Sie nun die gewünschten Einträge vornehmen.

   Nachdem Sie eine Migrationstabelle bearbeitet haben, sollten Sie die eingetragenen Werte überprüfen. Öffnen Sie dazu im Migrationstabellen-Editor das Menü EXTRAS/TABELLE VALIDIEREN. Das Fenster VALIDIERUNGSERGEBNISSE gibt Ihnen eine Zusammenfassung. Unter den Details sehen Sie Hinweise und Warnungen, bei welchen Tabelleneinträgen Probleme bei der Validierung aufgetreten sind.

Eine Migrationstabelle kann auch skriptgesteuert erstellt werden. Verwenden Sie hierzu das Skript *CreateMigrationTable.wsf*. Dabei wird die automatische Auffüllfunktion des Migrationstabellen-Editors benutzt. Die Werte für die neuen Pfade müssen danach manuell eingetragen werden.

8.6.19 Gruppenrichtlinienmodellierung und -ergebnisse

Über die Gruppenrichtlinienmodellierung der GPMC können Sie wie bereits bei Windows XP-Clients über das Resultant Set of Policy (RsoP), die Verteilung von Gruppenrichtlinien simulieren und die Ergebnisse der Gruppenrichtlinieneinstellungen ausgeben lassen. Um dieses Feature nutzen zu können, muss mindestens ein Domänencontroller in der Gesamtstruktur unter Windows Server 2003 ausgeführt werden. Andernfalls ist in der GPMC der Knoten GRUPPENRICHTLINIENMODELLIERUNG nicht verfügbar.

Um die Verteilung einer Gruppenrichtlinie und deren Auswirkungen zu simulieren, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des Knotens GRUPPENRICHTLINIENMODELLIERUNG den Eintrag GRUPPENRICHTLINIENMODELLIERUNGS-ASSISTENT.
2. Nach der Willkommensmeldung wählen Sie den Domänencontroller aus, auf dem die Simulation durchgeführt werden soll (siehe Abbildung 8.42). Hierbei muss es sich um einen Domänencontroller handeln, auf dem Windows Server 2003/SBS 2003 ausgeführt wird. Klicken Sie dann auf WEITER.

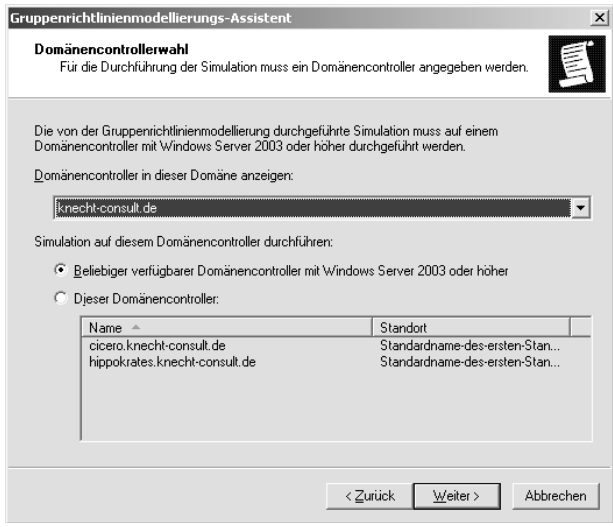


Abbildung 8.42: Auswahl des Domänencontrollers für die Simulation

3. Als Nächstes wählen Sie, ob die Richtlinien für einen bestimmten Benutzer und/oder Computer simuliert werden sollen oder für einen Container, in dem sich Benutzer-/Computerinformationen befinden (siehe Abbildung 8.43). Markieren Sie die gewünschte Checkbox und wählen dann den Container, den Benutzer oder den Computer aus. Klicken Sie dann auf WEITER.

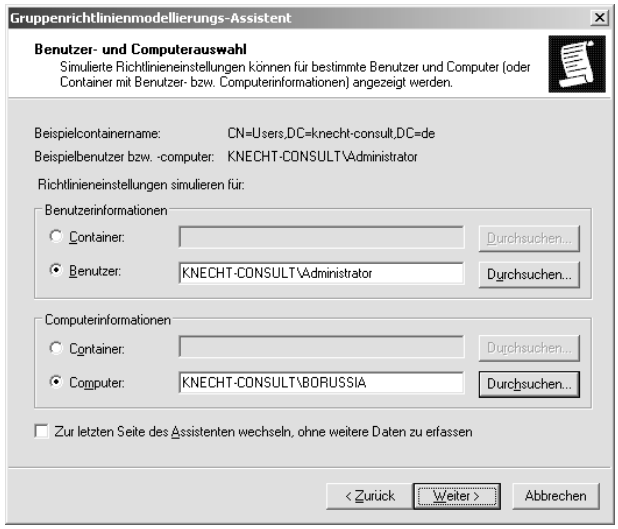


Abbildung 8.43: Auswahl des Benutzers oder Computers, für den die Richtlinie simuliert werden soll

4. Dann können Sie optional zusätzliche Simulationsparameter angeben (siehe Abbildung 8.44). Sie können eine langsame Netzwerkverbindung (DFÜ-Verbindung) simulieren. Auch die Loopback-Verarbeitung mit ihren Optionen ERSETZEN und ZUSAMMENFÜHREN (siehe Kapitel Abbildung 8.6.6) ist wählbar. Weiterhin können Sie einen bestimmten Standort für die Simulation wählen. Klicken Sie dann auf WEITER.

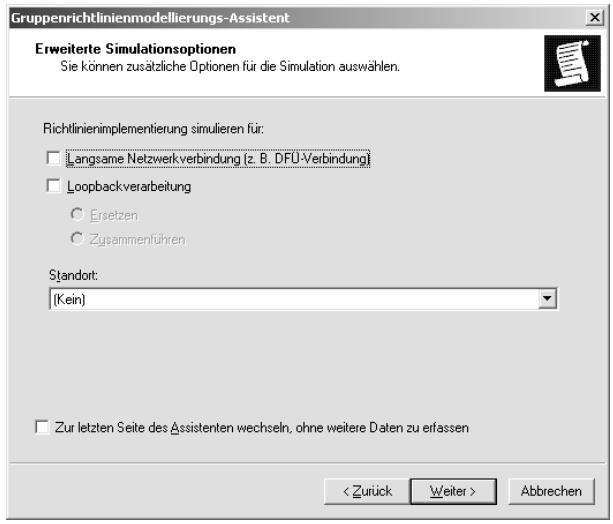


Abbildung 8.44: Angabe optionaler Simulationsparameter für die Gruppenrichtlinienmodellierung

5. Weiterhin können Sie alternative Active Directory-Pfade für den Benutzerstandort sowie den Computerstandort angeben. Für diese Einstellungen werden die Richtlinien simuliert. Klicken Sie dann auf WEITER.
6. Als Nächstes können Sie die Zugehörigkeit des gewählten Benutzers zu den Sicherheitsgruppen bestimmen. In der Liste SICHERHEITSGRUPPEN werden die aktuellen Zugehörigkeiten angezeigt. Über die Schaltflächen HINZUFÜGEN und ENTFERNEN können Sie die Mitgliedschaften modifizieren. Klicken Sie dann auf WEITER.
7. Wie im letzten Fenster für den Benutzer kann auch für den Computer die Gruppenzugehörigkeit bearbeitet werden. Klicken Sie dann auf WEITER.
8. Weiterhin können Sie WMI-Filter für die Benutzer auswählen, die mit dem GPO verknüpft werden sollen (siehe Abbildung 8.45). Sie haben die Möglichkeit, alle mit dem GPO verknüpften oder nur einzelne WMI-Filter zu wählen. Klicken Sie dann auf WEITER. Weitere Hinweise zu WMI-Filtern finden Sie in Kapitel Abbildung 8.6.21.
9. Auch für die Computer können WMI-Filter ausgewählt werden. Die Auswahl funktioniert genauso wie im letzten Schritt beschrieben. Klicken Sie dann auf WEITER.
10. Sie erhalten nun eine Zusammenfassung Ihrer Auswahl. Um die Gruppenrichtlinienmodellierung zu starten, klicken Sie hier auf WEITER und im folgenden Fenster auf FERTIG STELLEN.

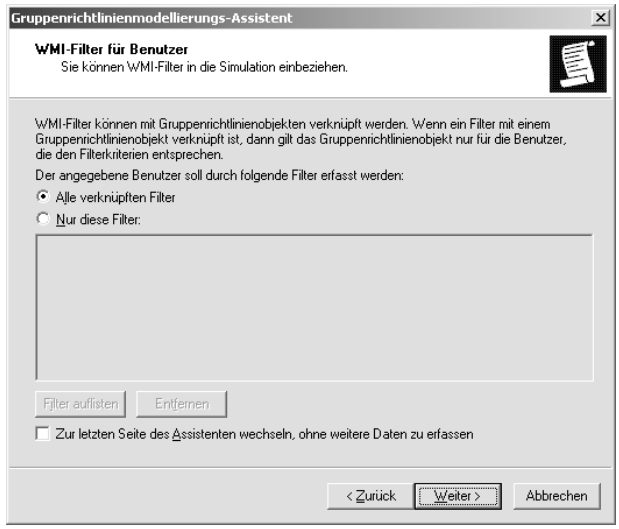


Abbildung 8.45: Auswahl von WMI-Filtern für die mit dem GPO verknüpften Benutzer

Nachdem Sie den Modellierungs-Assistenten beendet haben, befindet sich unter dem Knoten GRUPPENRICHTLINIENMODELLIERUNG ein neuer Eintrag. Der Knoten selbst zeigt auf der Registerkarte INHALT für alle vorhandenen Objekte Informationen über den verwendeten Domänencontroller, den gewählten Benutzer und Computer sowie das Durchführungsdatum an. Markieren Sie eines der Objekte, erhalten Sie die spezifischen Angaben zu diesem Objekt (siehe Abbildung 8.46). Die Registerkarte ZUSAMMENFASSUNG enthält einen HTML-basierten Bericht für die Benutzer- und Computerkonfiguration über die Gruppenmitgliedschaften, GPOs sowie WMI-Filter. Auf der Registerkarte EINSTELLUNGEN finden Sie einen HTML-Bericht über die simulierten Richtlinieneinstellungen. Die Registerkarte ABFRAGE enthält die Parameter, die Sie für die Generierung der Simulation eingegeben haben.

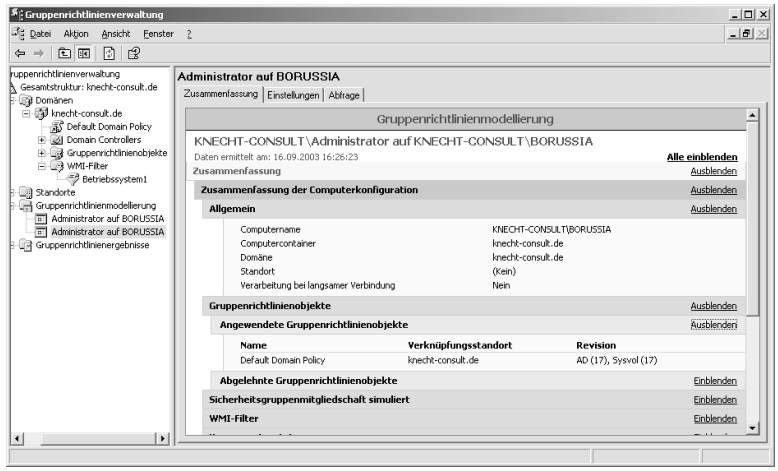


Abbildung 8.46: Die Gruppenrichtlinienmodellierung in der GPMC

Über das Kontextmenü des modellierten Objekts können Sie dieselbe Abfrage erneut ausführen, eine neue Abfrage erstellen, die auf dieser basiert, sowie einen Bericht erstellen.

Wählen Sie aus dem Kontextmenü den Eintrag ERWEITERTE ANSICHT, wird die mmc RICHTLINIENERGEBNISSATZ (RSoP) geöffnet. In dieser mmc sind dieselben Daten enthalten wie in dem HTML-Bericht.

Allerdings zeigt der HTML-Bericht nur den aktuellen Wert einer Richtlinie sowie das GPO, das diesen Wert setzt. Sind mehrere GPOs zugewiesen, so wird nur in der mmc RICHTLINIENERGEBNISSATZ die Liste aller GPOs sowie deren Verarbeitungsreihenfolge angezeigt.

Gruppenrichtlinienergebnisse

Die Gruppenrichtlinienergebnisse können nicht nur für Benutzer und Computer angezeigt werden, für die eine Gruppenrichtlinienmodellierung durchgeführt wurde, sondern auch für reale Benutzer und Computer. Es handelt sich hier also um reale Daten, die von einem vorhandenen Computer gesammelt werden. Es erfolgt keine Simulation auf einem Domänencontroller. Der Zielcomputer muss dafür unter Windows XP oder Windows Server 2003/SBS 2003 betrieben werden. Von Computern mit dem Betriebssystem Windows 2000 Professional/Server können keine Gruppenrichtlinienergebnisse bezogen werden.

Um Gruppenrichtlinienergebnisse vom Zielcomputer beziehen zu können, muss der Benutzer über lokale Administratorrechte für diesen Computer verfügen. Für die Delegierung von Richtlinienergebnisdaten ist es jedoch erforderlich, dass in der Gesamtstruktur das Windows 2003-Schema vorhanden ist. Benutzen Sie hierfür das Programm *ADPREP*. Ein Domänencontroller unter Windows Server 2003 ist nicht erforderlich.

Um Gruppenrichtlinienergebnisse anzuzeigen, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des Knotens GRUPPENRICHTLINIENERGEBNISSE den Eintrag GRUPPENRICHTLINIENERGEBNIS-ASSISTENT.
2. Klicken Sie bei der Willkommensmeldung auf WEITER. Danach wählen Sie den Computer aus, für den die Gruppenrichtlinienergebnisse angezeigt werden sollen. Sie können den aktuellen Computer oder einen beliebigen anderen auswählen. Wollen Sie für den Computer keine Richtlinienergebnisse anzeigen, so aktivieren Sie die Checkbox KEINE RICHTLINIENEINSTELLUNGEN FÜR DEN AUSGEWÄHLTEN COMPUTER IM ERGEBNIS ANZEIGEN. Klicken Sie dann auf WEITER.
3. Wählen Sie nun den Benutzer aus. Sie können den aktuellen oder einen anderen Benutzer wählen. Wollen Sie für den Benutzer keine Richtlinienergebnisse anzeigen, so aktivieren Sie die Checkbox KEINE BENUTZERRICHTLINIENEINSTELLUNGEN IM ERGEBNIS ANZEIGEN. Klicken Sie dann auf WEITER.
4. Sie erhalten eine Zusammenfassung Ihrer Einstellungen. Klicken Sie hier auf WEITER und dann auf FERTIG STELLEN.

   Der neu erstellte Richtlinienergebnissatz ist als neuer Knoten unter Gruppenrichtlinienergebnisse vorhanden. Standardmäßig trägt dieser Ergebnissatz den Namen im Format BENUTZERNAME AUF COMPUTERNAME. Er verfügt über die drei Registerkarten ZUSAMMENFASSUNG, EINSTELLUNGEN und RICHTLINIENEREIGNISSE. Die beiden Karten ZUSAMMENFASSUNG und EINSTELLUNGEN enthalten dieselben Informationen wie

unter der Gruppenrichtlinienmodellierung. Die Registerkarte RICHTLINIENEREIGNISSE (siehe Abbildung 8.47) enthält alle sicherheitsbezogenen Ereignisse (Informationen, Warnungen und Fehlermeldungen) des Ereignisprotokolls vom Zielcomputer. Hierzu muss der Benutzer über die Berechtigung verfügen, per Remote-Zugriff das Ereignisprotokoll lesen zu können. Unter Windows XP besitzen alle Benutzer diese Berechtigung, nicht jedoch unter SBS 2003 und Windows Server 2003.

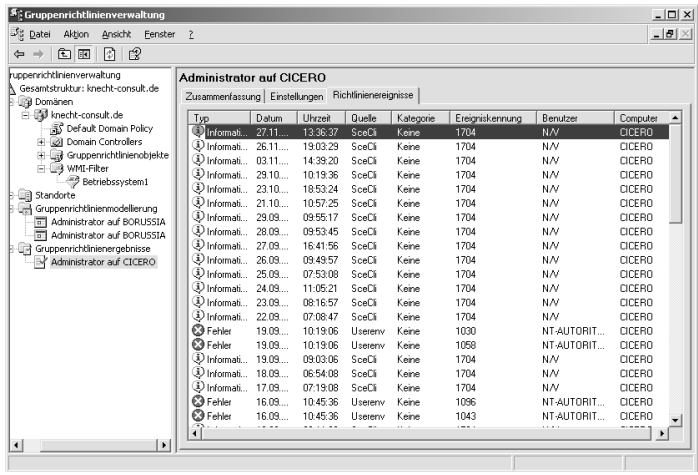


Abbildung 8.47: Die Richtlinienereignisse der Richtlinienergebnisse

8.6.20 Aufgabendelegierung

Da die Verwaltung der Gruppenrichtlinien ein sehr weites Feld ist, die nicht zwangsläufig von einer einzelnen Person allein durchgeführt werden muss, kann die Delegierung einzelner Teilaufgaben an weitere Personen erfolgen. So können Sie beispielsweise die Erstellung von GPOs, deren Verknüpfung und Bearbeitung oder die Gruppenrichtlinienmodellierung an bestimmte Personen delegieren. Die folgenden Abschnitte zeigen, wie die Delegierung für die wichtigsten Verwaltungsaufgaben durchgeführt wird. Je umfangreicher die GPO-Verwaltung wird, desto eher sollten Sie über die Delegierung von Aufgaben nachdenken

Erstellen von GPOs

Standardmäßig können alle Mitglieder der Sicherheitsgruppe Richtlinien-Ersteller-Besitzer GPOs erstellen. Sie können entweder weitere Benutzer zu dieser Gruppe hinzufügen oder direkt über die GPMC Benutzern und Gruppen diese Berechtigung erteilen. Da es sich bei der Gruppe Richtlinien-Ersteller-Besitzer um eine globale Domänengruppe handelt, konnten keine Benutzer hinzugefügt werden, die nicht der Domäne angehören. Sofern Sie die Benutzer über die GPMC hinzufügen, besteht dieses Problem nicht mehr. Öffnen Sie dazu in der GPMC die Registerkarte DELEGIERUNG des Knotens GRUPPENRICHTLINIENOBJEKTE und fügen neue Benutzer hinzu.

Sobald ein Benutzer die Berechtigung zum Erstellen von GPOs besitzt, ist er dennoch nicht in der Lage, bestehende GPOs zu bearbeiten oder löschen. Lediglich die von ihm erstellten können geändert und gelöscht werden.

Zugriff auf einzelne GPOs

Für jedes einzelne GPO können Sie Benutzern bestimmte Berechtigungen zuweisen. Öffnen Sie dazu die Registerkarte DELEGIERUNG des gewünschten GPO.

Tabelle 8.15 zeigt die verschiedenen Berechtigungen.

Berechtigung	Auswirkung
Lesen	Auf das GPO kann nur lesend zugegriffen werden.
Einstellungen bearbeiten	Erlaubt sind Lesen, Schreiben sowie das Erstellen und Löschen von untergeordneten Objekten.
Einstellungen bearbeiten, Löschen, Sicherheit verändern	Erlaubt sind Lesen, Schreiben, Löschen, Verändern der Berechtigungen, Übernahme des Besitzes sowie das Erstellen und Löschen von untergeordneten Objekten. Diese Berechtigung ermöglicht Vollzugriff auf das GPO.
Lesen (durch Sicherheitsfilterung)	Diese Berechtigung kann nicht direkt gesetzt werden. Sie wird lediglich für alle Benutzer angezeigt, die über die Leseberechtigung verfügen sowie in der Liste SICHERHEITSFILTERUNG auf der Registerkarte BEREICH des GPO angezeigt werden.
Benutzerdefiniert	Beliebige Kombinationen von Berechtigungen können zugewiesen werden. Über die Schaltfläche ERWEITERT wird der ACL-Editor für die erweiterten Berechtigungen gestartet.

Tabelle 8.15: Berechtigungen, die einem Benutzer für ein GPO zugewiesen werden können

Verknüpfen von GPOs

Damit die Einstellungen eines GPO wirksam werden, muss dieses mit einer Domäne, einem Standort oder einer OU verknüpft werden. Sie können Benutzern die Berechtigung erteilen, GPOs zu verknüpfen, die Verknüpfungsreihenfolge zu bearbeiten und die Vererbung von GPO-Einstellungen zu unterbrechen. Öffnen Sie dazu die Registerkarte DELEGIERUNG der gewünschten Domäne oder OU.

Gruppenrichtlinienmodellierung und Gruppenrichtlinienergebnisse

Die Berechtigung zur Gruppenrichtlinienmodellierung besitzen standardmäßig nur Domänenadministratoren, die Berechtigung zum Lesen der Gruppenrichtlinienergebnisse nur Benutzer mit lokalen Administratorrechten und Remote-Zugriff auf die Gruppenrichtlinienergebnisse.

Um diese Einstellungen zu ändern, öffnen Sie die Registerkarte DELEGIERUNG der gewünschten Domäne oder OU. Aus der Listbox BERECHTIGUNG wählen Sie entweder den Eintrag GRUPPENRICHTLINIENERGEBNISSE LESEN oder ANALYSEN ZUR GRUPPENRICHTLINIENMODELLIERUNG DURCHFÜHREN. Über die Schaltfläche HINZUFÜGEN können Sie weiteren Benutzern die gewünschte Berechtigung erteilen.

Alternativ können Sie die Berechtigungen auch über die Schaltfläche ERWEITERT direkt über den ACL-Editor zuweisen. Die Option GRUPPENRICHTLINIENERGEBNISSE LESEN entspricht der Berechtigung RICHTLINIENERGEBNISSATZ ERSTELLEN (PLANUNG) im ACL-Editor, die zweite Option der Berechtigung RICHTLINIENERGEBNISSATZ ERSTELLEN (PROTOKOLLIERUNG).

8.6.21 WMI-Filter

Über die GPMC können GPOs mit WMI-(Windows Management Instrumentation-)Filtern verknüpft werden. Über den WMI-Filter werden bestimmte Attribute vorgegeben, die der Zielcomputer erfüllen muss, damit das GPO angewendet wird. Treffen die Attribute nicht zu, wird das GPO nicht angewendet. Über WMI können Sie umfangreiche Inventarisierungsdaten zu Hard- und Software abfragen wie z.B. Angaben zu RAM, CPU, freiem Speicherplatz, installierten Treibern, Softwarekonfiguration usw. So ist es möglich, über eine Gruppenrichtlinie eine bestimmte Software nur an Clients zu verteilen, die z.B. mindestens über 128 MB RAM und 400 MB freien Speicherplatz verfügen.

WMI-Filter können lediglich für Windows XP sowie 2003 angewendet werden. Für Windows 2000 ist keine WMI-Filterung möglich, und das GPO wird grundsätzlich angewendet. Weiterhin muss in einer Domäne ein Domänencontroller unter SBS 2003/Windows Server 2003 vorhanden sein. Andernfalls wird in der GPMC der Knoten WMI-FILTER nicht angezeigt.

Jeder WMI-Filter beinhaltet mindestens eine Abfrage der Hard- bzw. Softwaredaten. Als Sprache für die Abfragen wird WQL (WMI Query Language) verwendet. Diese Sprache ist sehr eng mit SQL verwandt. Eine Abfrage wird immer für einen bestimmten WMI-Namensraum ausgeführt, der bei der Erstellung anzugeben ist. Standardmäßig handelt es sich um den Namensraum root\CIMv2. Ausführliche Hinweise zu WQL finden Sie unter

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wql_operators.asp.

Die Abfrage wird gegenüber dem Zielclient entweder als true oder false ausgewertet. Im Falle von true treffen die im Filter definierten Attribute zu, und das mit dem Filter verknüpfte GPO wird angewendet. Sie können pro GPO nur einen WMI-Filter anwenden. Ein WMI-Filter kann jedoch mit mehreren GPOs verknüpft werden. Die WMI-Filter werden domänenbasiert gespeichert. Ein GPO muss sich also immer in derselben Domäne befinden wie der WMI-Filter, mit dem es verknüpft werden soll.

Um einen neuen WMI-Filter zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie im Kontextmenü von WMI-FILTER auf NEU (siehe Abbildung 8.48) und dort auf die Schaltfläche HINZUFÜGEN. Soll ein GPO mit einem Filter verknüpft werden, so wählen Sie auf der Registerkarte BEREICH des GPO WMI-FILTERUNG. Dort wählen Sie den gewünschten Filter aus.

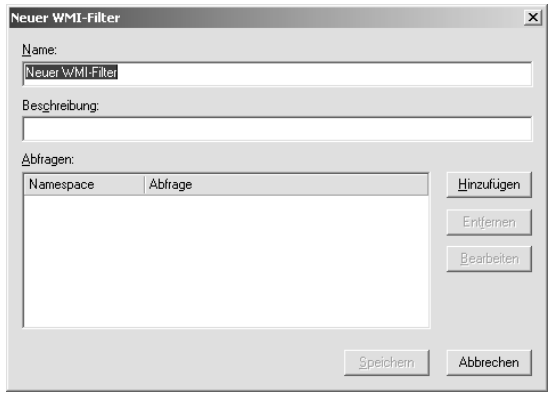


Abbildung 8.48: Erstellen eines neuen WMI-Filters

2. Angenommen, Sie möchten einen WMI-Filter für ein GPO erstellen, das nur bei Windows XP Professional angewendet wird, so verwenden Sie folgende Syntax (der Namensraum root\CimV2 ist bereits im Feld Namespace vorgegeben, siehe Abbildung 8.49):

   ```
   Select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP
   Professional"
   ```

Soll eine Softwareinstallation nur dann durchgeführt werden, wenn mindestens eine von zwei Applikationen bereits installiert ist, so verwenden Sie die folgende Syntax und bestätigen mit OK und klicken dann auf SPEICHERN.

```
Select * from Win32_Product where name = "MSIApplikation1" OR
"MSIApplikation2"
```

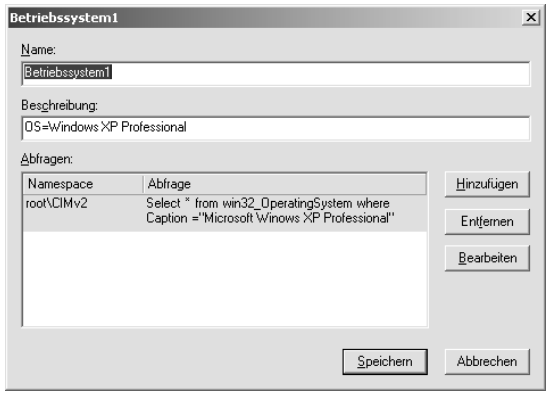


Abbildung 8.49: Erstellen einer Abfrage für einen WMI-Filter

Um den erstellten WMI-Filter mit einem GPO zu verknüpfen, öffnen Sie die Registerkarte BEREICH des GPO. Dort wählen Sie unten in der Sektion WMI-FILTER den gewünschten Filter aus. Bedenken Sie, dass jedes GPO mit nur einem WMI-Filter verknüpft sein kann.

Delegieren der WMI-Filter

Auch für WMI-Filter ist eine Delegierung der Verwaltung möglich. Es gibt zwei Typen von Zugriffsberechtigungen für WMI-Filter, nämlich Vollzugriff und Bearbeiten. Die Berechtigung Vollzugriff ist standardmäßig nur Domänen- und Unternehmens-Admins zugewiesen, die Berechtigung Bearbeiten den Erstellern des Filters. Mit dieser Berechtigung kann ein Benutzer neue WMI-Filter erstellen sowie die von ihm erstellten modifizieren und löschen. WMI-Filter, die von anderen Personen erstellt sind, können nicht geändert werden.

Um die Berechtigungen an weitere Personen zu delegieren, öffnen Sie die Registerkarte DELEGIERUNG des WMI-Filters. Über die Schaltfläche HINZUFÜGEN können Sie weitere Benutzer und Gruppen hinzufügen. Nachdem Sie den Benutzer ausgewählt haben, wählen Sie aus der Listbox BERECHTIGUNGEN die Option VOLLZUGRIFF oder BEARBEITEN aus.

8.6.22 Ordnerverwaltung über Gruppenrichtlinien

Über die Gruppenrichtlinien haben Sie die Möglichkeit, Ordner, die zum Benutzerprofil gehören, an eine zentrale Stelle im Netzwerk umzuleiten. Dazu zählen die Ordner Eigene Dateien, Eigene Bilder, Desktop, Startmenü und Anwendungsdaten, die sich standardmäßig auf der SYSTEMPARTITION\DOKUMENTE UND EINSTELLUNGEN\%BENUTZERNAME% befinden (bei einer Neuinstallation von Windows 2000/XP). Bei einer Aktualisierung von Windows NT befinden sie sich in %SYSTEMROOT%\PROFILE, bei einer Aktualisierung von Windows 9x in %SYSTEMROOT%\SYSTEM\PROFILE.

Insbesondere der Ordner Eigene Dateien kann im Laufe der Zeit sehr groß werden. Deshalb ist es sinnvoll, bei der Verwendung von servergespeicherten Profilen vor allem diesen Ordner umzuleiten. Wird dieser Ordner nicht umgeleitet, wird er als Teil des Profils bei jeder Benutzeranmeldung zwischen Client und Server hin- und herkopiert. Ist der Ordner umgeleitet, enthält das Profil lediglich den Verweis auf den umgeleiteten Speicherort des Ordners im Netzwerk. Werden alle Ordner sämtlicher Benutzer an einen zentralen Dateiserver weitergeleitet, wird damit auch die Sicherung der Daten vereinfacht, da nur ein einzelner Speicherort zu sichern ist. Auch wenn Sie kein servergespeichertes Benutzerprofil anwenden, können die Daten lokal von der Systempartition an eine andere lokale Festplatte weitergeleitet werden. Somit sind die Daten auch dann noch vorhanden, wenn eine Neuinstallation des Betriebssystems erforderlich wird.

1. Öffnen Sie das GPO des Standorts, der Domäne oder OU. Dieses GPO muss dem Benutzer zugewiesen sein, für den Sie die Ordnerumleitung konfigurieren möchten.
2. Öffnen Sie den Knoten BENUTZERKONFIGURATION/WINDOWS-EINSTELLUNGEN/ORDNERUMLEITUNG. Dort sehen Sie die vier Ordner ANWENDUNGSDATEN, DESKTOP, EIGENE DATEIEN (mit dem Unterordner EIGENE BILDER) sowie STARTMENÜ. Wählen Sie aus dem Kontextmenü des umzuleitenden Ordners EIGENSCHAFTEN. In unserem Beispiel wählen wir den Ordner EIGENE DATEIEN. Die Konfiguration der anderen Ordner erfolgt analog dazu.
3. Auf der Registerkarte ZIEL der Eigenschaften stehen Ihnen mehrere Einstellungsoptionen zur Verfügung. Sind bisher noch keine Einstellungen vorgenommen, befindet sich in der Listbox EINSTELLUNG die Angabe ES WURDEN KEINE ADMINISTRATORRICHTLINIEN ANGEGEBEN. Sie haben zu den Einstellungen die Wahl zwischen den Optionen

STANDARD – LEITET ALLE ORDNER AUF DEN GLEICHEN PFAD UM und ERWEITERT – GIBT PFADE FÜR VERSCHIEDENE BENUTZERGRUPPEN AN. Beide Optionen werden verschieden konfiguriert und deshalb getrennt beschrieben.

Standard – leitet alle Ordner auf den gleichen Pfad um

Bei diesem Verfahren werden für jeden Benutzer an einem Standort, einer Domäne oder OU die gewählten Ordner in einer bestimmten Freigabe auf einem Dateiserver gespeichert.

1. Wenn Sie sich für die Standardvariante entschieden haben, erhalten Sie folgendes Fenster (siehe Abbildung 8.50):

Abbildung 8.50: Die Standardeinstellung für die Ordnerumleitung

2. Wählen Sie über DURCHSUCHEN den Pfad des Ordners, an den der gewählte Ordner umgeleitet werden soll. Sie sollten dabei in jedem Fall mit der Variablen *%username%* arbeiten. Geben Sie beispielsweise den Pfad \\ARCHIMEDES\DATEN\%USERNAME%\EIGENE DATEIEN an, erhält jeder Benutzer seinen eigenen Ordner mit Unterordnern innerhalb der Freigabe auf dem Dateiserver. Der Pfad muss immer als UNC-Pfad angegeben werden.
3. Wechseln Sie dann auf die Registerkarte EINSTELLUNGEN. Standardmäßig sind dort bereits die Optionen DEM BENUTZER EXKLUSIVE ZUGRIFFSRECHTE FÜR EIGENE DATEIEN ERTEILEN sowie DEN INHALT VON EIGENE DATEIEN AN DEN NEUEN ORT VERSCHIEBEN aktiviert (siehe Abbildung 8.51). Sind die exklusiven Zugriffsrechte aktiviert, erhält lediglich der Benutzer selbst sowie das lokale System Vollzugriff auf den Ordner. Nicht einmal ein Administrator oder ein anderer Benutzer kann Änderungen an diesem Ordner vornehmen. Die zweite Option bewirkt, dass die Inhalte des ausgewählten Ordners in den umgeleiteten Zielordner verschoben und nicht mehr am ursprünglichen Speicherort vorgehalten werden.

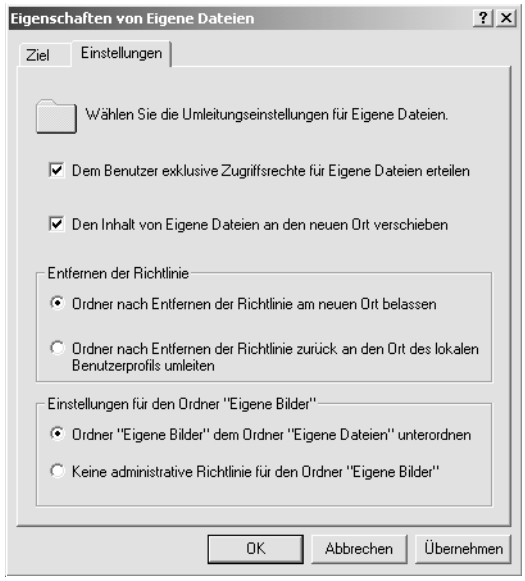


Abbildung 8.51: Die Einstellungen zur Ordnerumleitung

4. Weiterhin können Sie bestimmen, was mit dem umgeleiteten Ordner nach dem Entfernen der Richtlinie geschehen soll. Er kann dann entweder an seinem neuen Ort bleiben oder aber wieder lokal umgeleitet werden. Das Ergebnis dieser Einstellung ist abhängig von der Einstellung DEN INHALT VON EIGENE DATEIEN AN DEN NEUEN ORT VERSCHIEBEN auf dieser Registerkarte. Tabelle 8.16 gibt einen Überblick über die Effekte der Einstellungen.

Status der Einstellung Den Inhalt ... verschieben	Status von Entfernen der Richtlinie	Nach Entfernen der Richtlinie
Aktiviert oder deaktiviert	Ordner belassen	Der Ordner bleibt am umgeleiteten Ort; der Benutzer hat weiterhin Zugriff.
Aktiviert	Ordner umleiten	Der Ordner wird mit seinen Inhalten an den lokalen Ort des Benutzers kopiert, bleibt aber auch auf dem Server noch bestehen. Der Zugriff des Benutzers erfolgt aber nur noch auf die lokalen Dateien, nicht mehr auf die im Netzwerk.
Deaktiviert	Ordner umleiten	Der Ordner wird *ohne* seine Inhalte an den lokalen Speicherort kopiert. Werden die Inhalte nicht gesondert dorthin kopiert oder verschoben, hat der Benutzer keinen Zugriff mehr auf die Daten.

Tabelle 8.16: Einstellungen zum Entfernen einer Richtlinie

5. Lediglich für den Ordner Eigene Dateien finden Sie die Option für den Umgang mit dem Ordner Eigene Bilder. Dabei wird der Ordner Eigene Bilder dem Ordner Eigene Dateien untergeordnet. Vergeben Sie keine Richtlinie, wird Eigene Bilder nicht als Unterordner von Eigene Dateien umgeleitet. Damit Eigene Bilder der Umleitung von Eigene Dateien folgen kann, öffnen Sie im GPO den Pfad Benutzerkonfiguration/Windows-Einstellungen/Ordnerumleitung/Eigene Bilder. Wählen Sie aus den Eigenschaften den Eintrag DEM ORDNER EIGENE DATEIEN FOLGEN.

Erweitert – gibt Pfade für verschiedene Benutzergruppen an

Bei diesem Verfahren werden für jeden Benutzer die gewählten Ordner in einer bestimmten Freigabe auf einem Dateiserver gespeichert. Die Ordnerumleitung basiert dabei auf der Gruppenmitgliedschaft der Benutzer.

1. Wenn Sie sich für die erweiterte Variante entschieden haben, erhalten Sie folgendes Fenster (siehe Abbildung 8.52):

Abbildung 8.52: Erweiterte Einstellungen für die Ordnerumleitung

2. Klicken Sie auf HINZUFÜGEN. In der dann folgenden Dialogbox GRUPPE UND PFAD ANGEBEN wählen Sie die Sicherheitsgruppe aus, für die Sie einen bestimmten Zielordner einrichten möchten. Alternativ können Sie die Gruppe auch über DURCHSUCHEN auswählen. Geben Sie dann den Pfad zu der Freigabe ein, in welche die Ordner umgeleitet werden sollen. Arbeiten Sie mit der Variablen *%username%*, um für jeden Benutzer einen Ordner mit seinem Benutzernamen anzulegen. Der Pfad zur Freigabe sollte als UNC-Pfad angegeben werden.
3. Wechseln Sie dann auf die Registerkarte EINSTELLUNGEN des gewählten Ordners (siehe Abbildung 8.51). Die hier vorzunehmenden Einstellungen sind identisch mit den bereits dort beschriebenen.

Probleme bei der Ordnerumleitung unter Windows XP

Wenn Sie die eben beschriebene Ordnerumleitung auf einen Benutzer anwenden, der Windows XP Professional verwendet, kann das Problem auftreten, dass der Benutzer eine Warnmeldung über unzureichenden Speicherplatz erhält oder zumindest nur noch sehr wenig Speicherplatz verfügbar ist.

Dieses Problem liegt darin begründet, dass Windows XP Professional standardmäßig alle Inhalte der umgeleiteten Ordner lokal zwischenspeichert. Ist dabei der Inhalt der umgeleiteten Ordner größer als der lokal verfügbare Platz, kommt es zur Fehlermeldung. Ansonsten wird lokal die Größe der Freigabe belegt.

Um dieses Problem zu beheben, muss die standardmäßig nicht definierte Gruppenrichtlinie UMGELEITETE ORDNER NICHT AUTOMATISCH OFFLINE VERFÜGBAR MACHEN aktiviert werden. Um diese Richtlinie zu aktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das GPO, das auf den Benutzer angewendet wird, und wählen den Knoten BENUTZERKONFIGURATION/ADMINISTRATIVE VORLAGEN/NETZWERK/OFFLINE-DATEIEN.
2. Aktivieren Sie dort die Richtlinie UMGELEITETE ORDNER NICHT AUTOMATISCH OFFLINE VERFÜGBAR MACHEN.

8.7 Softwareverwaltung und -verteilung über Gruppenrichtlinien

Über die Gruppenrichtlinie können Sie nicht nur die Desktop-Umgebung Ihrer Clients verwalten, sondern den Benutzern auch Software zur Installation zuweisen. Diese Möglichkeit der Gruppenrichtlinien sollten Sie anwenden, sofern Ihr Unternehmen nicht bereits ein anderes Tool eines Drittanbieters zur Softwareverteilung einsetzt. Dieses Kapitel gibt Ihnen eine Übersicht über den theoretischen Planungsablauf. In den folgenden Kapiteln wird die praktische Umsetzung beschrieben.

Vor der Softwareverteilung sind verschiedene Punkte zu bedenken und zu klären. Den gesamten Prozess der Softwareverteilung kann man in vier große Abschnitte gliedern:

1. Vorbereitung
2. Quelle der Installation
3. Empfänger der Software
4. Installation

Vorbereitung

In der Vorbereitungsphase legen Sie allgemeine Punkte fest, die für jede Methode der Softwareverteilung gültig sind.

- Untersuchen Sie zunächst, welche Software momentan eingesetzt wird und welche davon an die Benutzer auch weiterhin verteilt werden soll.
- Unterteilen Sie diese Software in verbindliche und optionale Programme. Standardisieren Sie dadurch die Arbeitsplätze im Unternehmen.

- Ermitteln Sie weiter, bei welcher der Softwares es sich um reine Windows Installer-Pakete handelt, die direkt über die Gruppenrichtlinie zugewiesen werden können. Die Programme, die lediglich eine herkömmliche Setup-Routine bereitstellen, müssen für die Verteilung wieder gepackt werden. Im Lieferumfang von Windows 2000 Server befindet sich dafür das Programm *WinInstall LE* der Firma Veritas Software. Dieses Programm ist jedoch nicht mehr im Lieferumfang von Windows Server 2003/SBS 2003 enthalten, sondern kann direkt bei OnDemand-Software downgeloadet werden: *http://www.ondemandsoftware.com/freele.asp*.
- Legen Sie außerdem fest, ob bestimmte Anpassungen und Konfigurationen der Software für bestimmte Benutzer erforderlich sind. Ist es erforderlich, dass z.B. verschiedene Office-Versionen mit unterschiedlichen Features für verschiedene Einsatzbereiche gebildet werden? Weitere Hinweise dazu finden Sie in Kapitel 8.7.9.

Quelle der Installation

Als Nächstes müssen Sie festlegen, welche Computer die Softwareverteilungspunkte sein sollen, von denen aus die Softwarepakete auf den Clients installiert werden können. Hierbei müssen Sie anhand der eingesetzten Hardware selber entscheiden, ob Sie den SBS 2003 oder einen separaten Dateiserver verwenden möchten. Bestimmen Sie außerdem, ob Sie die Gruppenrichtlinie zur Softwareverteilung auf Standort- oder OU-Ebene anwenden wollen.

Empfänger der Software

Entscheiden Sie dann, ob die Software an einen Benutzer oder einen Computer verteilt werden soll. Bestimmen Sie dann die Benutzer und Computer, welche die Software erhalten sollen.

Die Softwareverteilung kann nicht bei Terminalserver-Clients durchgeführt werden.

Installation

Einem Benutzer können Sie Software zuweisen oder veröffentlichen/ankündigen, einem Computer nur zuweisen. Beim Zuweisen von Software wird diese bei der Benutzeranmeldung angekündigt. Die Installation erfolgt, wenn der Benutzer ein Dokument öffnet, das die Applikation erfordert, oder wenn er das entsprechende Icon im Startmenü oder auf dem Desktop anklickt. Die einem Benutzer zugewiesene Software wird auf jedem Arbeitsplatz installiert, unabhängig davon, an welchem Computer er sich anmeldet. Wird die Software einem Computer zugewiesen, wird die Installation beim Start des Computers durchgeführt. Unter SBS 2003 haben Sie auch die Möglichkeit, die komplette einem Benutzer zugewiesene Software bei dessen Anmeldung installieren zu lassen und nicht erst, wenn die Applikation das erste Mal benötigt wird. Dies bringt den Vorteil einer konsistenten Umgebung, da ab dem Zeitpunkt der Anmeldung alle Softwarepakete bereits vorhanden sind.

Das Veröffentlichen von Software funktioniert nur für Benutzer. Dabei werden jedoch keine Verknüpfungen auf dem Desktop oder im Startmenü angezeigt. Die bereitgestellte Software speichert ihre Informationen zur Veröffentlichung im Active Directory und nicht in der lokalen Registry des Computers. Die Applikation wird erst installiert, wenn der Benutzer eine Datei öffnet, welche die Applikation erfordert, oder wenn er unter SYSTEMSTEUERUNG/SOFTWARE die veröffentlichten Applikationen zur Installation auswählt.

Zur Installation der Softwarepakete verwendet die Softwareinstallation die systemimmanente Windows Installer-Technik. Im Zusammenhang mit der Windows Installer-Technologie sind die folgenden Dateiendungen wichtig:

- *.msi*: Die msi-Datei ist die zentrale Steuerungsdatei für das gesamte Setup einer Applikation, die den Windows Installer benutzt. Die Datei beinhaltet in einer Datenbankstruktur alle Features sowie entweder direkt die cab-Dateien, Kopieranweisungen etc. oder Verweise auf diese. Das Setup ruft intern den Befehl msiexec /i auf, wodurch das MSI-File gestartet wird. Eine Applikation kann auch mehrere MSI-Files enthalten, die sich während der Installation gegenseitig aufrufen. Diese Dateien können für ein Programm nativ vorliegen oder durch Repaketierung erzeugt worden sein.
- *.mst*: Die mst-Datei wird auch Transform-File genannt. Hierbei handelt es sich um eine Datei, die ein bearbeitetes Feature-Set für eine Applikation enthält. Eine solche Datei wird z.B. für Office 2000 über das Office Resource Kit erstellt. Das Erstellen eines MST-Files ist optional. Wenn Sie einer msi-Datei kein Transform-File hinzufügen, werden auf dem Client die Features installiert, die bei einer Standardinstallation von Hand auch ausgewählt werden.
- *.msp*: Hierbei handelt es sich um Patch-Dateien oder Service Pack-Dateien für eine Applikation, die den Windows Installer benutzt. Ein Beispiel hierfür ist das Office 2000 SR-1A oder SP2.
- *.ass*: Application Assignment Scripts. Diese Skripte enthalten spezielle Befehle für die Veröffentlichung oder Zuweisung eines bestimmten Softwarepakets.

Weitergehende Details zur Funktionsweise der Windows Installer-Technologie und den speziellen Pakettypen finden Sie in Kapitel 8.7.7.

Außerdem müssen Sie sich eine Strategie überlegen, wie die Software auf dem Arbeitsplatz aktualisiert oder deinstalliert werden kann. Testen Sie danach die Verteilung der Pakete daraufhin, ob alle Ihre Anforderungen erfüllt werden konnten.

8.7.1 Einrichten des Softwareverteilungspunktes und administratives Setup

Zunächst muss für die Applikation ein Softwareverteilungspunkt (SDP = Software Deployment Point) definiert werden.

1. Erstellen Sie auf einem Dateiserver oder dem SBS eine Freigabe, in der sämtliche Unterordner für die zu installierenden Applikationen angelegt werden. Für die Freigabe des SDP müssen Sie für die Benutzer die Berechtigung Lesen vergeben, die von dort aus die Software installieren sollen. Administratoren erhalten Lese- und Schreibrechte, damit diese auch Änderungen an den Softwarepaketen vornehmen können.

2. Für jede Applikation müssen Sie einen separaten Ordner anlegen, der alle notwendigen Installationsdateien, also die .msi-Datei sowie optionale .mst- oder .msp-Dateien, enthält.
3. Kopieren Sie nun in diesen Ordner alle Komponenten, die zur Applikation gehören.

Administratives Setup

Einige Applikationen können auch über das administrative Setup direkt in den SDP installiert werden. Im folgenden Beispiel wird das administrative Setup für Office 2003 beschrieben. Der Vorgang des administrativen Setups besteht im Wesentlichen aus dem Kopieren des CD-Inhalts in den SDP. Dabei haben Sie die Möglichkeit, das Paket mit dem CD-Schlüssel und dem Firmennamen zu personalisieren. Beim administrativen Setup sind die folgenden Schritte auszuführen:

1. Legen Sie die Office 2003-CD ins Laufwerk. Die CD sollte automatisch starten. Es erscheint die Willkommensseite. Brechen Sie hier den Installationsprozess ab und wechseln zur Eingabeaufforderung.
2. Wechseln Sie dort als aktuelles Laufwerk zum CD-Laufwerk und geben folgenden Befehl ein:

```
Setup.exe /a data1.msi shortfilenames=true
```

Es könnten bei anderen Applikationen noch weitere MSI-Files auf der CD vorhanden sein, die data2.msi, data3.msi usw. heißen. Wenn Sie ein administratives Setup für eines dieser MSI-Files erstellen, ersetzen Sie den Namen für data1.msi in der Kommandozeile entsprechend.

Der Parameter /a fordert den Windows Installer auf, das administrative Setup anstatt einer normalen Installation durchzuführen.

Der Parameter shortfilenames=true zwingt den Windows Installer dazu, kurze Dateinamen zu speichern. Damit ist die Kompatibilität zu verschiedenen Plattformen sichergestellt.

Einige CDs des MSDN unterstützen nicht den o.g. Befehl für das administrative Setup. Verwenden Sie stattdessen folgenden Befehl:

```
msiexec /a data1.msi shortfilenames=true
```

3. Nach der Eingabe dieses Befehls erscheint die grafische Oberfläche des administrativen Setups.
4. Geben Sie hier den CD-Schlüssel sowie den Namen der Organisation an. Klicken Sie auf WEITER.
5. Sie sehen nun das Fenster mit dem Endbenutzer-Lizenzvertrag (siehe Abbildung 8.53). Sie müssen hier die Checkbox zum Einverständnis aktivieren. Ansonsten können Sie die Installation nicht fortsetzen. Klicken Sie dann auf WEITER.

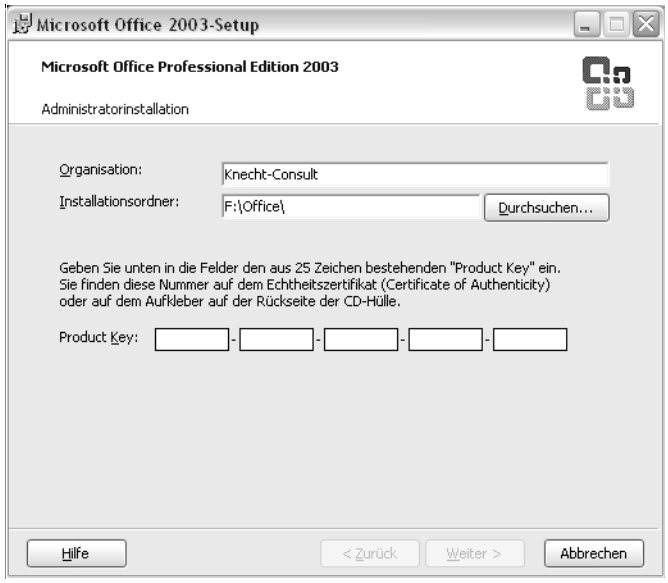


Abbildung 8.53: Das administrative Setup für Office 2003

6. Sie müssen nun den Pfad zur Freigabe des SDP als Zielort des administrativen Setups angeben. Klicken Sie danach auf JETZT INSTALLIEREN. Dieser Vorgang kann eine Weile dauern, da fast der gesamte CD-Inhalt auf die Platte kopiert werden muss. Eine Statusanzeige informiert Sie über den Fortschritt.
7. Markieren Sie nun alle Objekte und heben über das Kontextmenü EIGENSCHAFTEN den Schreibschutz auf.

Damit ist das administrative Setup abgeschlossen. Es befinden sich im SDP alle Dateien der Office 2003-CD. Wird nun eine Installation ausgeführt, erfolgt diese mit den Einstellungen des standardmäßigen Setups. Sollen zusätzlich benutzerdefinierte Setup-Einstellungen benutzt werden, so ist das Erstellen einer *.mst*-Datei erforderlich. Dieses Verfahren wird in Kapitel Abbildung 8.7.9 kurz beschrieben.

8.7.2 Festlegen der Installationsoptionen

Nachdem Sie serverseitig die Applikation bereitgestellt haben, beginnen die Einstellungen am GPO. Öffnen Sie dazu in der Benutzer- oder Computerkonfiguration des GPO den Knoten SOFTWAREEINSTELLUNGEN/SOFTWAREINSTALLATION und wählen aus dem Kontextmenü EIGENSCHAFTEN. Auf der Registerkarte ALLGEMEIN (siehe Abbildung 8.54) legen Sie Optionen für die Pakete fest.

Im Feld STANDARDPFAD FÜR PAKETE geben Sie den Pfad zu den Ordnern der jeweiligen *.msi*-Datei der Applikation an. Im Abschnitt NEUE PAKETE stehen Ihnen vier Möglichkeiten für das Hinzufügen neuer Pakete zu den Benutzereinstellungen zur Wahl.

Abbildung 8.54: Die Optionen zur Softwareinstallation

1. BEREITSTELLUNGSDIALOG ANZEIGEN bewirkt, dass das Dialogfeld SOFTWARE BEREITSTELLEN angezeigt wird (siehe Abbildung 8.55), wenn ein neues Paket zu den Benutzereinstellungen hinzugefügt wird. Dadurch können Sie die Eigenschaften des Pakets bearbeiten oder es zuweisen bzw. veröffentlichen.
2. VERÖFFENTLICHEN: Diese Option ist nicht verfügbar, wenn die Softwareeinstellungen der Computerkonfiguration geöffnet sind. Ein Softwarepaket wird nur mit den standardmäßigen Eigenschaften des Pakets veröffentlicht.
3. ZUWEISEN bedeutet, dass das Paket mit seinen standardmäßigen Eigenschaften einem Benutzer oder Computer zugewiesen wird.
4. ERWEITERT VERÖFFENTLICHT ODER ZUGEWIESEN bewirkt, dass beim Zuweisen oder Veröffentlichen eines Pakets das Dialogfeld PAKETEIGENSCHAFTEN KONFIGURIEREN angezeigt wird.

Im Bereich BENUTZEROBERFLÄCHENOPTIONEN FÜR DIE INSTALLATION können Sie festlegen, ob der Benutzer bei der Installation nur die standardmäßigen (Option EINFACH) oder alle Installationsfenster (Option MAXIMUM) erhalten soll. Eine Installation im Hintergrund (Silent Installation) von Software ist hier nicht vorgesehen.

Aktivieren Sie die Checkbox ANWENDUNGEN DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGEN, so wird die Anwendung deinstalliert, wenn das betreffende GPO nicht mehr auf den Computer oder Benutzer angewendet wird.

8.7.3 Zuweisen und Veröffentlichen von Paketen

Um eine Applikation zuzuweisen oder zu veröffentlichen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie im GPO in der Benutzer- oder Computerkonfiguration den Knoten SOFTWAREEINSTELLUNGEN/SOFTWAREINSTALLATION. Wählen Sie aus dem Kontextmenü NEU/PAKET.
2. Im Dialogfeld ÖFFNEN sehen Sie den Inhalt des Ordners, den Sie als Standardpfad zu den Applikationen ausgewählt haben (siehe Abbildung 8.54). Öffnen Sie den Ordner der gewünschten Applikation und wählen die gewünschte *.msi*-Datei aus. In unserem Beispiel handelt es sich um die Data1.msi der Applikation Office 2003.
3. Da Sie als Standardmethode für die Bereitstellung neuer Pakete den Bereitstellungsdialog (siehe Abbildung 8.54) gewählt haben, erhalten Sie nun das Dialogfeld SOFTWARE BEREITSTELLEN (siehe Abbildung 8.55).

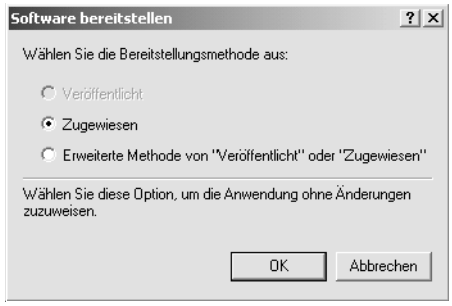


Abbildung 8.55: Das Dialogfeld SOFTWARE BEREITSTELLEN

4. Sie haben hier die Auswahlmöglichkeiten VERÖFFENTLICHT (nicht in der Computerkonfiguration), ZUGEWIESEN und ERWEITERTE METHODE VON VERÖFFENTLICHT UND ZUGEWIESEN. Wählen Sie eine der beiden ersten Optionen, wenn Sie die Anwendung ohne weitere Änderungen in der Standardkonfiguration zuweisen möchten. Wählen Sie die dritte Methode, erhalten Sie das Dialogfenster EIGENSCHAFTEN VON (NAME DER APPLIKATION) (siehe Abbildung 8.56). Hier können Sie beispielsweise auf der Registerkarte ÄNDERUNGEN Transform-Files auf die Standardkonfiguration anwenden.

Diese Änderungen müssen sofort an dem Paket vorgenommen werden, bevor es erstmalig veröffentlicht oder zugewiesen wird, da bei der erstmaligen Installation die Transform-Files abgearbeitet werden und nicht mehr nachträglich. Bevor nicht alle *.mst*-Dateien zugeordnet sind, dürfen Sie nicht auf OK klicken. Ansonsten müssen Sie später entsprechende Aktualisierungen zuweisen.

Die folgende Tabelle gibt eine kurze Zusammenfassung über die Unterschiede zwischen veröffentlichten und zugewiesenen Applikationen in Bezug auf Verfügbarkeit, Installation usw.

Kriterium	An Computer zugewiesene Applikation	An Benutzer zugewiesene Applikation	Veröffentlichte Applikation
Verfügbarkeitszeitpunkt des Pakets	Nächster Start des Computers	Nächste Anmeldung des Benutzers	Nächste Anmeldung des Benutzers
Installationsmethode	Automatische Installation	Installation über Verknüpfung in Startmenü oder Desktop	Applikation kann über SYSTEMSTEUERUNG/SOFTWARE gewählt werden.
Deinstallationsmöglichkeit für den Benutzer	Keine; nur mit lokalen Administratorrechten	Deinstallation und Neuinstallation möglich	Deinstallation möglich; kann über SYSTEMSTEUERUNG/SOFTWARE jederzeit neu installiert werden.

Tabelle 8.17: Unterschiede zwischen zugewiesener und veröffentlichter Software

5. Nachdem Sie die gewünschte *.msi*-Datei ausgesucht haben, wird das Paket erstellt. Sie sehen nun die Eigenschaftsseite des Pakets (siehe Abbildung 8.56). Bestätigen (oder ändern) Sie dann den vorgegebenen Namen des Pakets. Für Office 2000 lautet dieser *Microsoft Office 2000 Professional*.

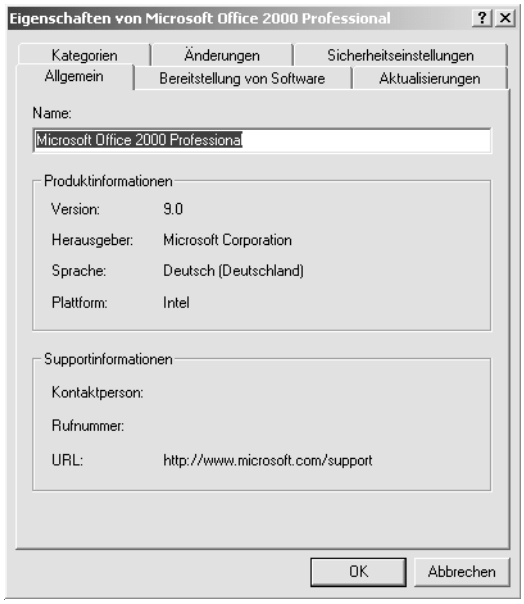


Abbildung 8.56: Die Eigenschaften eines Installationspakets

8.7.4 Allgemeine Einstellungen an den Applikationspaketen

Als Nächstes legen Sie nun noch einige allgemeine Einstellungen für die Pakete fest. Dazu zählen die mit den einzelnen Applikationen verknüpften Dateitypen sowie das Zusammenfassen der Applikationen in bestimmte Anwendungskategorien. Um diese beiden Einstellungen vorzunehmen, öffnen Sie den Knoten SOFTWAREEINSTELLUNGEN/SOFTWAREINSTALLATION in der Benutzer- bzw. Computerkonfiguration und öffnen über das Kontextmenü dessen EIGENSCHAFTEN.

Registerkarte Dateierweiterungen

Sie haben die Möglichkeit, bestimmten Dateitypen Anwendungen zuzuweisen, die innerhalb des GPO bereitgestellt sind, die automatisch installiert werden, wenn der Benutzer eine Datei mit einer derartigen Endung anklickt. Werden über ein GPO mehrere Applikationen bereitgestellt, die den jeweiligen Dateityp öffnen können, so können Sie auch die Priorität für die Installation dieser Applikationen treffen.

Auf der Registerkarte DATEIERWEITERUNGEN sehen Sie eine Liste aller vorhandenen Pakete (siehe Abbildung 8.57). Wählen Sie nun aus der Listbox DATEIERWEITERUNG AUSWÄHLEN die gewünschte Dateiendung aus. Sobald der Benutzer ein Dokument mit der gewählten Dateiendung öffnet, wird die gewählte Applikation ausgeführt.

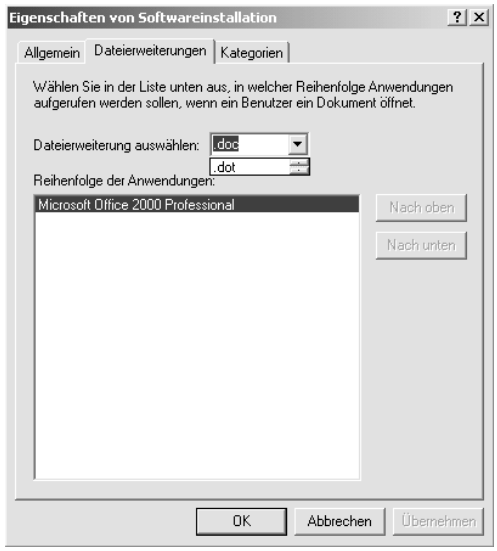


Abbildung 8.57: Die Dateierweiterungen bestimmen, die mit einer Applikation verknüpft sind

Sind mehrere Pakete in dem GPO vorhanden, können Sie über die Schaltflächen NACH OBEN und NACH UNTEN festlegen, welche Applikation automatisch installiert werden soll.

Sie müssen zwar diese Einstellungen nicht treffen, es ist aber in jedem Fall sinnvoll, dies zu tun, da der Benutzer sonst beim Öffnen eines unbekannten Dateityps das Dialogfeld ÖFFNEN MIT erhält. Dabei müsste er dann aus den auf dem Computer bereits vorhande-

nen Programmen eines auswählen, mit dem die Datei geöffnet werden soll. Dies kann jedoch schnell zu Problemen führen, wenn er nicht weiß, welches Programm für welche Dateien geeignet ist, oder noch kein kompatibles Programm installiert ist.

Diesen ÖFFNEN MIT-Dialog erhalten alle Benutzer, für die Applikationen nur veröffentlicht wurden, denen diese aber nicht zugewiesen sind, sofern nicht für sie eine automatische Installation festgelegt ist.

Registerkarte Kategorien

Auf der Registerkarte KATEGORIEN können Sie für die Applikationspakete Kategorien anlegen, in denen sie zusammengefasst werden. Unter diesen Oberkategorien finden die Benutzer ihre veröffentlichten Applikationen unter SYSTEMSTEUERUNG/SOFTWARE. Sie können zur Übersichtlichkeit Kategorien wie Office-Pakete, Grafiksuiten oder Utilities einrichten.

Um eine neue Kategorie einzurichten, klicken Sie auf HINZUFÜGEN und geben einen Namen ein. Über ENTFERNEN können nicht mehr benötigte Kategorien wieder gelöscht werden.

Die hier erstellten Kategorien gelten für die gesamte Domäne und nicht nur für das aktuelle GPO. Somit müssen diese Oberkategorien nur ein einziges Mal festgelegt werden.

8.7.5 Bearbeiten und Entfernen von Applikationspaketen

Nachdem Sie ein Paket für die Verteilung bereitgestellt und die allgemeinen Paketoptionen konfiguriert haben, können Sie nun zu jedem einzelnen Paket spezielle Eigenschaften einstellen. Dazu zählen etwa das Zuweisen zu Kategorien, Aktualisierungs- und Deinstallationseinstellungen oder die Sicherheitseinstellungen.

Wenn Sie die Eigenschaften eines vorhandenen Applikationspaketes öffnen, finden Sie die sechs Registerkarten ALLGEMEIN, BEREITSTELLUNG VON SOFTWARE, AKTUALISIERUNGEN, KATEGORIEN, ÄNDERUNGEN und SICHERHEITSEINSTELLUNGEN.

Registerkarte Allgemein

Hier sehen Sie die allgemeine Zusammenfassung (siehe Abbildung 8.56) mit Informationen wie Versionsnummer, Herausgeber oder Sprache des Applikationspaketes.

Registerkarte Bereitstellung von Software

Hier können Sie die Optionen für die Bereitstellung von Software einstellen oder Änderungen gegenüber der Standardeinstellung (siehe Abbildung 8.55) vornehmen. Sie können hier zwischen VERÖFFENTLICHT und ZUGEWIESEN umschalten.

Im Bereich BEREITSTELLUNGSOPTIONEN können Sie Eigenschaften der Installation und Bereitstellung festlegen. Dabei ist die erste Option AUTOMATISCH INSTALLIEREN, WENN DIE DATEIERWEITERUNG AKTIVIERT WIRD bereits aktiviert (und kann auch nicht deaktiviert werden), wenn Sie, wie in Kapitel 8.7.4 beschrieben, bestimmte Dateierweiterungen mit festen Applikationen verknüpft haben.

Mit der Option DIESE ANWENDUNG DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGT bestimmen Sie, ob eine Applikation deinstalliert werden soll, wenn sich der Computer bzw. Benutzer an einem Standort oder einer Domäne bzw. OU befindet, für die das GPO mit dieser Applikation nicht zugewiesen wurde. Die Deinstallation erfolgt in diesem Fall beim Computerstart oder bei der Benutzeranmeldung.

Über DIESES PAKET IN DER SYSTEMSTEUERUNG UNTER SOFTWARE NICHT ANZEIGEN können Sie dort ein Paket verbergen, das der Benutzer nicht selbstständig installieren soll.

Im Bereich BENUTZEROBERFLÄCHEN FÜR DIE INSTALLATION geben Sie an, ob der Benutzer nur die standardmäßigen (z.B. Zielpfad) oder alle Fenster und Dialoge während der Installation sehen darf.

Über die Schaltfläche ERWEITERT können Sie festlegen, ob die Spracheinstellungen ignoriert werden sollen oder nicht. Wenn Sie beispielsweise ein deutsches Windows-Betriebssystem verwenden, können Sie für ein englischsprachiges Applikationspaket bestimmen, ob dieses trotz der Sprachdiskrepanz bereitgestellt werden soll oder nicht. Ferner können Sie angeben, was mit einer Applikation geschehen soll, die bereits auf dem Computer installiert ist, aber nicht durch die Gruppenrichtlinie zugewiesen wurde. Diese Applikationen können deinstalliert werden.

Diese Einstellung gilt jedoch nur, wenn Sie z.B. Office 2000 bereits früher per Hand installiert haben und dasselbe Produkt nun zuweisen. Sie haben nicht die Möglichkeit, andere bereits vorhandene unerwünschte Software zu deinstallieren wie z.B. Moorhühner.

Registerkarte Aktualisierungen

In dieser Sektion konfigurieren Sie die Optionen für die Aktualisierung oder Deinstallation des Applikationspaketes. Bei einem Aktualisierungspaket handelt es sich entweder um eine neuere Version der Applikation oder um eine Applikation, welche die bisher verwendete ersetzen soll. So kann Office 2000 durch die neuere Version von Office XP ersetzt werden. Das Aktualisierungspaket wird, wie in Kapitel 8.7.1 und 8.7.2 beschrieben, im Active Directory bereitgestellt. Um ein Aktualisierungspaket hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus der Liste der Pakete unter SOFTWAREINSTALLATION in der mmc das Paket aus, das zur Aktualisierung dienen soll – *nicht das zu aktualisierende Paket*. Wählen Sie aus dessen Eigenschaften die Registerkarte AKTUALISIERUNGEN.
2. Klicken Sie nun auf HINZUFÜGEN, um das Aktualisierungspaket dem ursprünglichen Paket hinzuzufügen. Sie erhalten das Fenster AKTUALISIERUNGSPAKET HINZUFÜGEN. Wählen Sie hier aus, ob sich das zu aktualisierende Paket im aktuellen oder in einem anderen GPO befindet. Befindet es sich in einem anderen GPO, wird dieses über DURCHSUCHEN ermittelt. Sie sehen in der Liste ZU AKTUALISIERENDES PAKET alle im GPO vorhandenen Applikationspakete.
3. Markieren Sie das gewünschte Paket. Entscheiden Sie dann, was bei der Installation der Aktualisierung mit dem ursprünglichen Paket geschehen soll. Aktivieren Sie dazu die Checkbox BESTEHENDES PAKET DEINSTALLIEREN, AKTUALISIERUNGSPAKET INSTALLIEREN oder PAKET ÜBER DAS BESTEHENDE PAKET AKTUALISIEREN. Die erste

Option ist zu wählen, wenn Sie ein komplett neues Programmpaket eines anderen Herstellers installieren möchten. Diese Option wäre zu wählen, wenn Sie alle Microsoft Office-Anwendungen etwa durch eine Version von Star Office ersetzen möchten. Die zweite Option ist zu wählen, wenn das vorhandene Paket durch eine neuere Version derselben Anwendung ersetzt werden soll. Sie können so Office 2000 durch Office XP aktualisieren. Es bleiben dabei alle Einstellungen der Anwendung erhalten. Klicken Sie dann auf OK.

4. Aktivieren Sie dann auf der Registerkarte AKTUALISIERUNGEN die Checkbox BESTEHENDE PAKETE AKTUALISIEREN. Damit ist der Aktualisierungsvorgang verbindlich und wird ab sofort für alle Benutzer und Computer angewendet.

Registerkarte Kategorien

Wie bereits in Kapitel 8.7.4 beschrieben, sollten Sie aus Gründen der Übersichtlichkeit Kategorien für die Applikationen einrichten. Sie können hier nun aus der Liste VERFÜGBARE KATEGORIEN die passende auswählen und der Applikation über AUSWÄHLEN zuweisen. Sie können zwar mehrere Kategorien zu einer Applikation zuweisen, aber dadurch könnte die Einteilung wieder undurchsichtig werden, wenn der Benutzer dieselbe Applikation in verschiedenen Kategorien findet.

Registerkarte Änderungen

Diese Registerkarte wird bereits geöffnet, wenn Sie bei der Bereitstellung der Software die Option ERWEITERTE METHODE VON VERÖFFENTLICHT ODER ZUGEWIESEN wählen (siehe Abbildung 8.55). Hier weisen Sie den standardmäßigen Einstellungen der Windows Installer-Pakete Konfigurationsänderungen über *.mst*-Dateien (Transform-Files) zu. Weitere Hinweise zu *.mst-Dateien sowie ein Beispiel für deren Erstellung finden Sie in Kapitel 8.7.9.

Die Änderungen, die über die *.mst*-Dateien vorgenommen werden, müssen bereits bei der Bereitstellung des Pakets konfiguriert werden. Sie müssen konfiguriert sein, bevor das Paket zugewiesen oder veröffentlicht wird.

1. Um Änderungen für ein standardmäßiges Paket zu erstellen, wählen Sie aus dem Kontextmenü aus der Softwareinstallation den Menüpunkt NEU/PAKET. Wählen Sie aus der Liste der vorhandenen Windows Installer-Pakete die gewünschte *.msi*-Datei aus und klicken auf ÖFFNEN.
2. Wählen Sie im Dialogfeld SOFTWARE BEREITSTELLEN die dritte Option aus. Wählen Sie dann im Dialogfeld EIGENSCHAFTEN VON (APPLIKATIONSNAME) die Registerkarte ÄNDERUNGEN.
3. Klicken Sie auf HINZUFÜGEN, um eine *.mst*-Datei zum vorhandenen Installer-Paket hinzuzufügen. Falls Sie mehrere *.mst*-Dateien hinzufügen möchten, wiederholen Sie diesen Schritt. Über ENTFERNEN können bereits gewählte *.mst*-Dateien auch wieder gelöscht werden.
4. Haben Sie mehrere *.mst*-Dateien ausgewählt, so können Sie deren Reihenfolge zum Installieren der Änderungen über die Schaltflächen NACH OBEN und NACH UNTEN festlegen. Klicken Sie dann auf OK.

Registerkarte Sicherheitseinstellungen

Damit die Applikationspakete den Benutzern korrekt zugewiesen werden können, müssen Sie die geeigneten Sicherheitseinstellungen treffen. Sie müssen allen Benutzern, denen diese Applikation zugewiesen oder für die sie veröffentlicht werden soll, die Berechtigung Lesen zuweisen. Damit die Pakete von Administratoren bearbeitet werden können, müssen diese über die Berechtigung Vollzugriff verfügen.

Entfernen von Applikationspaketen

Wenn bestimmte Applikationspakete nicht mehr benötigt werden, sollten Sie diese entfernen. Um ein Paket zu entfernen, öffnen Sie in der Benutzer- oder Computerkonfiguration den Knoten SOFTWAREEINSTELLUNGEN/SOFTWAREINSTALLATION. Wählen Sie dort das zu entfernende Paket aus und aus dessen Kontextmenü ALLE TASKS/ENTFERNEN.

Sie erhalten das Dialogfeld SOFTWARE ENTFERNEN. Hier können Sie zwei verschiedene Arten der Deinstallation festlegen:

1. SOFTWARE SOFORT VON BENUTZERN UND COMPUTERN DEINSTALLIEREN: Hiermit wird die Applikation endgültig vom Computer deinstalliert. Die Deinstallation wird beim nächsten Start des Computers bzw. bei der nächsten Benutzeranmeldung vorgenommen. Die Applikation kann dann nicht mehr verwendet werden und steht dem Benutzer auch nicht mehr zur erneuten Installation bereit. Auch wenn er eine Datei mit der zugeordneten Dateiendung öffnet, wird die Applikation nicht mehr automatisch installiert. Sie sollten eine Applikation erst auf diese Weise entfernen, wenn Sie eine neue Applikation an die Benutzer/Computer verteilt haben, die dem Funktionsumfang der alten Applikation entspricht.
2. BENUTZER DÜRFEN DIE SOFTWARE WEITERHIN VERWENDEN, ABER NEUINSTALLATIONEN SIND NICHT ZUGELASSEN: Wenn Sie diese Option wählen, wird die Applikation selbst nicht vom Computer entfernt, sondern lediglich der Eintrag unter SYSTEMSTEUERUNG/SOFTWARE, damit der Benutzer sie nicht erneut installieren kann. Eine erneute Installation ist auch nicht über das Öffnen von Dateien mit der jeweiligen Dateiendung möglich. Damit ist die Benutzung sichergestellt, bis eine endgültige Deinstallation erfolgt.

Erneutes Bereitstellen einer Applikation

Im Kontextmenü jeder Applikation können Sie über ALLE TASKS/ANWENDUNG ERNEUT BEREITSTELLEN diese nochmals bereitstellen. Dabei wird die Applikation auf allen Computern, auf denen sie bereits vorhanden ist, neu installiert. Dieser Vorgang kann erforderlich werden, wenn Sie einer Applikation nicht alle oder nicht die korrekten *.mst*-Dateien zugewiesen und sie somit zu früh bereitgestellt haben, sodass sie bereits auf einigen Computern installiert wurde.

8.7.6 Strategie zur Konfiguration der Softwareinstallation

Dieses Kapitel beschreibt einige allgemein gültige Strategien zur Implementierung und Konfiguration der Richtlinie Softwareinstallation.

Sind im Unternehmen fast ausschließlich alle Benutzer an festen Arbeitsplätzen tätig, so sollten Sie die Software den entsprechenden Computern und nicht den einzelnen Benutzern zuweisen. Auf diese Weise wird die Software automatisch installiert, und die Benutzer können keinen Einfluss darauf nehmen.

Sie sollten andernfalls auch den Benutzern alle Softwarepakete zuweisen, die sie für ihre Arbeit benötigen. Damit wird sichergestellt, dass die Applikation entweder aus einer Desktop-Verknüpfung oder beim Öffnen einer Datei des festgelegten Dateityps installiert wird. Veröffentlichen sollten Sie nur solche Applikationen, die der Benutzer nicht zwingend für seine Arbeit benötigt, die aber unter Umständen nützlich sind und dann schnell zur Hand sein sollten. Informieren Sie die Benutzer darüber, wie sie über SYSTEMSTEUERUNG – SOFTWARE optionale Software installieren können. Dies sollte zahlreichen Anfragen an den Support vorbeugen. Zur besseren Auffindbarkeit von Applikationen unter SOFTWARE sollten Sie die Applikationen in Kategorien unterteilen.

Weiterhin sollten Sie ein Windows Installer-Paket in einem GPO nur ein einziges Mal zuweisen oder veröffentlichen. Es macht wenig Sinn, dieselbe Applikation einmal in der Computerkonfiguration den Computern und einmal in der Benutzerkonfiguration den Benutzern zuzuweisen. Sie erhalten zwar keine Fehlermeldung, aber dadurch wird der Anmeldevorgang der Benutzer an dem Computer unnötig verlangsamt.

Wenn Sie sich für den Einsatz einer neuen Software entscheiden, sollten Sie immer zuerst prüfen, ob die Applikation bereits als Windows Installer-Paket vorliegt oder nicht. Unter Umständen kann die Repaketierung sehr aufwändig werden. Auch die Bereitstellung von Resource Kits zu Applikationen zur Erstellung von *.mst*-Dateien kann ein wichtiger Faktor für den Erwerb einer Applikation sein.

8.7.7 Windows Installer-Technologie und Repaketierung

In diesem Kapitel werden die Grundlagen der Windows Installer-Technologie sowie der Repaketierung beschrieben. Diese beiden Themen sind als Grundlagenwissen zur Softwareverteilung nahezu unentbehrlich.

Mit Office 2000 wurde von Microsoft die erste Applikation veröffentlicht, die den Windows Installer als standardmäßiges Setup-Programm benutzt. Damit das Setup ordnungsgemäß ausgeführt werden kann, muss auf den Zielcomputern der Windows Installer vorhanden sein und als Dienst laufen. Den Windows Installer gibt es in verschiedenen Versionen. Folgende Betriebssysteme enthalten bereits nativ den Installer bzw. müssen eine entsprechende Version nachinstallieren:

Betriebssystem	Nativ vorhandene Version des Windows Installers	Folgende Versionen können nachinstalliert werden
Windows XP/Windows Server 2003/SBS 2003	2.0	–
Windows 2000	1.1	kann nicht die Version 1.2 nachinstallieren, nur Version 2.0
Windows ME	1.2	2.0

Betriebssystem	Nativ vorhandene Version des Windows Installers	Folgende Versionen können nachinstalliert werden
Windows NT SP3	–	1.x
Windows NT SP6	–	1.x, 2.0
Windows 98	–	1.x, 2.0
Windows 95	–	1.x, 2.0

Tabelle 8.18: Übersicht über die Windows Installer-Versionen

Installationspakete für den Windows Installer in der Version 2.0 finden Sie unter folgenden Adressen:

Für Windows NT 4, SP6 und Windows 2000:

http://www.microsoft.com/downloads/release.asp?releaseid=32832

Für Windows 95, Windows 98 und Windows Me:

http://www.microsoft.com/downloads/release.asp?releaseid=32831

Die Installationspakete des Windows Installers enthalten die Executables instmsi.exe sowie instmsiw.exe. instmsi.exe installiert den Windows Installer-Dienst unter Windows 9x, instmsiw.exe unter Windows NT. Der laufende Installer-Dienst auf den Clients wird von der msiexec.exe ausgeführt.

Die Installation erfolgt auf der Basis von msi-Dateien. Die Dateiendung *.msi* bedeutet Managed Software Installation. Jede msi-Datei entspricht dabei einer kleinen relationalen Datenbank. In ihr ist der Zielzustand enthalten, wie er nach der Installation auf dem Client vorliegen soll. Dies ist der sog. Post-Install-State. Dieser Zustand wird nicht wie bei herkömmlichen Setup-Programmen durch ein Installationsskript erreicht, sondern durch die Anwendung von bestimmten Regeln. Dieser definierte Zielzustand wird dann auf dem entsprechenden Computer gespeichert. Treten auf Seiten des Computers Änderungen am ursprünglich definierten Zielzustand auf, z.B. durch das versehentliche Löschen von Dateien, so wird der Post-Install-State durch den Windows Installer wiederhergestellt. Dieser automatische Reparaturmechanismus ist bei einem herkömmlichen Setup nicht gegeben.

Wird eine Windows Installer-Installation nicht erfolgreich abgeschlossen, erfolgt ein automatisches Rollback auf den Zustand vor der Installation des missglückten msi-Paketes. Ein weiteres Feature der Windows Installer-Technologie ist die Installation der Software bei Bedarf. Das heißt, dass bestimmte weniger häufig benutzte Features erst dann installiert werden, wenn der Benutzer sie tatsächlich das erste Mal benötigt.

Auch für die Definition von verschiedenen msi-Paketen bietet die Windows Installer-Technologie eine Möglichkeit: Sie können ein msi-Paket, z.B. Office 2000, durch den Einsatz von mst-Dateien mit speziellen Features konfigurieren. Die mst-Dateien werden auch als Transform-Files bezeichnet. Das Transform wird einmalig bei der ersten Installation des msi-Pakets angewendet. Nach der Installation des Basis-msi-Pakets können Sie keine weiteren Transform-Files zur Aktualisierung nachinstallieren. Sie können für ein msi-Paket beliebig viele Transform-Files erstellen. Das Erstellen von mst-Dateien ist zwar optional, wird aber sicherlich in den meisten Fällen durchgeführt werden.

Um ein msi-Paket verteilen zu können, muss zunächst ein administratives Setup der entsprechenden Applikation durchgeführt werden. Dies geschieht mit dem Parameter /a in der Setup-Anweisung (siehe Kapitel 8.7.1). Dabei wird der Inhalt der Applikations-CD an einen bestimmten Ort im Netzwerk kopiert, von dem aus später die Installation auf die Clients erfolgt. Das Standard-msi-Paket enthält dabei alle Features, die bei einer standardmäßigen Installation auch enthalten sind. Wollen Sie auf das Basispaket Änderungen anwenden, erstellen Sie mithilfe eines Resource Kits ein oder mehrere Transform-Files. Diese werden über die Gruppenrichtlinie dem msi-Paket zugewiesen und bei der ersten Installation auf dem Client angewendet.

8.7.8 Repaketierung

Die Repaketierung von Applikationen kann aus verschiedenen Gründen erfolgen. Der häufigste Grund dürfte wohl die Anpassung des Setups sein. Standardmäßig erhält der Benutzer bei der Installation eine Reihe von Dialogboxen, in denen er den Installationspfad oder Features festlegen kann. Diese Möglichkeit soll dem Benutzer jedoch in den meisten Fällen genommen werden. Idealerweise läuft der Installationsprozess im Hintergrund ab, wobei der Benutzer nicht eine einzige Dialogbox sieht. Er hat bei dieser Silent Installation keine Möglichkeit einzugreifen. Auch das Bereitstellen einer Applikation, deren Installationsinformationen in einer Setup.exe, nicht aber in einer msi-Datei enthalten sind, erfordert die Repaketierung.

Zur Repaketierung gibt es eine Reihe von Programmen von Drittanbietern. Eines der am häufigsten benutzten Produkte ist WinInstall LE 2003 von OnDemand-Software.

Beim Repaketieren einer Applikation wird ein neues Windows Installer-Paket aus den Änderungen gebildet, die während der Installation auf dem Computer durchgeführt werden, wie etwa das Hinzufügen oder Modifizieren von Dateien, Pfaden, Registry-Einträgen usw. Die meisten Programme verwenden dazu einen Mechanismus, bei dem der Zustand des Computers vor und nach der Installation verglichen wird. Aus den sich dabei ergebenden Differenzen wird das neue Paket gebildet. Also darf die zu repaketierende Applikation nicht bereits auf dem Rechner vorhanden sein. Ansonsten würden die Änderungen nicht erkannt und damit das Paket fehlerhaft werden.

8.7.9 Erstellen einer .mst-Datei (Transform-File)

In diesem Kapitel wird Ihnen kurz das Erstellen eines Transform-Files am Beispiel von Office 2003 erläutert. Wie bereits mehrfach erwähnt, ist dieser Arbeitsschritt zwar optional, wird aber sicherlich in den meisten Fällen umgesetzt werden. Um bei unserem Beispiel Office 2003 zu bleiben, würden alle Benutzer ohne angepasste Transform-Files die standardmäßige Installation des Office-Paketes erhalten. So ist es aber möglich, dass ein Teil der Benutzer unnötig viele Programmteile auf seinem Rechner installiert hat, während anderen Anwendern bestimmte Features nicht standardmäßig zur Verfügung stehen, sondern erst bei Bedarf nachinstalliert werden müssten. Für Benutzer, die lediglich für Korrespondenz zuständig sind, wären z.B. Word und Excel ausreichend, während z.B. den Benutzern der Marketingabteilung zusätzlich PowerPoint zur Verfügung stehen sollte.

Sie erzeugen ein MST-File für Office 2003, indem Sie den *Custom Installation Wizard* starten. Dieser ist eine Komponente des Office 2003 Resource Kit. Dieses ist ausschließlich in englischer Sprache verfügbar. Das Office 2003 Resource Kit können Sie unter folgender Adresse downloaden:

http://www.microsoft.com/office/ork/2003/default.htm

Resource Kits können für eine Reihe von Applikationen bezogen werden. Steht für eine bestimmte Anwendung kein Resource Kit zur Verfügung, so können verschiedene Pakete mit unterschiedlichen Feature-Sets durch Repaketierung erzeugt werden.

Wenn Sie den Wizard des Office Resource Kit starten, können bis zu 20 Fenster erscheinen, die Ihre Daten zur Änderung der Default-Einstellungen abfragen. Die gesammelten Daten werden in dem Transform-File gespeichert, dessen Namen Sie in dem Wizard festlegen. Diese Datei hat die Erweiterung .MST. Sie können ein .MST-File neu erstellen oder ein existierendes .MST-File editieren.

Alle Optionen der individuellen Anpassung im Custom Installation Wizard sind in dem Handbuch bzw. der Online-Hilfe zum Office Resource Kit ausführlich beschrieben. Eine explizite Beschreibung der einzelnen Fenster würde den Rahmen dieses Buches sprengen.

8.7.10 Fehlersuche bei Gruppenrichtlinien

Dieses Kapitel gibt Ihnen eine Übersicht über häufig auftretende Probleme im Zusammenhang mit den Gruppenrichtlinien. Dazu erhalten Sie zunächst eine Auflistung von Problemen mit Lösungsansätzen. Am Ende dieses Kapitels erhalten Sie Hinweise auf mögliche Fehlfunktionen von Gruppenrichtlinien nach der Migration von Windows NT.

1. Ein GPO-Snap-in kann nicht geöffnet und/oder bearbeitet werden.
   - Um ein GPO bearbeiten zu können, muss der Benutzer nicht nur über die Berechtigung Lesen, sondern über Vollzugriff auf das entsprechende Objekt verfügen. Lokale Administratoren können nur die lokalen GPOs bearbeiten, während standardmäßig ein Domänen-Admin auch die Active Directory-basierten GPOs bearbeiten kann.
   - Erhalten Sie die Fehlermeldung, dass das Objekt nicht geöffnet werden konnte, prüfen Sie die Netzwerkverbindung zum Objekt. Es kann auch ein Fehler in der DNS-Konfiguration vorliegen.
2. Die lokalen Richtlinieneinstellungen zeigen keinen Effekt.
   - Sind weitere Richtlinien auf Standort-, Domänen- oder OU-Ebene definiert, so überschreiben diese die lokalen Einstellungen, sofern sie nicht miteinander kompatibel sind.
3. Die Richtlinieneinstellungen im Active Directory zeigen keinen Effekt.
   - Wenn ein Benutzer oder Computer nicht die Einstellungen der Richtlinien erhält, kann dies verschiedene Ursachen haben. Prüfen Sie zunächst, ob die gewünschten Einstellungen auch tatsächlich eingestellt sind und die Richtlinie nicht mehr standardmäßig deaktiviert ist.

- Bedenken Sie, dass die GPOs in der Reihenfolge lokal, Standort, Domäne und OU abgearbeitet werden. Widersprechen sich dabei Konfigurationen, so wird die ranghöhere Einstellung die darunter liegende überschreiben.
- Die Benutzer bzw. Computer müssen sich in einem der Container Standort, Domäne oder OU befinden. Nur auf diese drei Container können Richtlinien angewendet werden.
- Prüfen Sie dann, ob das GPO auch auf die OU angewendet wird, in welcher der Benutzer oder Computer Mitglied ist. Alternativ dazu können Sie das GPO auch auf eine übergeordnete OU oder die Domäne anwenden, sofern die Einstellungen weitervererbt werden.
- Prüfen Sie, ob innerhalb einer OU mehrere GPOs definiert worden sind und dabei möglicherweise eines mit der Option KEIN VORRANG versehen worden ist. Dieses GPO vererbt seine Einstellungen zwingend. Ansonsten werden die Einstellungen des GPO übernommen, das als letztes abgearbeitet wird. Wenn die Optionen KEIN VORRANG sowie RICHTLINIENVERERBUNG DEAKTIVIEREN beide ausgewählt sind, so wird die Option KEIN VORRANG zuerst behandelt.
- Auch wenn die Gruppenrichtlinien nicht auf der Zugehörigkeit von Benutzern und Computern zu bestimmten Sicherheitsgruppen basieren, so müssen Sie trotzdem sicherstellen, dass ein Benutzer nicht Mitglied einer Gruppe ist, deren Berechtigung GRUPPENRICHTLINIE ÜBERNEHMEN auf VERWEIGERN gesetzt ist. Stattdessen muss für mindestens eine Gruppe das Übernehmen der Gruppenrichtlinie gestattet und Leseberechtigung dafür gegeben sein.
- Überprüfen Sie, ob der DNS-Server korrekt eingetragen ist. Es muss unbedingt der DNS-Server eingetragen sein, der die gesamten Ressourceneinträge enthält. Dies ist der DNS-Server, der als Erster in der Domäne eingerichtet worden ist. Verwenden Sie keinen DNS-Server unter einem Windows-Betriebssystem, so müssen Sie den Server angeben, auf dem Sie die Ressourceneinträge manuell vorgenommen haben.

4. Spezielle Probleme bei der Softwareinstallation
   - Wenn eine veröffentlichte Anwendung dem Benutzer nicht unter SYSTEMSTEUERUNG/SOFTWARE zur Verfügung steht, prüfen Sie, ob die entsprechende Gruppenrichtlinie auf ihn angewendet wurde (siehe vorherige Problemstellung). Stehen in den angewendeten GPOs überhaupt veröffentlichte Applikationen bereit? Außerdem darf es sich bei dem Client um keinen Terminalserver-Client handeln.
   - Erhält der Benutzer bei der Installation die Fehlermeldung, dass die Applikation nicht im Quellverzeichnis auffindbar ist, so prüfen Sie seine Berechtigungen für die Freigabe des Quellverzeichnisses. Der Benutzer muss über die Berechtigung Lesen für dieses Verzeichnis verfügen. Prüfen Sie auch die Netzwerkverbindung zum Quellverzeichnis.
   - Erhält der Benutzer die Meldung, dass die Bereitstellung des Pakets vom Active Directory nicht zugelassen wird oder das Paket nicht zur Bereitstellung vorbereitet werden kann, so liegt eine Beschädigung am Installationspaket vor. Prüfen Sie auch die Netzwerkverbindung zum Quellverzeichnis.
   - Nach der Installation des Pakets finden Sie im Ereignisprotokoll eine Fehlermeldung mit einer der folgenden IDs: 102, 108, 303 oder 1000, und das Paket ist nicht korrekt installiert. Dies deutet darauf hin, dass für den Computer nicht die ent-

sprechenden Berechtigungen für die Freigabe vorliegen, von der aus das Paket installiert werden soll. Das Abarbeiten einer Gruppenrichtlinie für einen Computer geschieht immer im Kontext des System Accounts der Maschine. Stellen Sie also sicher, dass auch der Computer über die Leseberechtigung für die Freigabe verfügt. Vergeben Sie z.B. diese Berechtigung an die Sicherheitsgruppe Domänencomputer.

- Treten Fehler bei der Installation auf, wenn sich das Quellpaket in einer DFS-Freigabe befindet, so müssen Sie überprüfen, ob die Berechtigungen sowohl auf Freigabe- als auch auf NTFS-Ebene ausreichend sind. Dies gilt für alle Repliken des DFS-Root-Verzeichnisses und die Freigaben des DFS-Links.
- Befindet sich der Server, der die Freigabe für das Installationspaket enthält, in einer anderen Gesamtstruktur als der Client, der das Paket erhalten soll, so ist es möglich, dass Sie im Ereignisprotokoll eine Fehlermeldung mit der ID 1612 (evtl. auch 102) erhalten. Die Berechtigungen für die Freigabe und dem darin enthaltenen Installationspaket sind dem Computer zugewiesen. Allerdings kann sich ein Computer an einem Rechner in einer anderen Gesamtstruktur nur über NTLM, nicht jedoch über Kerberos identifizieren. Dabei findet jedoch keine Überprüfung des Computerkontos statt. Computerkonten benötigen jedoch Kerberos für die Authentifizierung, also kann auf das Installationspaket nicht zugegriffen werden. Um dieses Problem zu beheben, müssen Sie die Berechtigungen den entsprechenden Benutzern zuweisen.
- Wird die Software nicht automatisch installiert, sobald sie für das Öffnen eines bestimmten Dokuments benötigt wird, so sind die Optionen für die Softwareinstallation nicht auf AUTOMATISCH INSTALLIEREN gesetzt.

5. Spezielle Probleme bei der Softwaredeinstallation
   - Wird eine Applikation wieder deinstalliert und entfernt dabei nicht alle Bestandteile, so etwa Verknüpfungen auf dem Desktop oder in der Taskleiste, so sind diese nach der Installation vom Benutzer selbst angelegt worden. Mit der Deinstallation werden nur die zur Applikation gehörenden Komponenten wieder entfernt, die bei der Installation eingespielt worden sind.

Ein sehr nützliches Programm zur Analyse der einzelnen Gruppenrichtlinieneinstellungen ist das Support-Tool GPResult.exe. Mit GPResult haben Sie die Möglichkeit, die Effekte der GPO-Einstellungen für einen Computer und/oder angemeldeten Benutzer zu sehen. Das Programm GPResult können Sie unter folgender Adresse downloaden:

http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp

8.8 Überwachung und Berichterstattung

Um die Überwachung und Berichterstattung in der Serververwaltung konfigurieren zu können, müssen Sie zuvor in der Aufgabenliste den Punkt ÜBERWACHUNG KONFIGURIEREN abgeschlossen haben (siehe Kapitel 2.7.9). Ist dies nicht der Fall, werden Sie zunächst aufgefordert, diesen Schritt nachzuholen. Dort legen Sie fest, an welche E-Mail-Adresse die Warnungen und Leistungsberichte gesendet werden sollen und ob die Leistungsberichte für bestimmte Personen auf der Firmenwebsite zur Verfügung stehen sollen.

8.8.1 Einrichten der Überwachung

Um die Überwachung einzurichten, öffnen Sie in der Serververwaltung unter ÜBERWACHUNG UND BERICHTERSTATTUNG den Link ÜBERWACHUNGSBERICHTE UND WARNUNGEN EINRICHTEN.

1. Im Fenster KONFIGURATIONSMODUS entscheiden Sie, ob eine bereits vorhandene Überwachungsfunktion geändert oder die Überwachungsfunktion neu installiert werden soll. Die zweite Option sollten Sie jedoch nur verwenden, wenn die Überwachung nicht mehr korrekt ausgeführt wird, da bei diesem Vorgang sämtliche vorhandenen Überwachungsdaten gelöscht werden. Klicken Sie dann auf WEITER.
2. Egal, ob Sie die Option Überwachungsfunktion ändern oder neu installieren gewählt haben, können Sie nacheinander alle Einstellungen bearbeiten, die Sie bereits im Rahmen der Aufgabenliste für die Überwachung konfiguriert haben. Sie können also die folgenden Einstellungen modifizieren:
   - Auswahl, ob Nutzungs- und/oder Leistungsberichte per E-Mail versendet werden sollen und ob die Nutzungsberichte in der Serververwaltung angezeigt werden sollen.
   - Auswahl der E-Mail-Adresse, an welche die Berichte versendet werden sollen
   - Auswahl der Benutzer, für welche die Leistungsberichte im Intranet angezeigt werden sollen
   - Auswahl, ob Leistungswarnungen ebenfalls per E-Mail verschickt werden sollen
3. Nehmen Sie jeweils die gewünschten Änderungen vor und beenden dann den Assistenten.

8.8.2 Der Serverleistungsbericht

Sofern Sie bei der Konfiguration die Option gewählt haben, den Leistungsbericht in der Serververwaltung anzuzeigen, wird dieser jedes Mal neu geladen und angezeigt, wenn Sie auf ÜBERWACHUNG UND BERICHTERSTATTUNG klicken. Dort finden Sie Einträge zu den folgenden Bereichen (siehe Abbildung 8.58):

- Serverspezifikation: Hier finden Sie Informationen zu Betriebssystem, Prozessor und RAM-Ausstattung des Servers.
- Leistungszusammenfassung: Hier werden die aktuellen Leistungsindikatoren zur Auslastung der Festplattenkapazität und der CPU sowie die des letzten Monats und die Wachstumsrate zwischen beiden Werten dargestellt.
- Top-Prozesse: Es werden jeweils die fünf Prozesse angezeigt, die den meisten Speicher belegt und die höchste CPU-Auslastung bewirkt haben.
- Sicherung: Hier finden Sie die Informationen zur Sicherung.
- Nicht ausgeführte Dienste: Es werden alle Dienste aufgeführt, für welche die Startart AUTOMATISCH konfiguriert ist, deren automatischer Start jedoch fehlgeschlagen ist.
- Kritische Warnungen: Hier werden die kritischen Warnungen des Servers zusammengefasst.
- Kritische Fehler in den Ereignisprotokollen: Es werden die kritischen Warnungen der Protokolle Anwendung, Verzeichnisdienst, DNS-Server, Dateireplikationsdienst, Sicherheit und System angezeigt.

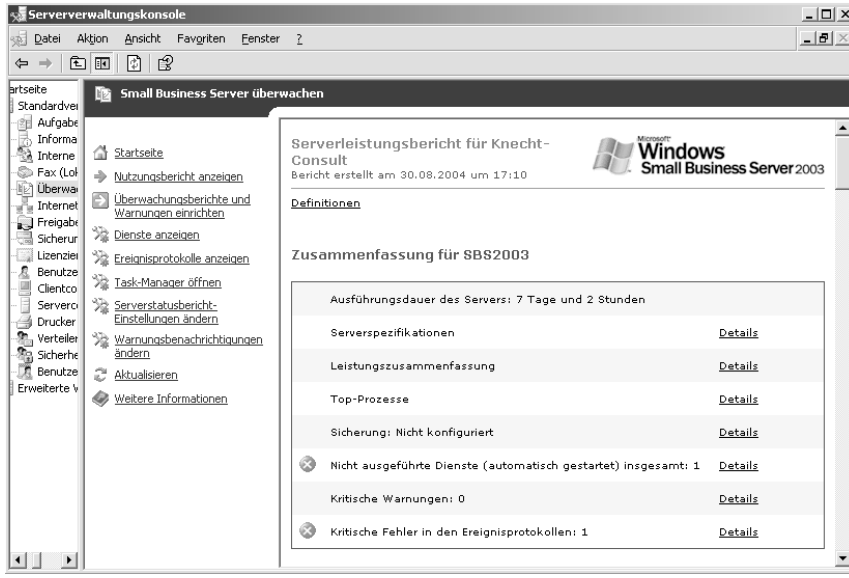


Abbildung 8.58: Der Serverleistungsbericht im Überblick

Indem Sie jeweils auf DETAILS klicken, erhalten Sie genauere Informationen zu dem gewählten Bereich. Im folgenden Beispiel (siehe Abbildung 8.59) sehen Sie die Details des Bereichs TOP-PROZESSE.

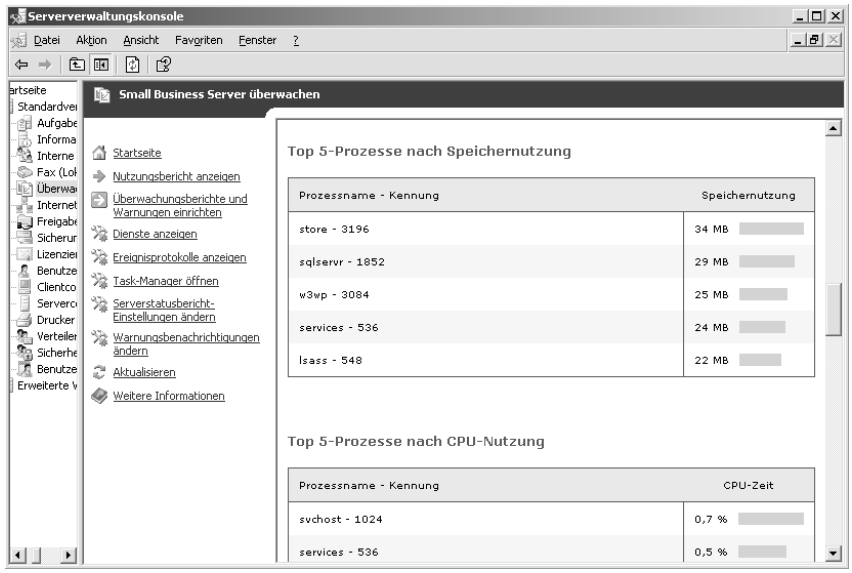


Abbildung 8.59: Details des Serverleistungsberichts im Bereich Top-Prozesse

8.8.3 Der Nutzungsbericht

Um den Nutzungsbericht für den Server anzuzeigen, klicken Sie auf den entsprechenden Link unter ÜBERWACHUNG UND BENACHRICHTIGUNGEN. Ein Nutzungsbericht umfasst immer die Daten von 14 Tagen.

Um einen neuen Bericht anzulegen, klicken Sie auf NEUEN BERICHT ERSTELLEN. Dabei müssen Sie den Zeitraum für den Bericht festlegen sowie den Umfang des Berichts (siehe Abbildung 8.60).

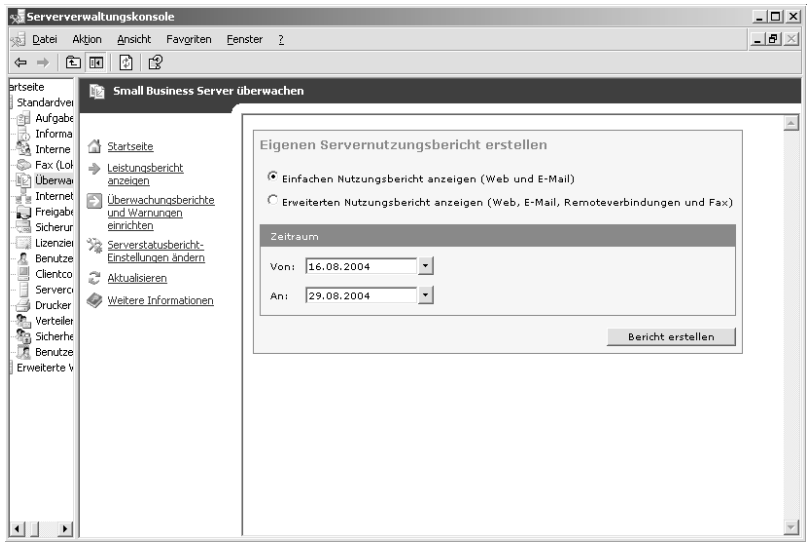


Abbildung 8.60: Das Erstellen eines neuen Nutzungsberichts

8.8.4 Die Berichtseinstellungen bearbeiten

Nachdem Sie die Optionen für die Leistungs- und Nutzungsberichte konfiguriert haben, können Sie die Optionen für beide später jederzeit ändern. Klicken Sie hierzu auf den Link SERVERSTATUSBERICHT-EINSTELLUNGEN ÄNDERN.

Im Fenster SERVERSTATUSBERICHTE (siehe Abbildung 8.61) können Sie neue Berichte hinzufügen, vorhandene bearbeiten, löschen sowie das Senden eines Berichts erzwingen.

Am interessantesten ist das Bearbeiten der Berichte. Indem Sie auf die entsprechende Schaltfläche klicken, erhalten Sie das Eigenschaftsfenster des Berichts mit verschiedenen Registerkarten (siehe Abbildung 8.62).

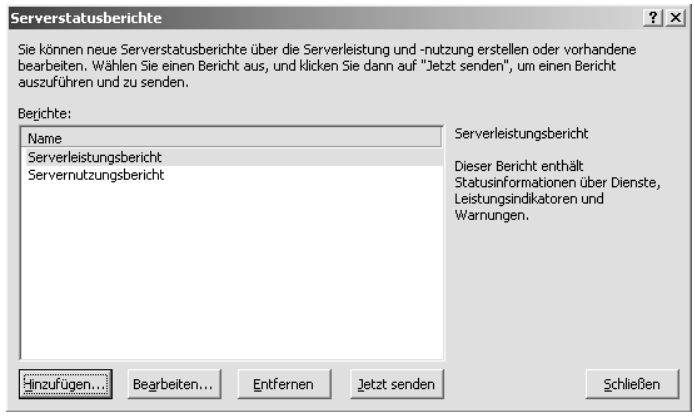


Abbildung 8.61: Bearbeiten der Serverstatusberichte

Abbildung 8.62: Auswahl der zu protokollierenden Bereiche

Auf der Registerkarte ALLGEMEIN können Sie einen neuen Namen sowie eine Beschreibung für den Bericht vergeben.

Unter INHALT wählen Sie die Optionen aus, die in den Leistungs- bzw. Nutzungsbericht aufgenommen werden sollen.

Unter E-MAIL-OPTIONEN legen Sie die E-Mail-Adresse(n) fest, an welche die Berichte gesendet werden sollen.

Auf der Registerkarte TASK bestimmen Sie, ob der Task automatisch zur angegebenen Zeit ausgeführt werden soll.

Unter ZEITPLAN schließlich legen Sie den Zeitplan für das Ausführen des Tasks fest.

8.9 Sicherung und Wiederherstellung

Unter SICHERUNG in der Serververwaltung können Sie über SICHERUNG KONFIGURIEREN die Grundeinstellungen zur Sicherung vornehmen. Dabei handelt es sich um dieselben Einstellungen, die Sie im Rahmen der Aufgabenliste (siehe Kapitel 2.7.10) vorgenommen haben. Diese Einstellungen können hier nun modifiziert werden.

Über den Link WEITERLEITUNG DES ORDNERS EIGENE DATEIEN KONFIGURIEREN können Sie die Ordnerumleitung dieses Benutzerordners einstellen. Dieses Verfahren wurde bereits im Zuge der Benutzerverwaltung in Kapitel Abbildung 8.2.6 beschrieben.

Der Link INFORMATIONEN ÜBER DIE SERVERWIEDERHERSTELLUNG ANZEIGEN führt Sie auf eine html-Seite mit zusätzlichen Informationen zum Thema Sicherung.

Sobald Sie auf den Link SHAREPOINT-DATEIEN WIEDERHERSTELLEN klicken, erhalten Sie ebenfalls eine html-Seite mit einigen Hinweisen. Das Wiederherstellen von SharePoint-Dateien wurde bereits im Zusammenhang mit den SharePoint Services in Kapitel 5.5 beschrieben.

Unter EINZELNE DATEIEN WIEDERHERSTELLEN können Sie das neue Feature der Schattenkopien konfigurieren. Dies wird ausführlich in den nächsten Kapiteln beschrieben.

8.9.1 Wiederherstellen einzelner Dateien mit Hilfe des Features Schattenkopie

Der Windows Server 2003 wie auch der SBS 2003 verwenden das neue Feature der Volumenschattenkopie. Dazu läuft auf dem Server der Dienst Volumenschattenkopie (Volume Shadow Copy Service, VSS). Dabei wird automatisch für jede Datei, die der Benutzer auf der Serverfreigabe anlegt, eine Kopie gespeichert. Diese automatische Speicherung erfolgt nach einem frei definierbaren Zeitplan. Standardmäßig erfolgt die Sicherung zweimal täglich. Dabei ist es unerheblich, ob sich die Datei gerade in Benutzung befindet oder nicht. Diese Schattenkopien werden im Ordner SYSTEM VOLUME INFORMATION angelegt; es ist kein separates Sicherungsmedium erforderlich. Dort können bis zu 64 Sicherungen pro Volume angelegt werden.

Damit ist es möglich, im Rahmen der Wiederherstellung eine Datei mit einer relativ neuen Version wiederherzustellen. Diese Wiederherstellung können auch die Benutzer selbst für ihre Dateien vornehmen, beispielsweise wenn eine Datei beschädigt oder aus Versehen gelöscht wurde. Für die Wiederherstellung einer früheren Dateiversion ist nun nicht mehr der Administrator notwendig, da der Benutzer diesen Arbeitsschritt selbst durchführen kann.

Schattenkopien können nur für die Freigaben des Servers konfiguriert werden, nicht jedoch für lokale Laufwerke der Clients. Zudem können Sie die Schattenkopien entweder nur für sämtliche Freigaben des Servers einrichten oder für gar keine.

Begehen Sie jedoch nicht den Fehler zu denken, dass die Funktionalität der Schattenkopien die herkömmliche Sicherung ersetzt. Wie bereits erwähnt werden hierbei lediglich die Daten in den Serverfreigaben gespeichert, nicht jedoch System- und Systemstatusdateien.

8.9.2 Clientkonfiguration für die Schattenkopien

Damit die Clients das Feature der Schattenkopien auch nutzen können, müssen diese entsprechend vorbereitet werden. Dazu muss sich auf dem Client der Shadow Copy Client (Client für vorherige Versionen) befinden.

Im Lieferumfang des SBS 2003 befindet sich der Shadow Copy Client für Windows XP-Clients. Sie finden die entsprechende Datei auf dem SBS 2003 im Ordner %Systemroot%\System32\Clients\twclient. Dort finden Sie die Clients für die verschiedenen Prozessorarchitekturen x86 (Ordner x86), Athlon64 bzw. AMD Opteron (Ordner amd64) sowie Intel Itanium (Ordner ia64). Die Installation erfolgt über die entsprechende msi-Datei. Dazu können Sie entweder den Ordner freigeben oder die Datei über die Softwareverteilung der Gruppenrichtlinien auf den Clients installieren.

Für Windows 2000 mit Service Pack 3 und höher sowie Windows 98 (hier muss der Windows Installer in der Version 2.0 installiert sein) können Sie die Shadow Copy Clients direkt bei Microsoft downloaden. Sie finden die entsprechende Version auch auf der mitgelieferten CD.

8.9.3 Einrichten von Schattenkopien auf dem Server

Nachdem Sie die Funktionalität für die Clients bereitgestellt haben, müssen Sie den Server ebenfalls für das neue Feature konfigurieren.

1. Hierzu wählen Sie den Kontextmenüeintrag EIGENSCHAFTEN des gewünschten Laufwerks und wechseln auf die Registerkarte SCHATTENKOPIEN (siehe Abbildung 8.63).

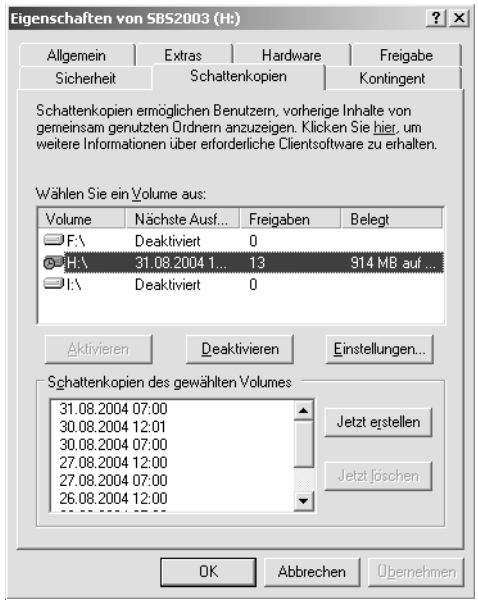


Abbildung 8.63: Die Schattenkopie-Funktion des SBS 2003

Dort sehen Sie, für welche Laufwerke die Schattenkopien bereits aktiviert und zu welchen Zeiten Schattenkopien angelegt worden sind. Aus der Liste können Sie bestimmte Einträge löschen oder auch über die Schaltfläche JETZT ERSTELLEN außerhalb des Zeitplans eine Schattenkopie anlegen.

2. Standardmäßig ist diese Funktionalität auf dem Server noch deaktiviert. Um die Schattenkopien für ein Laufwerk zu aktivieren, markieren Sie das Laufwerk und klicken auf AKTIVIEREN. Standardmäßig werden die Schattenkopien eines Laufwerks auch auf diesem angelegt. Sie haben jedoch die Möglichkeit, diesen Speicherort zu ändern. Dies bietet sich an, wenn auf dem Datenträger möglicherweise nicht genügend Speicherplatz bereitsteht (ist der Speicherplatz erschöpft, können neue Schattenkopien nur angelegt werden, wenn die jeweils älteste Version gelöscht wird) oder Sie eine andere, schnellere Festplatte für die Sicherung verwenden möchten. Um den Pfad zu ändern, klicken Sie auf EINSTELLUNGEN und wählen unter SPEICHERBEREICH die gewünschte Partition aus.

Das Ändern des Laufwerks ist nur möglich, wenn die Funktionalität der Schattenkopie für das Laufwerk noch nicht aktiviert wurde. Sobald die Schattenkopien aktiviert wurden, kann der Speicherort nicht mehr geändert werden.

3. Um die Einstellungen für die Schattenkopien zu ändern, klicken Sie auf EINSTELLUNGEN. Sie können nun verschiedene Optionen konfigurieren (siehe Abbildung 8.64).

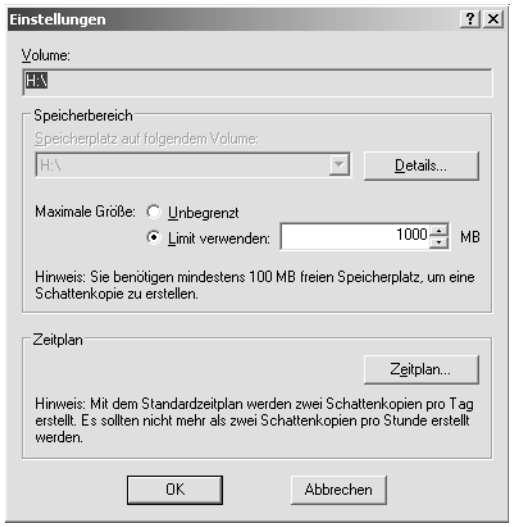


Abbildung 8.64: Die Einstellungsmöglichkeiten für die Schattenkopien eines Laufwerks

Unter SPEICHERBEREICH sehen Sie, auf welchem Laufwerk die Schattenkopien angelegt werden. Über DETAILS können Sie feststellen, wie viel Speicherplatz bereits durch die Schattenkopien belegt ist.

Weiterhin können Sie bestimmen, wie viel Speicherplatz auf dem Laufwerk für die Schattenkopien bereitgestellt werden soll. Die Standardeinstellung liegt bei 10 Prozent des freien Speicherplatzes. Da für eine Schattenkopie mindestens 100 MB benötigt werden, überlegen Sie sich gut, ob und, wenn ja, welches Limit Sie vergeben. Ist der Speicherplatz erschöpft, werden zwar weiterhin neue Schattenkopien angelegt, allerdings wird dabei jedes Mal die älteste Version automatisch gelöscht.

Über die Schaltfläche ZEITPLAN können Sie bestimmen, zu welchen Zeiten das Anlegen einer neuen Schattenkopie vorgenommen werden soll. Standardmäßig werden von Montag bis Freitag jeweils um 7:00 h und um 12:00 h Schattenkopien angelegt. Diesen Zeitplan können Sie beliebig anpassen oder auch mehrere Zeitpläne einrichten. Achten Sie jedoch darauf, dass Sie pro Stunde nicht mehr als eine Schattenkopie erstellen.

8.9.4 Wiederherstellung durch den Benutzer

Nachdem also Client und Server vorbereitet worden sind, können die Benutzer vorherige Versionen ihrer Dateien wiederherstellen. Am sinnvollsten ist es, den Benutzern generell einmal dieses Verfahren zu zeigen, so dass sie die Wiederherstellung künftig selber vornehmen können und damit nicht mehr den Administrator belasten müssen.

Wiederherstellung einer früheren Dateiversion

1. Die Wiederherstellung einer früheren Version geschieht über den Windows Explorer. Öffnen Sie dazu die EIGENSCHAFTEN der Datei und wechseln auf die Registerkarte VORHERIGE VERSIONEN (siehe Abbildung 8.65).

Abbildung 8.65: Die vorherigen Dateiversionen in einer Schattenkopie

2. Unter DATEIVERSIONEN finden Sie alle in den Schattenkopien vorhandenen Versionen der Datei. Zu jeder Version ist das Erstellungsdatum angegeben, so dass der Benutzer schnell feststellen kann, welche Version er wiederherstellen muss.
3. Haben Sie eine Datei markiert, können Sie über die Schaltfläche ANZEIGEN die Datei öffnen und betrachten. So stellen Sie schnell fest, welche Inhalte in der Datei vorhanden sind. Haben Sie sich entschlossen, diese Version wiederherzustellen, klicken Sie auf WIEDERHERSTELLEN. Damit wird die Datei an ihrem ursprünglichen Speicherort wiederhergestellt und die vorhandene Datei überschrieben. Möchten Sie hingegen die vorhandene Datei beibehalten und die frühere Version an einem anderen Ort speichern, verwenden Sie die Schaltfläche KOPIEREN. Dabei kann ein anderer Speicherort ausgewählt werden.

Wiederherstellen einer gelöschten Datei

Soll hingegen eine versehentlich gelöschte Datei wiederhergestellt werden, navigieren Sie zu dem Ordner, in dem sich die gelöschte Datei befunden hat, und wechseln über dessen EIGENSCHAFTEN auf die Registerkarte VORHERIGE VERSIONEN.

Sie können hier wie bei einer Datei die verschiedenen Versionen des Ordners betrachten und wiederherstellen.

Sobald Sie die frühere Version eines Ordners wiederherstellen, um so eine gelöschte Datei wiederzuerlangen, werden automatisch alle anderen im Ordner befindlichen Dateien ebenfalls auf dem Stand wiederhergestellt, der zum Zeitpunkt der Sicherung vorlag. Änderungen an anderen Dateien des Ordners, die nach dem Anlegen der Schattenkopie durchgeführt worden sind, gehen dabei verloren.

8.10 Verwaltung von Netzwerk, Internet und E-Mail

Unter dem Menüpunkt INTERNET UND E-MAIL finden Sie in der Serververwaltung eine Reihe von Einstellungen für die Netzwerkverbindung, Internetverbindung sowie E-Mail-Optionen.

Über die beiden Links VERBINDUNG MIT DEM INTERNET HERSTELLEN sowie RAS KONFIGURIEREN rufen Sie wieder die beiden Assistenten auf, die Sie schon aus der Aufgabenliste der Netzwerkaufgaben (siehe Kapitel 2.7.1) kennen.

8.10.1 Die Remote-Verbindungsdiskette

Über REMOTE-VERBINDUNGSDISKETTE ERSTELLEN können Sie eine Konfigurationsdiskette erstellen, die Sie für die Verbindung von Remote-Clients zum SBS 2003-Netzwerk verwenden. Dazu werden die Dateien *setup.exe* und *sbspackage.exe* auf die Diskette kopiert.

Nach der Installation der Remote-Verbindung auf dem Client finden Sie unter den Netzwerkverbindungen den neuen Eintrag VERBINDUNG MIT SMALL BUSINESS SERVER HERSTELLEN. Darüber kann die Anmeldung am SBS-Netzwerk vorgenommen werden.

8.10.2 Probleme bei der Remote-Unterstützung über den MSN Messanger

Möchten Sie auf einem SBS 2003 die Remote-Unterstützung im MSN Messanger verwenden und erhalten dabei die folgenden Fehlermeldung:

IHRE EINLADUNG KONNTE NICHT GESENDET WERDEN, DA SIE NICHT ÜBER DIE AKTUELLE VERSION DES WINDOWS MESSANGER VERFÜGEN, UM DIE REMOTE-UNTERSTÜTZUNG AUSZUFÜHREN,

so deutet dies darauf hin, dass auf dem SBS 2003 nicht die aktuelle Version des MSN Messangers installiert ist. Es sollte eine Version höher als MSN 6.0 vorhanden sein. Sie sollten sich die aktuelle Version aus dem Microsoft Download Center unter *http://www.microsoft.com/downloads* besorgen.

8.10.3 Bearbeiten von Verbindungskennwörtern und -konfigurationen

Nachdem Sie im Assistenten zur Herstellung der Internetverbindung den Verbindungstyp mit den erforderlichen Daten erstellt haben, können Sie hier die Kennwörter für die Verbindungen ändern.

Je nachdem, ob Sie über eine DFÜ-Verbindung oder eine Breitbandverbindung verfügen, können Sie über den entsprechenden Link das Kennwort für die Verbindung bearbeiten. Weiterhin können Sie auch Einstellungen an den Netzwerkverbindungen sowie den Telefon- und Modemoptionen vornehmen.

Sofern der SMTP-Connector für die TURN-Authentifizierung konfiguriert ist, können Sie hier auch das E-Mail-Kennwort ändern.

8.11 Interne Website

Die Konfigurationseinstellungen unter dem Link INTERNE WEBSITE beziehen sich alle auf die Website Companyweb der SharePoint Services. Die Verwaltung der internen Website wurde bereits in diesem Zusammenhang ausführlich ab Kapitel 5.2 beschrieben.

8.12 Freigaben (lokal)

Wenn Sie in der Serververwaltung den Menüpunkt FREIGABEN (LOKAL) aufrufen, sehen Sie eine Liste aller auf dem SBS 2003 vorhandenen Freigaben. Zusätzlich erfahren Sie den Ordnerpfad, eine Beschreibung der Freigabe sowie die Anzahl der Clients, die gerade mit der Freigabe verbunden sind. Über den jeweiligen Kontextmenüeintrag EIGENSCHAFTEN können Sie die Freigaben bearbeiten.

Weiterhin können Sie über den Link EINEN FREIGEGEBENEN ORDNER HINZUFÜGEN neue Freigaben erstellen. Durch diesen Vorgang leitet Sie ein Assistent. Für weitere Informationen zu Freigaben sei auf die Windows-Hilfe verwiesen.

8.13 Konfigurationseinstellungen des SBS 2003 ändern

Im Laufe der Betriebszeit des SBS 2003 kann es erforderlich werden, einige Konfigurationseinstellungen des Servers zu modifizieren. Dazu zählen etwa das Übertragen des DHCP-Serverdienstes auf den SBS 2003 oder das Ändern von DFÜ-Verbindungseinstellungen.

8.13.1 Ändern der Server-IP-Adresse

Bei der Installation des SBS 2003 wird dessen IP-Adresse festgelegt. Um diese nachträglich zu ändern, dürfen Sie lediglich in der Serververwaltung unter INTERNET UND E-MAIL den Link SERVER-IP-ADRESSE ÄNDERN verwenden (siehe Abbildung 8.66).

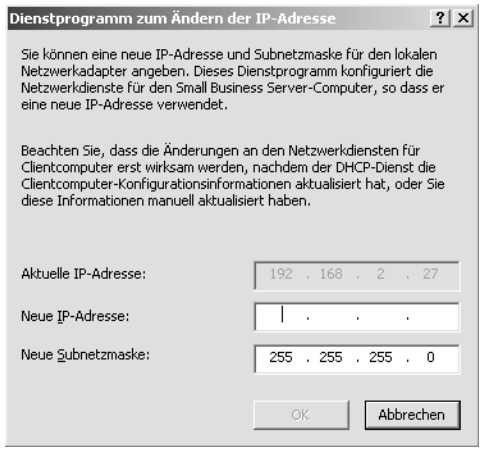


Abbildung 8.66: Das Ändern der IP-Adresse des SBS 2003 über das entsprechende Dienstprogramm

Allein bei diesem Verfahren ist sichergestellt, dass die IP-Adresse auch für alle auf dem SBS 2003 konfigurierten Dienste und Anwendungen geändert wird.

Ändern Sie nie die IP-Adresse des SBS 2003 über die Eigenschaften der Netzwerkverbindung im TCP/IP-Protokoll. So wird nur die Adresse des Servers geändert, nicht jedoch die mit dem Server verbundenen Dienste. Fehlfunktionen sind auf diese Weise vorprogrammiert.

8.13.2 Übertragen des DHCP-Serverdienstes auf den SBS 2003

Während der Installation konnten Sie entscheiden, ob der DHCP-Serverdienst auf dem SBS 2003 selbst oder einem anderen Gerät, beispielsweise einem bereits vorhandenen Router, ausgeführt werden soll. Nur durch den Einsatz des DHCP-Serverdienstes auf dem SBS 2003 können Sie sicherstellen, dass sämtliche benötigten Einstellungen für das Netzwerk wirklich korrekt konfiguriert sind. Gerade die DHCP-Bereichsoptionen können unter vielen Routern nicht immer wie erforderlich konfiguriert werden.

1. Um den DHCP-Serverdienst auf den SBS 2003 zu übertragen, müssen Sie zunächst den DHCP-Dienst auf dem Router beenden, da sich nur ein DHCP-Server im Netzwerk befinden darf. Zuvor sollten Sie sich die Konfiguration des alten DHCP-Servers notieren.

Damit der DHCP-Dienst auf dem Server ausgeführt werden kann, muss dieser über eine statische IP-Adresse verfügen.

2. Danach installieren Sie den DHCP-Serverdienst auf dem SBS 2003. Öffnen Sie dazu unter SYSTEMSTEUERUNG/SOFTWARE den Link WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN. Markieren Sie den Eintrag NETZWERKDIENSTE und klicken auf DETAILS. Aktivieren Sie dann die Checkbox DHCP-PROTOKOLL und klicken auf OK. Klicken Sie dann auf WEITER, und die Installation wird durchgeführt.
3. Danach nehmen Sie in der DHCP-Konsole in der Verwaltung die erforderlichen Einstellungen und DHCP-Bereichskonfigurationen vor.

8.13.3 Die IP-Adresse für die Internetverbindung von statisch auf dynamisch ändern und umgekehrt

Der Status der IP-Adresse muss dann geändert werden, wenn die durch den DHCP-Server des Internetdienstanbieters zugewiesene dynamische IP-Adresse für den Netzwerkadapter der Internetverbindung auf eine statische umgestellt wird. Dies gilt auch, wenn die Änderung in die umgekehrte Richtung durchgeführt wird.

Hierzu müssen Sie auf dem SBS 2003 unter SYSTEMSTEUERUNG/NETZWERKVERBINDUNGEN die umzukonfigurierende Verbindung markieren und auf INTERNETPROTOKOLL (TCP/IP) klicken. Wählen Sie dann als neue Einstellung entweder STATISCH und tragen die vom Internetdienstanbieter mitgeteilte IP-Adresse ein oder wählen AUTOMATISCH, wenn keine statische IP-Adresse mehr besteht.

Wird ein Router zur Herstellung der Internetverbindung verwendet, so müssen Sie auf diesem die externe Schnittstelle entsprechend mit der statischen oder dynamischen IP-Adresse konfigurieren.

8.13.4 Ändern der DFÜ-Verbindungseinstellungen

Hat sich bei der Verwendung einer DFÜ-Verbindung für den Internetzugriff die Rufnummer für die Verbindungsherstellung geändert, z.B. bei einem Wechsel des Internetdienstanbieters, so müssen Sie

8.14 Der Menüpunkt Erweiterte Verwaltung

Unter dem Menüpunkt ERWEITERTE VERWALTUNG finden Sie weitere wichtige Verwaltungsoptionen für den SBS 2003 sowie dessen Komponenten.

8.14.1 Active Directory-Benutzer und -Computer

Über diese mmc steuern Sie die Struktur der SBS 2003-Domäne (siehe Abbildung 8.67). Im Gegensatz zu einer Domäne unter einem Windows Server 2000 oder 2003 gibt es jedoch einige Unterschiede bezüglich der standardmäßigen Speicherorte.

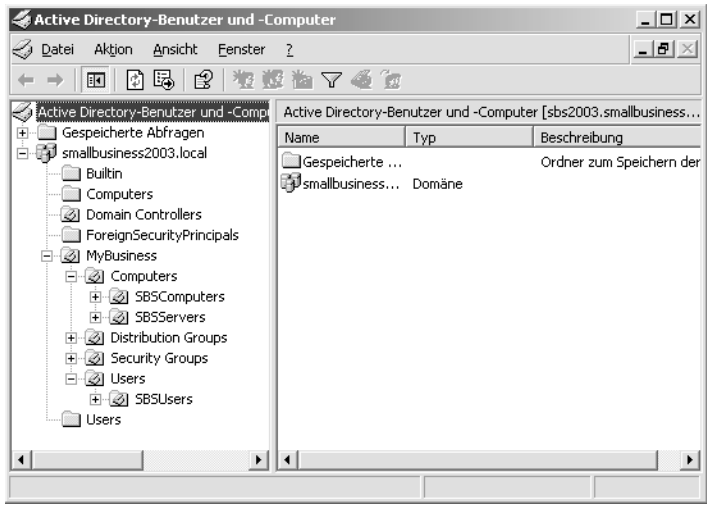


Abbildung 8.67: Die mmc Active Directory-Benutzer und -Computer im SBS 2003

Im Active Directory des SBS befindet sich die zusätzliche Organisationseinheit MYBUSINESS. In dieser OU werden die Active Directory-Objekte gespeichert, die auf dem SBS angelegt werden. Während die Computerobjekte im „normalen" Active Directory in der OU COMPUTERS angelegt werden, befinden diese sich hier unter MYBUSINESS/COMPUTERS und sind dort zusätzlich in Clientcomputer und Server in zwei OUs unterteilt. Weiterhin befinden sich die Sicherheits- und Verteilergruppen jeweils in den eigenen OUs DISTRIBUTION GROUPS und SECURITY GROUPS. Im herkömmlichen Active Directory befinden sich sämtliche Gruppenobjekte zusammen mit den Benutzerobjekten in der OU USERS. Auch die Benutzerobjekte befinden sich nicht in der OU USERS, sondern in MYBUSINESS/USERS. Die Standardcontainer des Active Directory, USERS und COMPUTERS, enthalten keine Objekte.

8.14.2 Gruppenrichtlinienverwaltung

Über diesen Punkt rufen Sie die GPMC auf. Das Group Policy Management wurde bereits ausführlich im Kapitel „Gruppenrichtlinien“ (siehe Kapitel 8.6.10) behandelt.

8.14.3 Computerverwaltung

Über COMPUTERVERWALTUNG (LOKAL) können Sie verschiedene Konfigurationsoptionen in den Bereichen SYSTEM, DATENSPEICHER und DIENSTE UND ANWENDUNGEN vornehmen, die sich nur lokal auf den SBS 2003 beziehen. Dazu zählen beispielsweise die Festplattenverwaltung, der Gerätemanager, die Ereignisanzeige oder das Defragmentierungsprogramm. Weitere Hinweise zu diesen Punkten entnehmen Sie der Windows-Hilfe.

8.14.4 Exchange und POP3-Connector

Über die beiden Verwaltungseinträge EXCHANGE-ORGANISATIONSNAME (EXCHANGE) und POP3-CONNECTOR-MANAGER werden die Verwaltungskonsolen für den Exchange Server 2003 aufgerufen. Die möglichen Optionen wurden bereits ab Kapitel 4.2 und 4.6 ausführlich abgehandelt.

8.14.5 Terminaldienstekonfiguration

Dem Zusammenspiel zwischen dem SBS 2003 und den Terminaldiensten ist das komplette Kapitel 10 gewidmet.

8.14.6 Internetinformationsdienste

Über diesen Punkt rufen Sie die mmc Internetinformationsdienste zur Steuerung des IIS auf. Auf die für den SBS wichtigsten Konfigurationseinstellungen im Rahmen des Exchange Servers und ISA-Servers wurde bereits in den betreffenden Kapiteln eingegangen. Für weitere Hinweise zum IIS sei auf die Windows-Hilfe verwiesen.

8.14.7 Servereinstellungen migrieren

Die Migration der Servereinstellungen wird verwendet, wenn die bestehende Konfiguration des SBS 2003 auf einem anderen Server verwendet werden soll. Sie können die Einstellungen für Internet und E-Mail migrieren sowie Benutzervorlagen und die Konfiguration des Health Monitors importieren und exportieren.

Bedenken Sie beim Exportieren von Vorlagen, dass Sie Benutzergruppen, die Mitglied der Vorlage und auf dem SBS erstellt worden sind, auch auf dem Ziel-SBS erstellt werden müssen. Weitere Hinweise zum Import und Export von Benutzervorlagen finden Sie in Kapitel 8.3.2.

Bei dem Export der Health-Monitor-Einstellungen wird die Konfiguration in einer Datei mit der Endung *.mof* gespeichert. Dabei handelt es sich um eine MSInfo-Datei.

9 Update-Verwaltung im SBS-Netzwerk über Software Update Services Server (SUS)

Die Installation der aktuellen Betriebssystem-Updates und Patches ist ein zentraler Bestandteil zur Sicherung Ihres Netzwerks. Microsoft stellt für diesen Zweck den SUS-Server (Software Update Services) bereit. Momentan ist die Version SUS 1.0 SP1 aktuell. Diese Version gibt es jedoch nur in einer englischen und einer japanischen Sprachversion. Die Version SUS 2.0 wird nach einigen Verzögerungen wohl im ersten Halbjahr des Jahres 2005 bereitgestellt werden. Diese wird es dann auch in einer deutschen Version geben.

9.1 SUS 1.0 und 2.0 sowie Alternativen

Im Folgenden werden die Versionen 1.0 und 2.0 des SUS-Server miteinander verglichen, der Zweck und Nutzen des Patch-Managements erläutert sowie Alternativen zum SUS aufgezeigt.

9.1.1 Wozu Patch-Management?

Beim Einsatz des SUS-Servers – oder auch einer anderen Lösung zum automatischen Patch-Management – im Netzwerk müssen die einzelnen Clients nicht mehr über die Update-Funktion ihre Patches, Updates und Service Packs aus dem Internet beziehen. Der SUS-Server bietet eine zentrale Verwaltung für die automatische Verteilung von Updates an die Clients.

Mit Hilfe des SUS-Servers können Sie Updates für Clients der folgenden Betriebssysteme verteilen:

- Windows 2000 Professional
- Windows 2000 Server
- Windows XP Professional (nicht jedoch Windows XP Home!)
- Windows Server 2003
- SBS 2003

Ältere Windows-Versionen können nicht über den SUS-Server automatisch mit Updates versorgt werden. Für das automatische Update via SUS-Server müssen die Clients Mitglied der SBS-Domäne sein.

Ein Einsatz des SUS-Servers ist in Netzwerken sinnvoll, in denen sich mindestens fünf Clients befinden. Anderenfalls sollten Sie auf den jeweiligen Clients das automatische Windows-Update aktivieren und konfigurieren (siehe Kapitel 9.10). Sofern Sie in Ihrem Unternehmen den Systems Management Server (SMS) 2003 einsetzen, können Sie über

diesen auch die komplette Verteilung und das Management der Patches steuern. Da in der Regel aber in einem SBS-Umfeld kein SMS eingesetzt wird, wird diese Methode an dieser Stelle ausgeklammert.

9.1.2 SUS 1.0 und 2.0 im Vergleich

Wie bereits erwähnt, wird die Version 2.0 des SUS höchstwahrscheinlich im ersten Quartal oder gar erst Halbjahr des Jahres 2005 erscheinen. Nach den bisherigen Verzögerungen seitens Microsoft kann jedoch noch keine Garantie für diesen Termin übernommen werden. Sie können sich allerdings jetzt schon für das Beta-Programm der Windows Update Services direkt bei Microsoft registrieren.

Die Version 2.0 des SUS verfügt über eine Reihe von Neuerungen und Verbesserungen gegenüber der Vorgängerversion. Diese sollen Ihnen im Hinblick darauf, ob diese für Ihr Unternehmen lohnenswert sind, im Folgenden vorgestellt werden.

Die größte Neuerung besteht darin, dass Sie nun nicht nur die Patches, Service Packs und Updates für die Betriebssysteme Windows 2000 (ab Service Pack 3), XP und 2003 automatisch verteilen können, sondern für sämtliche Microsoft-Produkte. Dazu zählen Microsoft Office (Office XP ab SP 2, Office 2003), Exchange Server (2003), SQL Server (2000) oder die MSDE (2000). Selbstverständlich können auch die SUS-Clients automatisch auf die neue Version erneuert werden. Auch die Verteilung von Feature-Sets für msi-basierte Applikationen wird möglich sein.

Auch die Scanfunktion auf den Zielsystemen nach fehlenden Patches und Updates ist verbessert worden. Weiterhin besteht die Möglichkeit, die Updates auch wieder zu deinstallieren sowie eine Installation bzw. Deinstallation bestimmter Patches auf einer Gruppe von Computern vorzunehmen. Vom Administrator aus kann auch geprüft werden, wie oft die einzelnen Benutzer ihr System auf neue Updates hin untersuchen. Zudem kann er auch einen Zeitpunkt bestimmen, zu dem das Update spätestens installiert werden muss bzw. die Installation erzwungen wird.

Auch bei der unvollständigen Übertragung einer Patch-Datei auf den Client wird künftig nur noch der noch nicht übertragene Teil auf den Client kopiert. Dies entlastet den SUS sowie den Netzwerkverkehr. Für die Datenübertragung zwischen dem SUS und dem Microsoft Update-Server sowie auch dem SUS und den Clients kann diese sogar verschlüsselt werden.

Auch die Reporting-Funktion wurde erheblich verbessert und ausgeweitet. Zudem können die Reporte an eine MSDE- oder SQL-Datenbank eingepflegt werden.

Auch der erforderliche Benutzereingriff für die Installation wurde minimiert. So können nun Patches, für die kein Neustart erforderlich ist, ohne Eingriff des Benutzers im Hintergrund installiert werden. Werden mehrere Patches installiert, die einen Neustart erfordern, so werden diese zu einem einzigen Neustart zusammengefasst. Unter Clients mit Windows XP SP2 wird der Neustart sogar erst dann durchgeführt, wenn das System ohnehin neu gestartet wird.

9.2 Die Inventarisierung der Clients

Sofern die Bedingungen für den Einsatz des SUS-Server im SBS 2003-Netzwerk hinsichtlich der Anzahl der Clients und deren Betriebssysteme erfüllt sind, sollten Sie eine Bestandsaufnahme der einzelnen Clients vornehmen. Dazu notieren Sie sich von jedem Client den Namen, das Betriebssystem sowie den Versionsstand bzw. das installierte Service Pack.

Um diese Informationen zu erhalten, öffnen Sie auf dem SBS die SERVERVERWALTUNG und darin den Eintrag CLIENTCOMPUTER. Im rechten Fensterabschnitt sehen Sie eine Liste aller Clients. Doppelklicken Sie den Client, um dessen Eigenschaften zu betrachten. Auf der Registerkarte BETRIEBSSYSTEM sehen Sie das installierte Betriebssystem sowie den Versionsstand. Um die Inventarisierung der Server vorzunehmen, klicken Sie in der SERVERVERWALTUNG auf SERVER-COMPUTER und wiederholen danach die eben beschriebenen Schritte.

Damit Windows 2000-Clients mit dem SUS-Server zusammenarbeiten können, muss auf ihnen mindestens Service Pack 3 installiert sein. Ist dies auf den Clients nicht der Fall, installieren Sie mindestens das Service Pack 3.

9.3 Die Installation des SUS-Servers 1.0 SP1

Bevor Sie den SUS-Server 1.0 installieren, müssen Sie diesen unter der Adresse *http://go.microsoft.com/fwlink/?LinkId=22337* downloaden. Sie finden auch eine aktuelle Version in englischer Sprache auf der Begleit-CD. Die selbstentpackende Installationsdatei ist ungefähr 33 MB groß.

Bevor Sie den SUS-Server auf dem SBS 2003 installieren können, müssen Sie die Installation sowie die Abarbeitung der Aufgabenliste abgeschlossen haben. Insbesondere die Konfiguration der Internetverbindung muss dabei in jedem Fall abgeschlossen sein.

1. Zur Installation des SUS-Servers 1.0 SP1 folgen Sie den Anweisungen des Installationsassistenten. Klicken Sie zunächst auf NEXT und stimmen dann dem Lizenzvertrag zu.
2. Unter CHOOSE SETUP TYPE wählen Sie die Option TYPICAL oder CUSTOM. Über CUSTOM können Sie den Installationspfad für die Programmdateien sowie den Speicherort für die Patches und Updates einzeln bestimmen.
3. Im Fenster LANGUAGE SETTINGS wählen Sie die Sprachen aus, in denen die Updates später downgeloadet werden. Hier sollten Sie unbedingt die Standardeinstellung ALL AVAILABLE LANGUAGES deaktivieren und lieber über SPECIFIC LANGUAGES und CHOOSE LANGUAGES die gewünschte(n) Sprache(n) aus den 31 verfügbaren auswählen. Klicken Sie dann auf NEXT.

4. Danach legen Sie fest, wie neuere Versionen bereits überprüfter Updates behandelt werden sollen. Sie haben die Wahl, den neuen Versionen automatisch (AUTOMATICALLY APPROVE NEW VERSIONS OF PREVIOUSLY APPROVED UPDATES) oder manuell zuzustimmen (I WILL MANUALLY APPROVE NEW VERSIONS OF APPROVED UPDATES). Klicken Sie dann auf NEXT.
5. Im Fenster READY TO INSTALL notieren Sie sich die URL, von der aus die Clients später automatisch die Updates installieren sollen. Diese URL lautet *http://SBSServername*. Klicken Sie dann auf INSTALL. Nach Abschluss der Installation klicken Sie auf FINISH.

   Die Verwaltungsseite des SUS wird über den Link *http://Name des SBS/SUSAdmin* aufgerufen.

Nach Abschluss der Installation erscheint die Verwaltungsseite des SUS. Dort klicken Sie unter OTHER OPTIONS auf SET OPTIONS.

Wird im SBS-Netzwerk der ISA-Server eingesetzt, müssen Sie SUS für die Benutzung des Proxy-Servers konfigurieren. Klicken Sie dazu auf USE A PROXY SERVER TO ACCESS THE INTERNET. Unter USE THE FOLLOWING PROXY SERVER TO ACCESS THE INTERNET tragen Sie die URL und unter PORT die Portnummer 8080 ein.

Mit Hilfe des SUS-Server können Sie Client-Updates in verschiedenen Sprachen an die Clients verteilen. Um die Sprachen auszuwählen, scrollen Sie in diesem Fenster weiter nach unten, markieren die Checkbox und wählen dann die Sprachen aus, die Sie in Ihrem Netzwerk verteilen möchten. Klicken Sie dann auf APPLY und im Fenster VBSCRIPT auf OK.

9.4 Download der verfügbaren Updates auf den SUS-Server

Nach der Installation und Konfiguration des SUS-Servers werden nun die Updates für die Clients downgeloadet. Für den Download eines kompletten Update-Satzes einer Sprache werden ca. 600 MB Festplattenkapazität benötigt. Um den Download zu starten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in einem Browser die Verwaltungsseite des SUS-Servers. Diese erreichen Sie über die Adresse *http://SBSServername/SUSAdmin*.
2. Klicken Sie in der Konsolenstruktur auf SYNCHRONIZE SERVER.
3. Klicken Sie dann auf SYNCHRONIZATION SCHEDULE.
4. Wählen Sie dann unter SYNCHRONIZE USING THIS SCHEDULE einen Zeitplan aus. Standardmäßig wird täglich um 3:00 h nach neuen Updates gesucht. Dabei werden drei Wiederholungen durchgeführt, wenn der Download nicht korrekt durchgeführt werden konnte. Klicken Sie dann auf OK.
5. Klicken Sie dann auf SYNCHRONIZE NOW, um die Updates zu downloaden.

   Die Updates werden jedoch erst an die einzelnen Clients verteilt, nachdem Sie diesen zugestimmt haben. Dieses Verfahren wird in Kapitel 9.7 beschrieben.

6. Im Fenster VBSCRIPT klicken Sie zum Abschluss auf OK. Danach erhalten Sie das Fenster APPROVE UPDATES.

Führen Sie an dieser Stelle noch keine weiteren Schritte durch!

9.5 Die Clients für die Benutzung des SUS-Servers vorbereiten

Auch die Clients müssen für die Benutzung des SUS-Servers zum Update-Download vorbereitet werden, genauer gesagt deren Programm des automatischen Updates, wenn die Clients eines der folgenden Betriebssysteme ausführen:

- Windows 2000 Professional Service Pack 2
- Windows 2000 Server Service Pack 2
- Windows XP Professional ohne Service Pack

Auf den genannten Betriebssystemen mit höheren Service Pack-Ständen sowie Windows Server 2003 müssen Sie keine Aktualisierung des automatischen Update-Programms durchführen. Auf allen älteren Betriebssystemen kann das Update über den SUS nicht ausgeführt werden.

Um eine Aktualisierung auf dem Clientcomputer vorzunehmen, führen Sie die folgenden Schritte durch:

1. Melden Sie sich mit administrativer Berechtigung am Clientcomputer an.
2. Öffnen Sie den Browser und gehen auf die Seite AUTOMATIC UPDATES unter *http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp*
3. Wählen Sie hier die gewünschte Sprachversion für die Installation des *Automatic Update Client* aus. Sie finden den Client in der deutschen Version auch auf der Begleit-CD. Diesen Update-Client müssen Sie auf den eben aufgeführten Betriebssystemen installieren, bevor diese den SUS-Server nutzen können.

9.6 Einstellungen für automatische Updates konfigurieren

Im nächsten Schritt wird festgelegt, wie und wann die Updates im Netzwerk verteilt und installiert werden. Hierzu wird eine Gruppenrichtlinie verwendet. Genauer gesagt konfigurieren Sie die Gruppenrichtlinienobjekte (GPO) *Basic SUS Config* sowie *Scheduled Install SUS Config*.

Das GPO *Basic SUS Config* konfiguriert die Updates so, dass der Benutzer entscheiden kann, wann er die Updates installieren möchte. In der Regel wird dieses GPO auf im Netzwerk vorhandene Server angewendet, es kann jedoch auch auf Clients angewendet werden, wenn es dem Benutzer überlassen sein soll, wann er die Updates installieren möchte.

Ein zeitgesteuerter Download sowie die Installation werden über das GPO *Scheduled Install SUS Config* konfiguriert. Hierbei bestimmen Sie einen Zeitplan, nach dem die Client-Updates vom SUS-Server downgeloadet und installiert werden sollen.

Vor der Anwendung der GPOs müssen Sie sicherstellen, dass sich sämtliche Clientcomputer an der korrekten Lokation befinden, auf die das GPO angewendet werden soll. Im SBS 2003-Netzwerk wird diese Lokation typischerweise die Domäne oder eine Organisationseinheit sein. Befinden sich die Clients nicht in der Domäne, sondern in einer Arbeitsgruppe, können keine GPOs angewendet werden.

Um zu prüfen, ob sich sämtliche Clients in der korrekten Lokation befinden, öffnen Sie in der Serververwaltung unter ERWEITERTE VERWALTUNG die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Stellen Sie sicher, dass Sie für den Vorgang über Administratorrechte verfügen. Doppelklicken Sie dort auf die Domäne und markieren den Eintrag COMPUTERS.

1. In der rechten Fensterhälfte finden Sie eine Liste aller im Container COMPUTERS vorhandenen Computer. Dieses ist der standardmäßige Speicherort für die Computerobjekte im Active Directory unter Windows Server 2000 und 2003. Unter SBS 2003 sollten sich hier jedoch keine Computer befinden. Sollten Sie dort Einträge vorfinden, müssen die Computer verschoben werden.
2. Müssen die Computer verschoben werden, so wählen Sie den Eintrag VERSCHIEBEN aus dem Kontextmenü des jeweiligen Clients.
3. Im Fenster VERSCHIEBEN doppelklicken Sie MYBUSINESS. Doppelklicken Sie dann COMPUTER. Handelt es sich bei dem Computer um einen Client, klicken Sie auf SBS-COMPUTERS, handelt es sich um einen Server, klicken Sie auf SBSSERVERS und dann auf OK.

Als Nächstes erstellen Sie das GPO *Basic SUS Config*.

1. Melden Sie sich hierzu mit Administratorberechtigung an.
2. In der Serververwaltung doppelklicken Sie ERWEITERTE VERWALTUNG und danach GRUPPENRICHTLINIENVERWALTUNG.
3. Doppelklicken Sie dann nacheinander GESAMTSTRUKTUR: IHRDOMÄNENNAME, DOMÄNEN und danach IHRDOMÄNENNAME.
4. Wählen Sie aus dem Kontextmenü von IHRDOMÄNENNAME den Eintrag GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN. Geben Sie in das Textfeld den Namen *Basic SUS Config* ein und klicken auf OK. Das GPO erscheint rechts im Detailabschnitt der mmc.
5. Wählen Sie dort aus dem Kontextmenü von *Basic SUS Config* den Eintrag BEARBEITEN. Damit öffnet sich der Gruppenrichtlinien-Editor.
6. Im Gruppenrichtlinien-Editor öffnen Sie den folgenden Pfad: COMPUTERKONFIGURATION, ADMINISTRATIVE VORLAGEN, WINDOWS-KOMPONENTEN und WINDOWS-UPDATE. Rechts im Detailbereich doppelklicken Sie AUTOMATISCHE UPDATES KONFIGURIEREN.
7. Klicken Sie im Eigenschaftsfenster auf AKTIVIERT. Wählen Sie dann die Option 3 – AUTOM. DOWNLOADEN, ABER VOR INSTALLATION BENACHRICHTIGEN. Klicken Sie dann auf OK.

8. Doppelklicken Sie dann auf INTERNEN PFAD FÜR DEN MICROSOFT-UPDATEDIENST ANGEBEN. Klicken Sie auf AKTIVIERT. Geben Sie in die beiden Textfelder INTERNER UPDATEDIENST ZUM ERMITTELN VON UPDATES sowie INTRANETSERVER FÜR DIE STATISTIKEN *http://SBSServername* ein. Stellen Sie unbedingt sicher, dass Sie den Zusatz http:// hinzugefügt haben.
9. Schließen Sie dann den Gruppenrichtlinien-Editor.

Als Nächstes erstellen Sie wie eben beschrieben das GPO *Scheduled Install SUS Config*.

Dieses GPO für die zeitgesteuerte Installation der Updates kann nicht auf Server, sondern lediglich auf Clients angewendet werden.

1. Öffnen Sie dazu wie eben beschrieben den Gruppenrichtlinien-Editor und klicken unter WINDOWS-UPDATE im Detailbereich auf AUTOMATISCHE UPDATES KONFIGURIEREN.
2. Klicken Sie auf AKTIVIERT und wählen unter AUTOMATISCHES UPDATE KONFIGURIEREN den Eintrag 4 – AUTOM. DOWNLOADEN UND LAUT ZEITPLAN INSTALLIEREN.
3. Unter GEPLANTER INSTALLATIONSTAG belassen Sie es bei der Standardeinstellung 0-Täglich.
4. Unter GEPLANTE INSTALLATIONSZEIT wählen Sie beispielsweise 5:00 h. Idealerweise handelt es sich hier um einen Zeitpunkt, zu dem die Benutzer nicht an ihrem Arbeitsplatz sind und durch die Installation abgelenkt werden können. Klicken Sie dann auf OK.
5. Doppelklicken Sie dann auf INTERNEN PFAD FÜR DEN MICROSOFT-UPDATEDIENST ANGEBEN. Im Eigenschaftsfenster klicken Sie auf AKTIVIERT. Geben Sie dann in die beiden Textboxen INTERNER UPDATEDIENST ZUM ERMITTELN VON UPDATES und INTRANETSERVER FÜR DIE STATISTIKEN *http://SBSServername* ein. Achten Sie darauf, dass http:// hinzugefügt ist. Klicken Sie dann auf OK.
6. Doppelklicken Sie dann GEPLANTE INSTALLATIONEN AUTOMATISCHER UPDATES ERNEUT PLANEN. Es öffnet sich das zugehörige Eigenschaftsfenster.
7. Klicken Sie auf AKTIVIERT und übernehmen den Wert 5 unter NACH DEM SYSTEMSTART WARTEN (MINUTEN). Klicken Sie dann auf OK.
8. Doppelklicken Sie dann KEIN AUTOMATISCHER NEUSTART FÜR GEPLANTE INSTALLATIONEN AUTOMATISCHER UPDATES. Es erscheint das zugehörige Eigenschaftsfenster.
9. Klicken Sie hier auf DEAKTIVIERT und OK. Schließen Sie danach den Gruppenrichtlinien-Editor.

9.7 Die Clients über den SUS-Server updaten

Nach der Konfiguration der GPOs für die Verteilung der Updates an die Clients müssen Sie festlegen, welche Updates Sie für den Download und die Installation auf den Clients zulassen möchten.

Nach dem Download und der Installation müssen Sie sicherstellen, dass die Updates korrekt angekommen sind. Der SUS-Server führt nur einen Download und eine Installation der Updates durch, die auf das Betriebssystem und die Sprachversion des Clients zutreffen. Sobald Microsoft neue Updates bereitstellt, wiederholen Sie den im Folgenden beschriebenen Vorgang.

9.7.1 Testen der Updates

Ein Testen der einzelnen Updates muss nur dann erfolgen, wenn Sie nicht sicher sind, dass ein Update beispielsweise mit einer installierten Applikation oder einem Treiber kompatibel ist. Anderenfalls können Sie mit dem Bestätigen der Updates fortfahren.

9.7.2 Bestätigen der Updates

Im Netzwerk können nur die Updates verteilt werden, die Sie zuvor bestätigt haben. Zum Bestätigen der Updates führen Sie die folgenden Schritte aus:

1. Melden Sie sich mit administrativen Berechtigungen am SBS-Server an. Öffnen Sie STARTMENÜ/PROGRAMME/VERWALTUNG/MICROSOFT SOFTWARE UPDATES SERVICES.
2. Klicken Sie auf APPROVE UPDATES. Scrollen Sie sich durch die Liste der verfügbaren Updates und markieren die Checkboxen der Updates, deren Installation Sie zulassen möchten. Um einen besseren Überblick über die Updates zu bekommen, können Sie diese über die Drop-down-Liste SORT BY nach Installationsstatus, Betriebssystem, Name und Datum sortieren (siehe Abbildung 9.1).

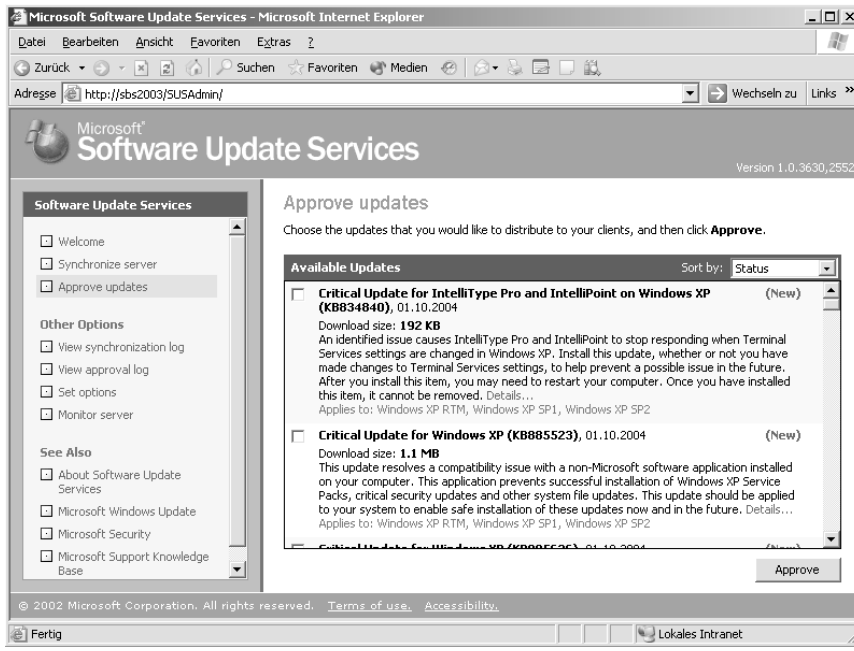


Abbildung 9.1: Auswahl der Updates, die installiert werden sollen

3. Nachdem Sie die Updates ausgewählt haben, klicken Sie auf APPROVE und JA zum Fortfahren. Im Fenster der Lizenzbestimmungen klicken Sie auf ACCEPT. Danach erscheint ein Statusfenster. Klicken Sie hier auf OK. Schließen Sie danach das Fenster der SUS-Verwaltung.

9.7.3 Den Empfang der Updates überprüfen

Nach der Installation des SUS sollten die Clients je nach der eingestellten Zeit ihre Updates vom SUS-Server downgeloadet und installiert haben. Sollte die Installation nach 48 Stunden immer noch nicht erfolgt sein, sei auf das Kapitel 9.7.4, „Fehlersuche“, verwiesen.

Die Installation auf den Clients sollte in jedem Fall korrekt erfolgen, wenn sich die Benutzer abends von ihrem Computer abgemeldet, sämtliche Applikationen geschlossen und Daten gesichert haben. Natürlich dürfen die Benutzer ihren Computer nicht ausschalten.

Haben Sie nicht das GPO *Scheduled Install SUS Config* erstellt, dann folgen Sie den Anweisungen für die Update-Installation auf Servern in Kapitel 9.7.5.

Um zu prüfen, ob die Updates korrekt auf den Clients installiert worden sind, führen Sie die folgenden Schritte durch:

1. Melden Sie sich mit administrativer Berechtigung am Client an. Öffnen Sie STARTMENÜ/EINSTELLUNGEN/SYSTEMSTEUERUNG/SOFTWARE.
2. Unter PROGRAMME ÄNDERN UND ENTFERNEN sehen Sie die Liste der dort installierten Updates. Vergleichen Sie deren Inhalt mit der Liste der bestätigten Updates auf dem SUS-Server.

9.7.4 Fehlersuche: Die Updates werden nicht an die Clients verteilt

Dieses Kapitel gibt Ihnen einige Hilfestellungen, wenn beim Einsatz des SUS-Servers die Updates nicht korrekt auf den Clients installiert werden.

Überprüfen Sie die Gruppenrichtlinieneinstellungen (Windows XP)

Um die Gruppenrichtlinieneinstellungen für die Clients zu überprüfen, stellt Windows XP das Tool *Resultant Set of Policy (RSoP)* bereit. Für Windows 2000 ist dieses nicht verfügbar.

Geben Sie unter Windows XP unter AUSFÜHREN den Befehl rsop.msc ↵ ein. Sie erhalten kurz die Meldung DER RICHTLINIENERGEBNISSATZ WIRD VERARBEITET und danach das Fenster RICHTLINIENERGEBNISSATZ.

Öffnen Sie in der mmc die folgenden Einträge: COMPUTERKONFIGURATION, ADMINISTRATIVE VORLAGEN, WINDOWS-KOMPONENTEN und doppelklicken auf WINDOWS-UPDATE.

Haben Sie das GPO *Scheduled Install SUS Config* erstellt, sollte sich auf dem Client die folgende Einstellung finden (beide GPOs wurden erstellt):

Wurde das GPO *Scheduled Install SUS Config* nicht erstellt, sondern nur das GPO *Basic SUS Config*, finden Sie auf dem Client den folgenden Eintrag:

Sind hier die Einstellungen nicht korrekt angezeigt, so überprüfen Sie die GPOs und erstellen diese, wie in Kapitel Abbildung 9.6 beschrieben, neu. Finden sich hier die korrekten Einträge und werden die Updates dennoch nicht installiert, so sollten Sie das Update des GPO auf dem Client erzwingen.

Update des SUS-bezogenen GPOs erzwingen (Windows XP und 2000)

Das Erzwingen der GPO-Einstellungen auf einem Client ist sowohl unter Windows XP als auch unter Windows 2000 möglich.

Öffnen Sie dazu unter Windows XP die Eingabeaufforderung und geben den Befehl gpupdate/force ↵ ein.

Unter Windows 2000 öffnen Sie die Eingabeaufforderung und geben folgenden Befehl ein: secedit /refreshpolicy machine_policy /enforce ↵

In beiden Fällen werden die GPO-Einstellungen vom SBS-Server auf den Clients aktualisiert.

Haben Sie nicht das GPO *Scheduled Install SUS Config* erstellt, kann es einige Zeit dauern, bis auf dem Clients die zu den installierten Updates zugehörigen Icons sichtbar werden.

9.7.5 Update-Installation auf Servern

Auf den im SBS 2003-Netzwerk vorhandenen Servern inklusive dem SBS 2003 selbst sollten Sie die Updates manuell installieren. So können Sie den Installationszeitpunkt selbst bestimmen, und es kommt zu keiner Überschneidung mit parallel auf den Servern ausgeführten Anwendungen.

Für die manuelle Installation müssen Sie sich mit administrativen Berechtigungen auf dem Server einloggen. In der Taskbar unten rechts sehen Sie das Windows-Update-Symbol, wenn Updates für den Server verfügbar sind. Diese sind zu diesem Zeitpunkt bereits downgeloadet und können installiert werden.

Doppelklicken Sie das Symbol, um mit der Installation zu beginnen.

9.7.6 Fehlersuche: Die Updates werden nicht an die Server verteilt

Ist auch nach 48 Stunden noch kein Update-Symbol verfügbar, führen Sie zur Problemlösung die folgenden Schritte aus:

Überprüfen Sie die Gruppenrichtlinieneinstellungen (Windows Server 2003)

1. Um die Gruppenrichtlinieneinstellungen für die Clients zu überprüfen, stellt Windows Server 2003 das Tool *Resultant Set of Policy (RSoP)* bereit. Für Windows Server 2000 ist dieses nicht verfügbar.

2. Geben Sie unter Windows Server 2003 unter Ausführen den Befehl rsop.msc ↵ ein. Sie erhalten kurz die Meldung DER RICHTLINIENERGEBNISSATZ WIRD VERARBEITET und danach das Fenster RICHTLINIENERGEBNISSATZ.
3. Öffnen Sie in der mmc die folgenden Einträge: COMPUTERKONFIGURATION, ADMINISTRATIVE VORLAGEN, WINDOWS-KOMPONENTEN und doppelklicken auf WINDOWS UPDATE.
4. Auf den Servern sollten sich die folgenden Einstellungen finden:
5. Sind hier die Einstellungen nicht korrekt angezeigt, so überprüfen Sie die GPOs und erstellen diese, wie in Kapitel Abbildung 9.6 beschrieben, neu. Finden sich hier die korrekten Einträge und werden die Updates dennoch nicht installiert, so sollten Sie das Update des GPO auf dem Server erzwingen.

Update des SUS-bezogenen GPO erzwingen (Windows Server 2003 und 2000)

Das Erzwingen der GPO-Einstellungen auf einem Client ist sowohl unter Windows Server 2003 als auch unter Windows Server 2000 möglich.

Öffnen Sie dazu unter Windows Server 2003 die Eingabeaufforderung und geben den Befehl gpupdate/force ↵ ein.

Unter Windows Server 2000 öffnen Sie die Eingabeaufforderung und geben folgenden Befehl ein: secedit /refreshpolicy machine_policy /enforce ↵.

In beiden Fällen werden die GPO-Einstellungen vom SBS-Server auf den Servern aktualisiert. Es kann allerdings einige Stunden dauern, bis auf den Servern das Update-Symbol in der Taskleiste erscheint.

9.8 Die weitere Aktualisierung durch Updates

Der SUS-Server wird nun sämtliche Updates, die Microsoft für die gewählten Betriebssysteme und Sprachversionen bereitstellt, automatisch downloaden. Sie müssen also in festen Intervallen immer wieder die SUS-Verwaltungsseite aufrufen, um festzustellen, ob neue Updates vorliegen, deren Installation Sie bestätigen müssen.

Am sichersten ist es, wenn Sie sich unter *http://www.microsoft.com/security/bulletins/alerts.mspx* eintragen, um automatisch eine E-Mail zu erhalten, wenn Microsoft neue Updates bereitgestellt hat.

Um zu ermitteln, welche neuen Updates verfügbar sind, öffnen Sie die SUS-Verwaltungsseite. Unter APPROVE UPDATES sehen Sie, welche Updates auf den Computer downgeloadet worden sind. Neue Updates sind in der Liste mit dem Status NEW gekennzeichnet.

9.9 Testen von Updates vor der Clientinstallation

In einigen Fällen kann es wichtig sein, die Updates vor der Installation auf den Clients zu testen. Dies ist insbesondere der Fall, wenn nicht sichergestellt werden kann, ob das Update mit einer auf dem Client ausgeführten Applikation kompatibel ist.

Zum Testen der Updates konfigurieren Sie einen oder mehrere Testcomputer, auf denen Sie die kritischen Applikationen installieren. Sie sollten in jedem Fall für jedes eingesetzte Betriebssystem mindestens einen Test-Client haben. Auf diesen Test-Clients werden die Updates direkt von der Microsoft Windows-Update-Seite installiert.

Auf dem Windows XP-Test-Client sollten Sie zusätzlich die Systemwiederherstellung aktivieren. Sollten also Probleme durch die Installation eines Updates auftreten, so können Sie wieder den Systemstatus von vor der Installation herstellen. Um unter Windows XP einen Wiederherstellungspunkt zu setzen, führen Sie die folgenden Schritte aus:

1. Wählen Sie START/HILFE UND SUPPORT. Unter EINE AUFGABE AUSWÄHLEN klicken Sie auf COMPUTERÄNDERUNGEN MIT DER SYSTEMWIEDERHERSTELLUNG RÜCKGÄNGIG MACHEN.
2. Wählen Sie dann die Option EINEN WIEDERHERSTELLUNGSPUNKT ERSTELLEN und klicken auf WEITER.
3. Geben Sie unter BESCHREIBUNG DES WIEDERHERSTELLUNGSPUNKTES einen Namen an und klicken dann auf ERSTELLEN.

Alternativ können Sie unter Windows XP wie auch unter Windows 2000 die Updates über SYSTEMSTEUERUNG/SOFTWARE wieder deinstallieren. Allerdings können einige Updates nicht wieder vom Betriebssystem deinstalliert werden. Weitere Hinweise dazu finden Sie in der Beschreibung des jeweiligen Updates.

Bei weiteren Fragen bezüglich der Kompatibilität von Applikationen mit bestimmten Updates wenden Sie sich an den Hersteller der jeweiligen Applikation.

9.10 Konfiguration des automatischen Updates ohne den Einsatz des SUS-Servers

Soll der SUS-Server im Netzwerk nicht zum Einsatz kommen, so können Sie dennoch das automatische Update für sämtliche Clientcomputer mit den Betriebssystemen Windows 2000 und XP konfigurieren. Auch Server unter Windows Server 2000 und 2003 können für das automatische Update eingerichtet werden.

Da die Konfiguration auf jedem Clientcomputer separat vorgenommen werden muss, ist die Konfiguration sehr zeitaufwändig, wenn Sie über mehr als eine Hand voll Clients verfügen. Im Folgenden wird die Konfiguration des automatischen Updates für Windows XP beschrieben.

1. Öffnen Sie aus den EIGENSCHAFTEN des Arbeitsplatzes die Registerkarte AUTOMATISCHE UPDATES (siehe Abbildung 9.2).
2. Um die automatische Aktualisierung zu aktivieren, markieren Sie den Eintrag AUTOMATISCH (EMPFOHLEN). Danach haben Sie verschiedene Optionen, wie das automatische Update gesteuert werden soll.

Abbildung 9.2: Abbildung 9.2: Die manuelle Konfiguration des Windows-Updates unter Windows XP

- UPDATES DOWNLOADEN, ABER DEN INSTALLATIONSZEITPUNKT MANUELL FESTLEGEN: Sobald vom System bei der Überprüfung der Windows-Update-Seite ein neuer Patch gefunden wird, wird dieser automatisch downgeloadet. Die Installation geschieht jedoch erst zu dem Zeitpunkt, den Sie über das Kalenderelement bestimmt haben.
- BENACHRICHTIGEN, ABER NICHT AUTOMATISCH DOWNLOADEN ODER INSTALLIEREN: Dies ist die Standardeinstellung, wenn Sie das automatische Update auswählen. Hierbei erhalten Sie im System-Tray das Symbol einer Weltkugel, wenn ein neues Update verfügbar ist. Sie müssen dieses Icon doppelklicken, um dann den Download und die Installation zu starten.
- AUTOMATISCHE UPDATES DEAKTIVIEREN: Über diese Option werden der automatische Download sowie die Installation der Patches unterbunden. Haben Sie diese Option gewählt, müssen Sie in jedem Fall sicherstellen, dass Sie den Client über die Microsoft-Update-Seite im Internet regelmäßig auf dem neuesten Stand halten. Den Link zu der Seite finden Sie unter WINDOWS-UPDATE-WEBSITE auf der Registerkarte.

10 Terminalserver in der SBS 2003-Umgebung

Dieses Kapitel beschreibt den Einsatz von Windows Server 2003-Terminalserver in einer SBS 2003-Umgebung. Um innerhalb der SBS-Umgebung Benutzerdesktops zu hosten, müssen Sie einen zusätzlichen Windows Server 2003 oder Windows Server 2000 oder NT Server 4.0 einrichten und diesen als Terminalserver konfigurieren. Ein Ausführen des Terminalservers im Anwendungsmodus direkt auf dem SBS 2003 ist nicht möglich.

Die Installation des Terminalservers sollte am besten erst erfolgen, nachdem die Aufgabenliste des SBS 2003 abgearbeitet worden ist.

10.1 Zweck eines Terminalservers

Ein Windows Server 2003 kann – wie auch schon seine Vorgänger Windows Server 2000 und NT – als Terminalserver eingerichtet werden. In dieser Rolle stellt der Server von einem zentralen Ort aus für die Terminalserver-Clients den Windows-Desktop sowie Windows-basierte Applikationen bereit. Bei dem Terminalserver-Client muss es sich nicht zwangsläufig um einen Windows-Client handeln. Es können auch Macintosh- oder Unix-basierte Clients (z.T. mit Add-Ons) eine Terminalsitzung durchführen.

Jeder Benutzer kann während der Verbindung immer nur seine eigene aktuelle Sitzung sehen.

Bei einer Sitzung zwischen dem Terminalserver und seinem Client wird vom Server die Benutzeroberfläche an den Client übertragen. Der Client sendet an den Server lediglich die Tastatureingaben und Mausklicks. Dadurch wird die zu übertragende Datenmenge zwischen Client und Server auf einem minimalen Level gehalten. Für die Übertragung dieser Daten benutzen der Terminalserver und seine Clients das Remote Desktop Protocol (RDP). Die Verwaltung der Clienteingaben erfolgt auf dem Server und benötigt keinerlei Rechenkapazität des Clientcomputers. Neben der Benutzung des Terminalservers im lokalen Netzwerk können Clients auch über eine Internetverbindung auf den Terminalserver zugreifen. Hierzu wird die Remote-Desktop-Webverbindung benutzt. Weitere Hinweise zu diesem Thema finden Sie in Kapitel 10.10.

Der Einsatz eines Terminalservers bringt somit den Vorteil, dass an die Hardware eines Terminal-Clients gegenüber einem herkömmlichen Client deutlich weniger Ansprüche gestellt werden. Dies spart zum einen Kosten in der Anschaffung der Hardware, zum anderen sparen Sie auch Zeit und Kosten für die Einrichtung und Pflege der Clients.

Ein weiterer Verwendungszweck des Terminalservers kann darin bestehen, spezielle Anwendungen zu hosten und dadurch die Administration der Programme und Daten im Netzwerk zentral an einer Stelle im Netzwerk durchführen zu können. Allerdings müssen Sie in diesem Fall sicherstellen, dass die Applikation auch mit dem Terminalserver kompatibel ist.

10.1.1 Der Terminalserver im SBS-Netzwerk

Auf dem Terminalserver können neben weiteren Windows-Applikationen auch die Komponenten des SBS 2003, nämlich Outlook 2003 oder die Faxdienste, ausgeführt werden. Weitere Hinweise dazu finden Sie in Kapitel 10.8. Beim Einsatz eines Terminalservers in einem SBS-Netzwerk ergibt sich also folgende Konstellation (siehe Abbildung 10.1):

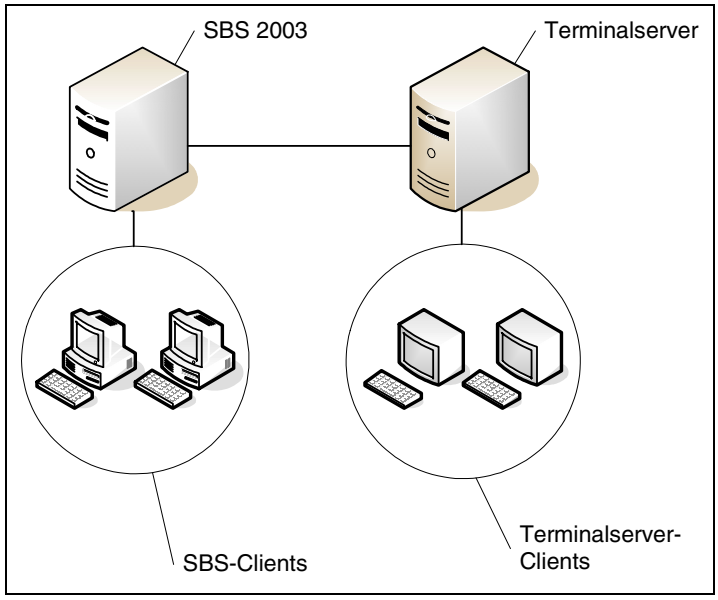


Abbildung 10.1: Der Einsatz eines Terminalservers in einem SBS-Netzwerk

Der Terminalserver wird auf einem anderen Server als der SBS 2003 selbst ausgeführt. So können einerseits die herkömmlichen SBS-Clients direkt auf ihren SBS-Server zugreifen, führen aber ihre Applikationen selbst aus, benutzen den SBS als Datenspeicher und erhalten von diesem ihre Konfigurations- und Sicherheitseinstellungen. Die Terminalserver-Clients stellen eine Verbindung zum Terminalserver her und führen mit dessen Hilfe ihre Anwendungen aus. Über eine konfigurierbare Ordnerumleitung (siehe Kapitel 10.7) können auch die Terminalserver-Clients ihre Daten auf dem SBS 2003 speichern.

10.1.2 Typische Szenarien für den Einsatz eines Terminalservers

Einige typische Beispiele für die Verwendung von Terminalservern sind:

- *Lokationen mit geringer Bandbreite*: In Lokationen, die über keine oder nur eine hochpreisige Verbindung mit hoher Bandbreite verfügen, verbessert der Terminalserver bei Remote-Benutzern die Performance, da nur wenige Daten über die langsame Verbindung übertragen werden müssen.
- *Einsatz von Thin Clients*: Thin Clients sind Computer, die über keine eigene Festplatte verfügen. Sie sind beispielsweise für den Einsatz an Terminals konzipiert und in den Anschaffungs- und Wartungskosten günstiger als ein herkömmlicher Clientcomputer. Thin Clients eignen sich z.B. gut für die Benutzung von Personen, die hauptsächlich Dateneingaben in Datenbanken durchführen, wobei der Terminalserver die eigentliche Datenbankapplikation ausführt.
- *Benutzer fremder Betriebssystemplattformen*: Sofern Sie über Benutzer verfügen, die fast ausschließlich unter einem anderen Betriebssystem als Windows arbeiten, z.B. ein Grafikdesigner, der unter einem Macintosh-System arbeitet, aber dennoch zeitweise den Zugriff auf eine Windows-basierte Applikation benötigt, so müssen Sie für diesen Benutzer keine separate Hardware bereitstellen, damit er die Windows-Software benutzen kann. Er kann über den Terminalserver von seinem Macintosh-System auf die entsprechenden Applikationen zugreifen.
- *Software, die sich in der Entwicklung befindet*: Wird eine Software, die sich noch in der Entwicklung befindet, auf dem Terminalserver gehostet, können Sie sicherstellen, dass für alle Benutzer stets die aktuelle Version zur Verfügung steht, da jedes Update für die Applikation mit wenig Verwaltungsaufwand stets aktuell auf den Server aufgespielt werden kann.

10.2 Planung und Bereitstellung des Terminalservers

Nachdem Sie die Installation und Konfiguration des SBS 2003 komplett abgeschlossen haben, können Sie mit der Planung und Bereitstellung des Terminalservers für die SBS-Domäne beginnen. Diese Planungs- und Bereitstellungsphase kann man in folgende Schritte gliedern:

1. Ansprüche für den Terminalserver und das Netzwerk festlegen
2. Den zusätzlichen Server als Terminalserver einrichten
3. Einrichten eines Administratorkontos und eines Computerkontos für den Terminalserver auf dem SBS 2003 sowie Verbindungsherstellung
4. Einrichten des Terminalserver-Lizenzservers
5. Umleiten des Ordners Eigene Dateien
6. Installation der Client-Applikationen
7. Konfiguration der Terminalserver-Clients

Diese Schritte werden Ihnen in den nächsten Kapiteln näher erläutert.

10.3 Ansprüche an Terminalserver und Netzwerk

Das Einsatzgebiet des Terminalservers ist natürlich abhängig von den Erfordernissen Ihres Unternehmens. Zudem hat das Einsatzgebiet auch Auswirkungen auf die Planung des Servers beispielsweise bezüglich der Hardwareanforderungen. Im Folgenden sehen Sie eine Auflistung typischer Einsatzgebiete:

- *Benutzer für eingeschränkte Aufgabenbereiche*: Verfügen Sie über Benutzer, die lediglich eine bestimmte Aufgabe durchführen und keinen weiteren Zugriff auf andere Ressourcen besitzen sollen, bietet sich für diese ein terminalserver-basierter Arbeitsplatz an.
- *Administrative Verwaltungsaufgaben*: Sollen Administratoren bzw. Personen, die nur zeitweise administrative Aufgaben ausführen, für ihre herkömmlichen Aufgaben lediglich Benutzerrechte am lokalen Client besitzen, bietet es sich an, auf dem Terminalserver Verwaltungswerkzeuge zu installieren, für die Administrator- oder Domänenadministratorberechtigungen erforderlich sind. So muss der Benutzer nur auf dem Terminalserver über die administrativen Berechtigungen verfügen, was aus Sicherheitsaspekten durchaus sinnvoll sein kann.
- *Einsatz von Applikationen, die an ein Betriebssystem gebunden sind*: Verwenden Sie eine bestimmte Applikation, die nur auf einem bestimmten Betriebssystem ausgeführt werden kann, das jedoch nicht auf den Clients installiert ist, so sollten Sie ebenfalls über einen Zugriff über den Terminalserver auf diese Applikation nachdenken. Dieses Szenario ist beispielsweise denkbar, wenn eine Applikation lediglich unter Windows NT 4.0 lauffähig ist, Sie jedoch die Desktops der Benutzer auf Windows 2000 oder XP aktualisieren möchten.
- *Applikationen mit einem großen zentralen Datenpool*: Auch für Applikationen, die regelmäßig auf eine bestimmte zentrale Datenquelle zugreifen, ist der Betrieb auf dem Terminalserver sinnvoll, da somit der Netzwerkverkehr für die einzelnen Datenzugriffe entlastet wird, die nun nicht mehr an die einzelnen Benutzer gesendet werden müssen, sondern zentral auf dem Terminalserver erfolgen.
- *Einsatz von älterer Hardware*: Verwenden Sie noch ältere Hardware, die nicht oder nur bedingt für den Einsatz von Windows 2000 oder Windows XP geeignet ist, können Sie diese Hardware ähnlich wie Thin Clients verwenden, um auf die Applikationen auf dem Terminalserver zuzugreifen. Möglicherweise lassen sich so Kosten bei der Anschaffung neuer Hardware sparen.

Weiterhin stellt sich die Frage, ob der Terminalserver lediglich einzelne Applikationen oder den kompletten Desktop von Clients hosten soll. Meldet sich ein Benutzer an, wird ihm sein kompletter Desktop mit all seinen Einstellungen vom Terminalserver bereitgestellt.

10.4 Den Server als Terminalserver einrichten

Nachdem der neue Server dem Netzwerk hinzugefügt wurde, müssen Sie diesen als Terminalserver konfigurieren. Führen Sie dazu die folgenden Schritte aus:

1. Wählen Sie den Eintrag START/PROGRAMME/VERWALTUNG/SERVERKONFIGURATIONS-ASSISTENT und auf der Willkommensseite sowie den Hinweisen zur Vorbereitung jeweils auf WEITER.

   Auf der Seite Konfigurationsoptionen wählen Sie BENUTZERDEFINIERTE KONFIGURATION. Sie können so selbst die zu installierenden Komponenten auswählen. Klicken Sie dann auf WEITER.

2. Im Fenster SERVERFUNKTION (siehe Abbildung 10.2) markieren Sie den Eintrag TERMINALSERVER. Klicken Sie dann auf WEITER.

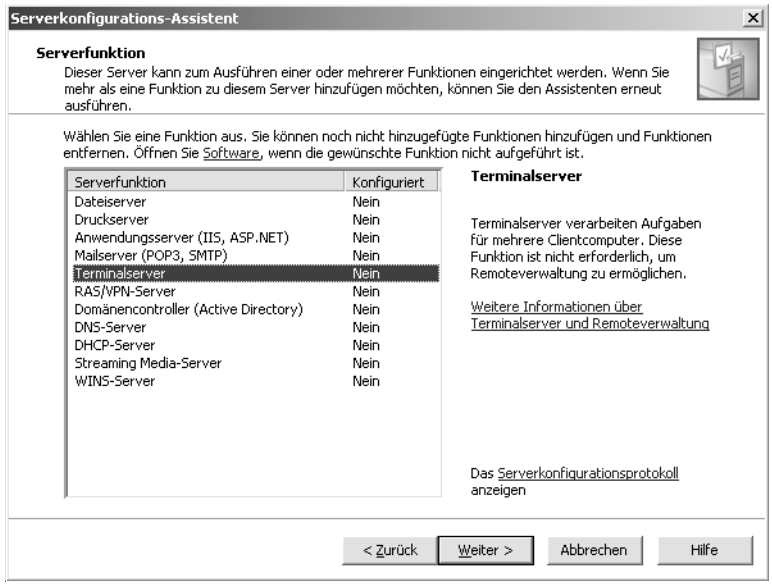


Abbildung 10.2: Dem Mitgliedserver die Rolle des Terminalservers hinzufügen

3. Im Fenster ZUSAMMENFASSUNG DER AUSWAHL klicken Sie erneut auf WEITER. Sie werden im Fenster ASSISTENT FÜR WINDOWS-KOMPONENTEN über den Status der Installation informiert. Sie benötigen für die Installation des Terminalservers das Installationsmedium. Im Zuge der Konfiguration des Servers als Terminalserver erfolgt ein Neustart.
4. Nach Durchführung des Neustarts erhalten Sie den Hinweis, dass dieser Server jetzt ein Terminalserver ist. Klicken Sie auf FERTIG STELLEN. Zusätzlich wird die Hilfe zum Terminalserver angezeigt.

10.5 Einrichten eines Administrator- und Computerkontos sowie Herstellen der Verbindung

Als Nächstes wird auf dem SBS 2003 ein Administrator- und ein Computerkonto für den Terminal Server eingerichtet.

Um das Administratorkonto einzurichten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie in der SERVERVERWALTUNG den Eintrag BENUTZER und klicken auf EINEN BENUTZER HINZUFÜGEN.
2. Damit wird der Assistent zum Hinzufügen eines neuen Benutzers gestartet. Wählen Sie als Benutzervorlage die ADMINISTRATORVORLAGE, und fügen Sie dem Benutzer keinen Computer hinzu. Weitere Hinweise zum Erstellen neuer Benutzer finden Sie in Kapitel 8.2.1.

Um das neue Computerkonto hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der SERVERVERWALTUNG den Eintrag SERVERCOMPUTER und klicken dann auf SERVERCOMPUTER EINRICHTEN.
2. Es wird der Assistent zum Hinzufügen eines neuen Servercomputers gestartet. Folgen Sie den Anweisungen des Assistenten. Weitere Hinweise finden Sie in Kapitel 8.5.2.

Nachdem die beiden Konten eingerichtet worden sind, können Sie den Terminalserver mit dem Netzwerk verbinden. Führen Sie dazu die folgenden Schritte durch:

1. Melden Sie sich mit dem lokalen Administrator an dem Terminalserver an.
2. Starten Sie den Internet Explorer und geben folgende Adresse ein: *http://Name des Terminalservers/ConnectComputer*. Auf der danach erscheinenden Seite klicken Sie auf NETZWERKVERBINDUNG JETZT HERSTELLEN.

Kann die Seite nicht aufgerufen werden, liegt vermutlich eine Sicherheitseinschränkung vor, die standardmäßig jedoch nicht aktiviert ist. Öffnen Sie im Internet Explorer das Menü EXTRAS/INTERNETOPTIONEN und wählen dort die Registerkarte SICHERHEIT. Dort klicken Sie auf VERTRAUENSWÜRDIGE SITES und dann auf SITES. Fügen Sie in das Feld VERTRAUENSWÜRDIGE SITES den Eintrag *http://Name des Terminalservers/connectcomputer* hinzu. Die Checkbox FÜR SITES DIESER ZONE IST EINE SERVERÜBERPRÜFUNG (HTTPS:) ERFORDERLICH muss unbedingt deaktiviert sein.

3. Es erscheint ein Assistent für die Verbindung des Servers mit dem Netzwerk. Benutzen Sie dabei das Konto und Kennwort, das Sie beim Hinzufügen des Benutzers verwendet haben.

10.6 Einrichten des Terminalserver-Lizenzservers

Nachdem der Terminalserver als solcher installiert und mit dem Netzwerk verbunden worden ist, muss auf ihm die Terminalserverlizenzierung eingerichtet werden. Dazu führen Sie folgende Schritte aus:

1. Öffnen Sie den Eintrag START/EINSTELLUNGEN/SYSTEMSTEUERUNG/SOFTWARE. Dort klicken Sie auf WINODWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN.
2. In dem Dialogfeld KOMPONENTEN klicken Sie auf TERMINALSERVERLIZENZIERUNG und dann auf WEITER.
3. Im Fenster TERMINALSERVERLIZENZIERUNG – SETUP (siehe Abbildung 10.3) klicken Sie auf WEITER, wenn Sie die hier angebotenen Standardeinstellungen übernehmen möchten. Sie bestimmen hier den Installationspfad für die Lizenzserverdatenbank sowie den Gültigkeitsbereich des Lizenzservers (DOMÄNE ODER ARBEITSGRUPPE). Standardmäßig wird die Lizenzserverdatenbank im Verzeichnis &systemroot%\System32\Lserver angelegt.

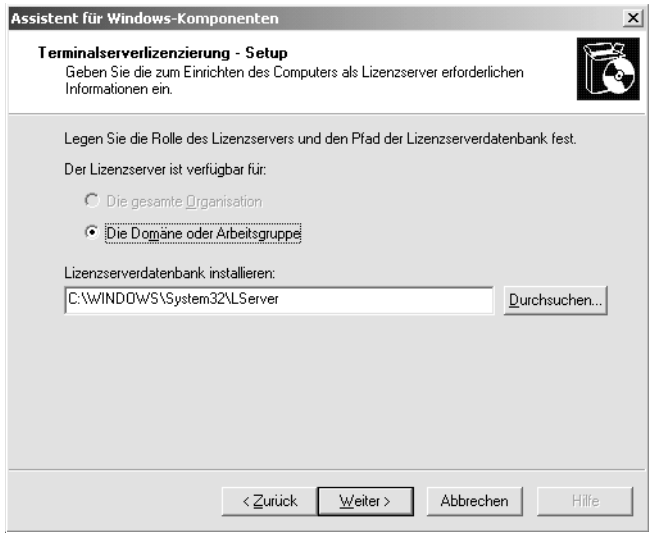


Abbildung 10.3: Installationspfad und Verfügbarkeitsbereich der Lizenzserverdatenbank festlegen

Nachdem die Lizenzserverdatenbank eingerichtet worden ist, dient sie als Speicher für die Terminalserver-Clientlizenzen. Der Terminalserver-Lizenzserver ist in der Lage, für Clients Lizenzen auszustellen, deren Gültigkeit auf 120 Tage beschränkt ist. Als Startdatum gilt das Datum der ersten Clientanmeldung. Ist die Gültigkeit abgelaufen, kann keine Verbindung zum Terminalserver mehr hergestellt werden, sofern dieser Client keinen Terminalserver-Lizenzserver für die Erteilung von Clientlizenzen erreichen kann.

Es ist möglich, die während der Installation festgelegten Eigenschaften des Lizenzierungs-Assistenten wie z.B. Firmeninformationen oder die Aktivierungsmethode nachträglich zu ändern.

Um den Terminalserver-Lizenzserver zu aktivieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie unter START/EINSTELLUNGEN/SYSTEMSTEUERUNG/VERWALTUNG den Eintrag TERMINALSERVERLIZENZIERUNG.
2. In der mmc wählen Sie aus dem Kontextmenü des zu aktivierenden Lizenzservers den Eintrag SERVER AKTIVIEREN. Damit wird der Assistent für die Konfiguration gestartet.
3. Als Aktivierungsmethode (siehe Abbildung 10.4) wählen Sie die Option AUTOMATISCHE VERBINDUNG (EMPFOHLEN) aus. Weitere mögliche Methoden sind Webbrowser und Telefon. Klicken Sie dann auf WEITER.

Abbildung 10.4: Auswahl der Aktivierungsmethode für den Terminalserver-Lizenzserver

4. Es wird dann versucht, eine Internetverbindung mit dem Microsoft Clearinghouse herzustellen. Geben Sie dann Ihren Namen, den Firmennamen und das Land ein. Diese Informationen sind erforderlich. Im Fenster FIRMENINFORMATIONEN tragen Sie Informationen wie E-Mail, Adresse und Ort ein. Bei diesen Informationen handelt es sich um optionale Einträge. Klicken Sie dann auf WEITER.

Was ist Microsoft Clearinghouse?

Bei Microsoft Clearinghouse handelt es sich um eine von Microsoft verwaltete Datenbank zur Verwaltung von Lizenzen. Auf diese Datenbank haben lediglich Mitarbeiter des Microsoft-Kundendienstes Zugriff, um bei Problemen schnelle Hilfe leisten zu können. Mit dieser Microsoft-Datenbank stellt der als Terminalserver-Lizenzserver konfigurierte Server eine Verbindung über das Internet her, um z.B. neue Schlüsselpakete für Clientlizenzen zu erwerben.

Bei der Verbindung über das Internet werden folgende Informationen an Microsoft übermittelt: Firmenname, Name des Benutzers sowie Name und ID des Lizenzservers. An diesen Server werden die Schlüsselpakete gesendet. Die Kommunikation erfolgt über eine gesicherte SSL-Verbindung (Secure Sockets Layer).

Die Aktivierung von Schlüsselpaketen kann auch telefonisch oder per Fax durchgeführt werden. Starten Sie hierzu den Lizenzierungs-Assistenten, wählen aus der Liste Ihr Land aus und rufen die dort angegebene Telefonnummer an. Bei der Aktivierung via Fax müssen Sie im Konfigurationsassistenten eine Seite mit den notwendigen Lizenzierungsinformationen generieren lassen. Die Antwort von Microsoft erfolgt an die angegebene Faxnummer.

5. Sie erhalten dann das Statusfenster DER MICROSOFT AKTIVIERUNGSSERVER WIRD GESUCHT. Danach sollte die Meldung erfolgen, dass der Assistent erfolgreich abgeschlossen worden ist. Achten Sie darauf, dass im Fenster FERTIGSTELLEN DES ASSISTENTEN (siehe Abbildung 10.5) die Checkbox ASSISTENT FÜR DIE TERMINALSERVER-CLIENTLIZENZIERUNG STARTEN aktiviert ist, und klicken auf WEITER.

Abbildung 10.5: Fertigstellen des Assistenten für die Terminalserver-Lizenzserveraktivierung

Das Einrichten der Clientlizenzierung wird im folgenden Kapitel beschrieben.

10.6.1 Einrichten der Lizenzserverdatenbank

Nachdem Sie den Terminalserver-Lizenzserver über den Assistenten konfiguriert haben, können Sie nun Clientlizenzen zum Lizenzserver hinzufügen. Sie benötigen für jeden Client, der eine Verbindung mit dem Terminalserver herstellt, eine Clientzugriffslizenz (CAL). Diese Lizenzen werden auf dem Lizenzserver installiert. Als Zugriffsmethode ist standardmäßig die *Pro-Geräte-Modus*-Lizenzierung aktiviert. Möchten Sie diese Einstellung auf den *Pro-Benutzer-Modus* ändern, öffnen Sie START/PROGRAMME/VERWALTUNG/TERMINALDIENSTKONFIGURATION. Klicken Sie links in der Konsole auf SERVEREINSTELLUNGEN und doppelklicken im rechten Teil auf LIZENZIERUNG. Im Dialogfeld LIZENZIERUNGSMODUS wählen Sie den Eintrag PRO BENUTZER und klicken dann auf OK.

Danach ist noch die Installation der Schlüsselpakete für Clientlizenzen erforderlich. Führen Sie dazu die folgenden Schritte aus:

Die ersten drei Schritte sind nicht erforderlich, wenn der eben beschriebene Assistent zur Lizenzserverkonfiguration bereits gestartet wurde.

1. Öffnen SIE START/PROGRAMME/VERWALTUNG/TERMINALSERVERLIZENZIERUNG.
2. Prüfen Sie, ob die Installationsmethode für den Lizenzserver auf AUTOMATISCH gesetzt wurde. Um dies zu ermitteln, wählen Sie aus dem Kontextmenü des Lizenzservers, für den Sie die Schlüsselpakete installieren möchten, den Eintrag EIGENSCHAFTEN. Falls erforderlich, ändern Sie auf der Registerkarte INSTALLATIONSMETHODE den entsprechenden Eintrag.
3. Wählen Sie dann aus dem Kontextmenü des Lizenzservers den Eintrag LIZENZEN INSTALLIEREN. Klicken Sie dann auf WEITER.
4. Nach der Willkommensmeldung klicken Sie auf WEITER. Im Fenster LIZENZIERUNGSPROGRAMM (siehe Abbildung 10.6) wählen Sie unter LIZENZPROGRAMM die Lizenz aus, durch die Sie die Terminalserver-Clientzugriffslizenzen erworben haben, damit die Schlüsselpakete bereitgestellt werden können. Sie haben hier acht verschiedene Optionen wie z.B. VOLLPRODUKTERWERB, OPEN LICENSE oder SELECT LICENSE zur Auswahl. Klicken Sie dann auf WEITER.
5. Im Fenster LIZENZNUMMER geben Sie die Lizenznummern der erworbenen Lizenzpakete oder die Vertragsnummer einer OPEN License o.Ä. ein. Klicken Sie dann auf WEITER. Das verschlüsselte Clientlizenz-Schlüsselpaket wird über *Microsoft Clearinghouse* auf dem Terminalserver-Lizenzserver installiert.
6. Klicken Sie dann auf FERTIG STELLEN. Ab diesem Zeitpunkt kann der Lizenzserver Lizenzen an die Clients vergeben, die Verbindungen zu einem Terminalserver herstellen.

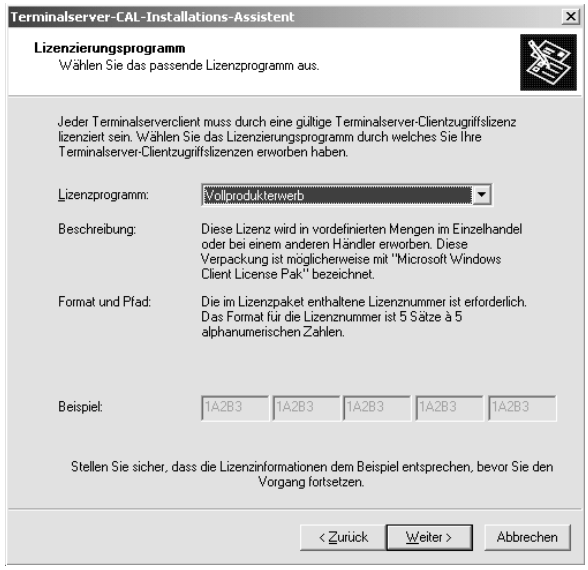


Abbildung 10.6: Auswahl des Lizenzierungsprogramms für den Erwerb der Clientzugriffslizenzen

10.7 Umleiten des Ordners Eigene Dateien

Bei der Verwendung eines Terminalservers werden das Benutzerprofil sowie der Ordner Eigene Dateien auf dem Terminalserver gespeichert. Allerdings sollten Sie den Ordner Eigene Dateien auf den SBS 2003 umleiten. Dies bietet den Vorteil, dass Sie die Ordner über das Backup-Programm des SBS sichern können und keine separate Sicherung von Clientdaten auf dem Terminalserver durchführen müssen. Zusätzlich sollten für diese Ordner Datenträgerkontingente eingerichtet werden.

Eine Umleitung des Ordners Eigene Dateien wirkt sich auf sämtliche Benutzer der SBS-Domäne aus und kann nicht nur für einzelne Benutzer eingerichtet werden.

Um auf dem Terminalserver eine Ordnerumleitung des Ordners Eigene Dateien an den SBS 2003 einzurichten, folgen Sie den Schritten, die bereits in Kapitel 8 beim Thema Ordnerumleitung beschrieben worden sind.

10.8 Installation der Client-Applikationen

Für die Installation auf dem Terminalserver sind sämtliche Client-Applikationen verwendbar, welche die Benutzung des Programms durch Terminalserver-Clients zulassen. Es ist möglich, sämtliche Client-Applikationen, die Bestandteil des SBS sind, auf dem

Terminalserver zu installieren. Im Folgenden finden Sie einige Hinweise zur Installation der Applikationen Outlook 2003, der Faxdienste sowie des Internet Explorers auf dem Terminalserver.

10.8.1 Installation von Outlook 2003

Outlook 2003 kann auf dem Terminalserver vom SBS 2003 aus installiert werden.

Bevor Sie mit der Installation beginnen, prüfen Sie, ob die Ausführung von Applauncher.exe beendet ist. Öffnen Sie dazu den Task-Manager und prüfen auf der Registerkarte PROZESSE, ob dort noch der Eintrag Applauncher.exe angezeigt wird. Beenden Sie diesen Prozess gegebenenfalls.

Für die Installation von Outlook 2003 führen Sie die folgenden Schritte durch:

1. Melden Sie sich mit der Berechtigung eines Domänenadministrators am Terminalserver an.
2. Klicken Sie auf START/AUSFÜHREN und geben \\Servername des SBS an.
3. Doppelklicken Sie CLIENTAPPS und danach OUTLOOK2003. Dann doppelklicken Sie die *Setup.exe* und folgen den Anweisungen.
4. Nach Abschluss der Installation klicken Sie auf WEITER und FERTIG STELLEN. Der mit dem Setup gestartete Assistent muss unbedingt geschlossen sein.

Sobald sich ein Terminalserver-Client das erste Mal am SBS-Netzwerk anmeldet, wird Outlook im Zuge der Clientinstallation automatisch konfiguriert.

Für Terminalserver-Benutzer steht der Exchange-Cachemodus nicht zur Verfügung.

10.8.2 Installation der Faxdienste

Der SBS 2003 kann auch für die Terminalserver-Benutzer als Faxserver eingerichtet werden. Die Installation und Konfiguration des Faxdienstes auf dem SBS haben Sie bereits in Kapitel *4.9* kennen gelernt. Damit die Terminalserver-Benutzer den Faxdienst benutzen können, müssen Sie sowohl die Clients als auch den Terminalserver entsprechend vorbereiten.

Konfiguration des Terminalservers

Zur Konfiguration des Terminalservers führen Sie die folgenden Schritte durch:

1. Auf dem Terminalserver öffnen Sie START/EINSTELLUNGEN/SYSTEMSTEUERUNG/SOFTWARE und klicken dort auf WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN.
2. Wählen Sie die Eintrag FAXDIENSTE und klicken dann auf WEITER.

3. Klicken Sie auf DRUCKER NICHT FREIGEBEN und danach auf WEITER. Im Laufe der Konfiguration müssen Sie möglicherweise das Installationsmedium des Windows Servers 2003 zur Hand haben. Klicken Sie dann auf FERTIG STELLEN.

Die Konfiguration der Terminalserver-Clients für den Faxdienst wird in Kapitel 10.9 beschrieben.

10.8.3 Installation des Internet Explorers

Der Internet Explorer muss im Gegensatz zu den beiden anderen Applikationen nicht auf dem Terminalserver installiert werden. Bei der Installation des SBS-Clients werden automatisch die Einstellungen für die Internetverbindung sowie das Menü FAVORITEN konfiguriert. Im Menü FAVORITEN sind einige Hyperlinks enthalten, die auf Elemente für die Installation von *ActiveX-Steuerelementen* oder *-Zertifikaten* notwendig ist.

10.9 Konfiguration der Clients

Damit die Clients auf den Terminalserver zugreifen können, muss für jeden Client die Remote-Desktop-Verbindung installiert werden. Standardmäßig wird die Remote-Desktop-Verbindung bei der Installation der Betriebssysteme Windows XP, Windows Server 2003 sowie Windows CE automatisch mit installiert. Bei allen älteren Windows-Versionen sowie bei Pocket-PCs muss die Remote-Desktop-Verbindung manuell installiert werden. Führen Sie hierzu folgende Schritte aus:

1. Öffnen Sie auf dem Client START/AUSFÜHREN und geben \\Name des Servers\clientapps ein.
2. Klicken Sie dann auf TSCLIENT.
3. Doppelklicken Sie den Ordner Win32 und darin die Datei *setup.exe*.
4. Der Assistent leitet Sie durch die Installation der Remote-Desktop-Verbindungen.

Nachdem Sie die Remote-Desktop-Verbindung eingerichtet haben, können Sie die Clients auch für die Verwendung der Faxdienste konfigurieren. Führen Sie dazu folgende Schritte aus:

Sobald sich ein Terminalserver-Benutzer anmeldet, ermittelt der Terminalserver den lokalen Drucker des Benutzers und installiert den passenden Druckertreiber auf dem Remote-System.

1. Öffnen Sie auf dem Client START/PROGRAMME/ZUBEHÖR/KOMMUNIKATION/REMOTE-DESKTOP-VERBINDUNG.
2. Melden Sie sich über die Remote-Desktop-Verbindung am Terminalserver an.
3. Öffnen Sie START/EINSTELLUNGEN/DRUCKER UND FAXGERÄTE und dann DRUCKER HINZUFÜGEN. Der Druckerinstallationsassistent wird gestartet, klicken Sie auf WEITER.
4. Wählen Sie die Option NETZWERKDRUCKER ODER DRUCKER, DER AN EINEN ANDEREN COMPUTER ANGESCHLOSSEN IST und klicken auf WEITER.

5. Wählen Sie die Option EINEN DRUCKER IM VERZEICHNIS SUCHEN und klicken dann auf WEITER.
6. Sie erhalten das Dialogfeld DRUCKER SUCHEN. Klicken Sie hier auf die Schaltfläche SUCHEN. In der Suchergebnisliste sollte ein Drucker mit dem Namen FAX vorhanden sein. Wählen Sie diesen Drucker aus und klicken auf OK. Während der Installation müssen Sie möglicherweise das Installationsmedium des Betriebssystems zur Hand haben.
7. Legen Sie den Drucker nicht als Standarddrucker fest (Option NEIN) und klicken dann auf FERTIG STELLEN.

10.10 Die Remote-Desktop-Webverbindung

Bei der Remote-Desktop-Webverbindung handelt es sich um ein ActiveX-Steuerelement, das die Funktionen des herkömmlichen Remote-Desktop beinhaltet und noch erweitert. So ist es möglich, die Funktion einer Applikation bei der Verbindung über das Web auch dann bereitzustellen, wenn die Applikation auf dem Client nicht installiert ist. Ist das ActiveX-Steuerelement in einer Webseite eingebunden, so kann sich der Benutzer über eine TCP/IP- oder Internetverbindung mit dem Terminalserver verbinden und den Windows Desktop innerhalb des Internet Explorers darstellen. Für die Anmeldung via Remote-Desktop-Webverbindung am Terminalserver erhält der Benutzer die folgende Anmeldemaske (siehe Abbildung 10.7):

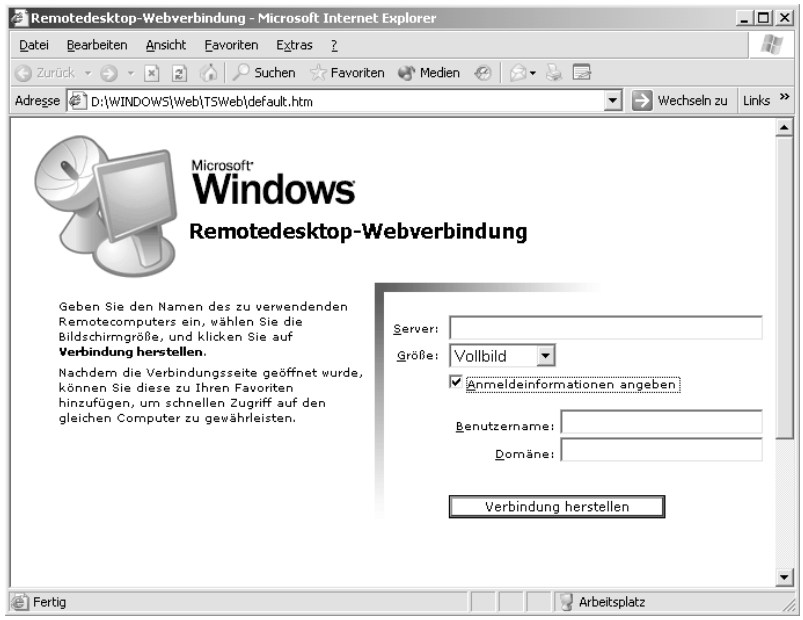


Abbildung 10.7: Die Anmeldemaske für die Anmeldung am Terminalserver über die Remote-Desktop-Webverbindung

Der Einsatz der Remote-Desktop-Webverbindung ist bei Benutzern ohne festen Arbeitsplatz (Roaming Users) sinnvoll. So ist sichergestellt, dass sie von jedem Computer aus, der über einen Internet Explorer verfügt, eine sichere Verbindung zu ihrem eigentlichen Clientcomputer herstellen können.

Möchten Sie Ihren Kunden oder Partnern den Zugriff auf interne Applikationen gewähren, so bietet sich auch der Einsatz der Remote-Desktop-Webverbindung an. Sie müssen damit weder die Applikation auf Ihrem Computer ausführen, noch besteht die Gefahr, dass ein Zugriff auf das interne Netzwerk Ihres Unternehmens erfolgt.

Um die Remote-Desktop-Webverbindung nutzen zu können, muss auf dem Terminalserver der Internet Information Server bzw. die Internetinformationsdienste (IIS) ab der Version 4.0 und höher installiert sein.

Generell ist die Remote-Desktop-Webverbindung für die folgenden Betriebssysteme verwendbar, auf denen ein IIS installiert ist: Windows NT 4.0, Windows 2000, 2000 SP2, 2000SP3, Windows Server 2003 sowie Windows XP und Windows XP Media Center Edition.

Die installierbare Version der Remote-Desktop-Webverbindung finden Sie in der deutschen Version auf der Begleit-CD. Diese installiert das ActiveX-Steuerelement sowie eine Beispielwebsite für das Hosten von webbasierten Clientverbindungen mit den Terminaldiensten unter IIS 4.0 und höher. Benötigen Sie die Komponente in einer anderen Sprache, können Sie diese unter der Adresse *http://www.microsoft.com/downloads/details.aspx?FamilyID=e2ff8fb5-97ff-47bc-bacc-92283b52b310&displaylang=de* downloaden.

10.10.1 Installation und Deinstallation

Bei der Installation unter Windows Server 2003 und Windows XP müssen Sie ein Installationsverzeichnis für die Komponente angeben. Geben Sie dazu den Pfad C:\Windows\Web\TsWeb an (übernehmen Sie *nicht* den vorgeschlagenen Pfad C:\Inetpub\wwwroot\TsWeb) und klicken auf OK. Verwenden Sie unter Windows NT den IIS in der Version 4.0, geben Sie den Pfad C:\Inetpub\wwwroot\TsWeb ein. Bestätigen Sie jeweils, dass dieser Ordner erstellt werden soll, wenn er nicht vorhanden ist.

Um die Komponente wieder zu deinstallieren, wählen Sie unter SYSTEMSTEUERUNG/SOFTWARE den Eintrag REMOTEDESKTOP-WEBVERBINDUNG.

10.10.2 Einbetten des ActiveX-Steuerelements in eine Website

Das ActiveX-Steuerelement wird über html in die betreffende Website eingefügt. Hierzu wird der html-Tag <OBJECT> benutzt. Der Quelltext für die Einbettung kann dabei folgendermaßen aussehen:

```
<OBJECT language="vbscript" ID="MsRdpClient"> CLASSID="CLSID:9059f30f-4eb1-
4bd2-9fdc-36f43a218f4a" CODEBASE="msrdp.cab#version=5,2,xxxx,0 WIDTH=<%
resWidth = Request.QueryString(„rW") if resWidth < 200 or resWidth
VIEWASTEXT > 1600 then resWidth = 800 end if Response.Write resWidth %>
```

```
HEIGHT=<% resHeight = Request.QueryString (rH“) if resHeight < 200 or
resHeight > 1200 then resHeight = 600 end if Response.Write resHeight %>></
OBJECT>
```

Listing 10.1: html-Beispielcode für die Einbettung des ActiveX-Steuerelements in eine Website

In diesem Beispielcode steht der Wert xxxx für die Build-Nummer des Steuerelements. Die Build-Nummer des mitgelieferten ActiveX-Elements lautet 3790. Sie finden die Build-Nummer im Quelltext der Seite default.htm im Installationsverzeichnis, und zwar dort in der Sektion CONNECT.

Unter Codebase ist der Speicherort der Datei *Msrdp.cab* angegeben. Diese Datei enthält den Code für die Remote-Desktop-Webverbindung. Sie befindet sich ebenfalls im Installationsverzeichnis. Sämtliche gültigen Objektparameter für das ActiveX-Steuerelement können Sie betrachten, indem Sie die Datei *Msrdp.ocx* öffnen. Diese Datei befindet sich in der *Msrdp.cab*. Öffnen Sie die Datei *Msrdp.ocx* beispielsweise mit dem Programm *Oleview.exe* oder dem Visual Basic-Objektbrowser.

10.11 Terminalserver auf dem SBS 2003

Auf einem SBS 2003 werden die Terminaldienste über den Remote-Desktop nur im Verwaltungsmodus konfiguriert. Sobald Sie die Konsole TERMINALDIENSTKONFIGURATION in der Verwaltung öffnen und unter SERVEREINSTELLUNGEN die LIZENZIERUNG des Terminalservers ändern möchten, können Sie dort nur den Eintrag REMOTEDESKTOP FÜR VERWALTUNG einstellen (siehe Abbildung 10.8).

Abbildung 10.8: Der Lizenzierungsmodus für einen auf dem SBS 2003 installierten Terminalserver

Sobald Sie dann SYSTEMSTEUERUNG/SOFTWARE/WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN öffnen, wird der Terminalserver nicht als Windows-Komponente angezeigt, wie dies in allen Versionen des Windows Servers 2003 der Fall ist. Dies liegt darin begründet, dass unter SBS 2003 lediglich der Remote-Desktop für den Verwaltungsmodus verfügbar ist. Hierbei handelt es sich um einen Sicherheitsmechanismus, da der SBS 2003 grundsätzlich auf einem Domänencontroller ausgeführt wird und deshalb auf Domänencontrollern lediglich der Verwaltungsmodus, nicht aber der Anwendungsmodus zur Verfügung steht.

Möchten Sie den Terminalserver im SBS 2003-Netzwerk nicht nur im Verwaltungsmodus, sondern auch im Anwendungsmodus einsetzen, müssen Sie, wie weiter oben in diesem Kapitel beschrieben, einen zusätzlichen Windows Server 2003 einrichten und diesen als Terminalserver konfigurieren.

Sie können auch kein Update eines Windows Servers 2000 oder SBS 2000 auf SBS 2003 durchführen, wenn auf diesem der Terminalserver im Applikationsmodus ausgeführt wird. Führen Sie die Installation hingegen direkt über die Datei *Winnt32.exe* aus dem Verzeichnis \I386 der SBS2003 CD1 aus, erhalten Sie keine Warnmeldung bezüglich des Terminalserver-Applikationsservermodus. Stattdessen wird ohne weiteren Hinweis der Remote-Desktop für den Verwaltungsmodus des Terminalservers konfiguriert.

11 Der Business Contact Manager 2003

Bei dem *Business Contact Manager 2003* (BCM) handelt es sich um ein Add-On für Outlook 2003, das Sie für ein effektives Kundenmanagement einsetzen können. BCM bietet die zentrale Verwaltungsmöglichkeit von Geschäftsbeziehungen, Sales-Informationen, Verkaufshistorien und entsprechenden Reporten unter Outlook 2003. Dieses Produkt ist speziell für kleine Unternehmen mit maximal 25 Mitarbeitern konzipiert und passt deshalb ideal in das Einsatzgebiet des SBS 2003. Der BCM kann auch als Erweiterung für das im Lieferumfang des SBS enthaltene Outlook 2003 eingesetzt werden. Der BCM ist auch auf die anderen Office 2003-Produkte abgestimmt und garantiert so eine problemlose und flexible Zusammenarbeit z.B. mit Excel oder Word 2003.

11.1 Die Features des BCM 2003

Der Vorteil der Integration des BCM in Outlook 2003 besteht auch darin, dass Sie die neuen Aufgaben in einer bereits bekannten Umgebung durchführen können. So entfällt eine Lernphase für die effektive Nutzung einer komplett neuen Software.

BCM hilft Unternehmern, Angestellten und Verkaufsmitarbeitern bei der Übersicht, Pflege und Verwaltung der unternehmensbezogen Kontakt- und Verkaufsdaten sowie der Erschließung weiterer Vertriebsmöglichkeiten. Im Einzelnen besitzt BCM folgende Features:

- Die unter dem Office-System 2003 erstellten Daten werden den jeweiligen Kontakten im BCM hinzugefügt, damit sie schneller auffindbar sind.
- Die Office-Daten können unter Outlook 2003 mit BCM geöffnet und betrachtet werden.
- Verkaufs- und kundenbezogene Berichte können nach Excel oder Word 2003 exportiert werden. Ein Import, z.B. von Preis- oder Kundenlisten, ist von Excel 2003 aus möglich.
- Es wird das Senden von Dokumenten an mehrere Empfänger gleichzeitig von Word 2003 sowie Publisher 2003 aus ermöglicht.
- Word und Publisher 2003 bieten eine Vielzahl von Vorlagen für den Versand von Newslettern. Verfolgen Sie den Erfolg dieser Werbemaßnahmen.
- Zu den Kundeninformationen können auch Faxe oder andere eingescannte Dokumente hinzugefügt werden.
- Es können individuell die Sortierungs- und Organisationsoptionen für die bestehenden Daten unter Outlook 2003 angepasst werden.
- Zu allen Vorgängen können Sie Statistiken wie den Verkaufsstatus, den erzielbaren Gewinn oder einen Verkaufsstatus abrufen.
- Über das Aktivitätsprotokoll haben Sie einen schnellen Überblick über alle Aktivitäten, die sich auf einen bestimmten Kunden, Kontakt oder Verkauf beziehen. Dies erleichtert auch die Pflege zusammengehörender Informationen.

- Es können Berichte mit umfangreichen Filterfunktionen erstellt werden. So können Sie z.B. ermitteln, mit welchen Kontakten im letzten Quartal nicht kommuniziert wurde oder welche Verkaufsaussichten für das folgende Quartal bestehen. Es kann auch gewählt werden, welche Informationen angezeigt werden sollen, um die wichtigsten Punkte schnell zu überblicken.

11.2 Die Integration des BCM

Der BCM ist ein Bestandteil der Office Small Business-Edition 2003. BCM kann jedoch auch im Rahmen des Volume Licensing-Programms erworben werden. In einer Office 2003 Home- oder Professional-Version ist der BCM nicht enthalten – entgegen anders lautender Mitteilungen selbst durch Microsoft.

Outlook 2003 mit installiertem BCM kann in E-Mail-Systemen arbeiten, die POP3-, IMAP- oder HTML-basiert sind. BCM kann jedoch nicht verwendet werden, wenn Outlook 2003 zusammen mit einem Exchange-Server verwendet wird. Allerdings hat Microsoft einen Patch bereitgestellt, der unter dem SBS 2003 die Zusammenarbeit mit Outlook unter Exchange ermöglicht.

Unter folgender Adresse bietet Microsoft das BCM-Update an: *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=EAB86AF5-1F5E-4EF3-9691-90F9B870B9B6*. Dieses Update finden Sie auch auf der Begleit-CD.

Der BCM ist eine Umgebung für einen einzelnen Desktop. Es ist nicht möglich, die im BCM erarbeiteten Daten mit anderen Benutzern im Netzwerk auszutauschen, da in kleinen Unternehmen der Datenaustausch nicht unbedingt Priorität besitzt. Wollen Sie zusätzliche Funktionalitäten wie den Austausch der Business-Daten nutzen, sollten Sie auf Microsoft CRM (Customer Relationship Management) updaten. Die bestehenden Daten des BCM mit Outlook können in Microsoft CRM importiert werden. BCM bietet im Gegensatz zu CRM auch nur eine beschränkte Möglichkeit der Anpassung. So können lediglich benutzerdefinierte Ansichten oder Reports erstellt werden.

11.3 Installation des BCM 2003

Dieses Kapitel beschreibt die separate Installation des BCM 2003. Unter Office Small Business Edition 2003 kann der BCM bereits während der Installation aus der Featureliste ausgewählt werden und wird dann mit installiert.

Während der Installation des BCM muss Outlook 2003 geschlossen sein.

1. Als Erstes wird überprüft, ob auf dem System bereits das *.Net-Framework* in der Version 1.1 installiert ist (siehe Abbildung 11.1). Ist dies nicht der Fall, klicken Sie auf OK, um das *.Net-Framework* zu installieren. Anderenfalls kann die Installation des BCM nicht fortgesetzt werden.

Abbildung 11.1: Prüfung, ob bereits das .Net-Framework in der Version 1.1 installiert ist.

Nach Abschluss der Installation des *.Net-Framework* erhalten Sie eine entsprechende Meldung, die Sie mit OK bestätigen.

2. Nach der .Net-Framework-Installation erhalten Sie das Willkommensfenster der Installation.
3. Im Zuge der Installation wählen Sie lediglich das Installationsverzeichnis aus. Standardmäßig schreibt sich der BCM in das Installationsverzeichnis von Outlook 2003.

   Beim ersten Start nach der Installation werden Sie gefragt, ob Sie den BCM auf Ihr aktuelles Outlook-Profil anwenden möchten. Nachdem Sie dies bestätigt haben, wird eine neue Datenbank erstellt.

Nach der Installation des BCM erhalten Sie unter Outlook 2003 das zusätzliche Menü UNTERNEHMENSTOOLS. Zusätzlich wird in der Spalte ALLE E-MAIL-ORDNER der Eintrag BUSINESS CONTACT MANAGER erstellt (siehe Abbildung 11.2).

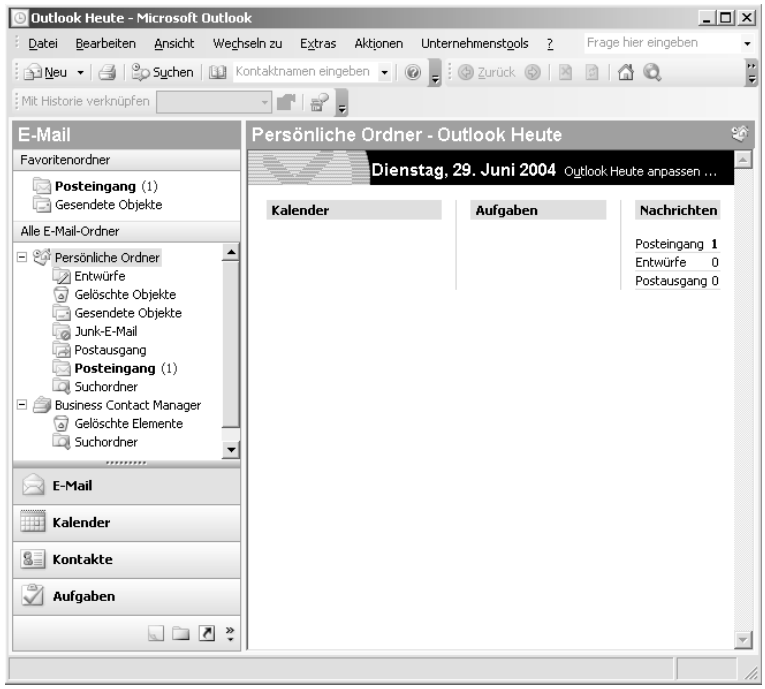


Abbildung 11.2: Outlook 2003 nach der Installation des BCM

11.4 Arbeiten mit dem BCM 2003

In diesem Kapitel werden Sie in die Grundfunktionen des BCM 2003 eingewiesen. Wie bereits erwähnt, ist der BCM komplett in die Oberfläche von Outlook 2003 integriert, so dass Sie eigentlich keine komplett neue Software in der Bedienung erlernen müssen.

Die Bedienung des BCM wird über den Menüpunkt UNTERNEHMENSTOOLS unter Outlook vorgenommen. Dort finden Sie alle verfügbaren Optionen des Programms (siehe Abbildung 11.3).

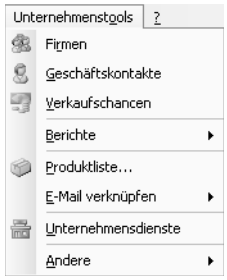


Abbildung 11.3: Das Menü UNTERNEHMENSTOOLS *unter Outlook 2003*

11.4.1 Anlegen der Grunddaten

Um effektiv mit dem BCM arbeiten zu können, sollten Sie in diesen zunächst eine Reihe von Basisdaten eintragen. Dazu gehören Firmeneinträge, Geschäftskontakte, Produktlisten und Verkaufschancen.

Firmen und Geschäftskontakte

Unter FIRMEN und GESCHÄFTSKONTAKTE können Sie neue Einträge vornehmen, die wie die herkömmlichen Kontakte unter Outlook angelegt werden. Unter KONTAKTE können Sie später unter MEINE KONTAKTE zwischen den Einträgen KONTAKTE (dies sind die unter Outlook erstellten) sowie FIRMEN IN BUSINESS CONTACT MANAGER und GESCHÄFTSKONTAKTE IN BUSINESS CONTACT MANAGER wechseln.

Produktliste

Über die PRODUKTLISTE können Sie sämtliche vom Unternehmen angebotenen Produkte eintragen (siehe Abbildung 11.4). Um ein neues Produkt in die Liste aufzunehmen, klicken Sie auf HINZUFÜGEN. Dort geben Sie den Namen des Produkts, eine optionale Beschreibung, den Einzelpreis sowie die Standardmenge an und klicken auf OK. Vorhandene Einträge können auch wieder aus der Produktliste entfernt sowie bearbeitet werden.

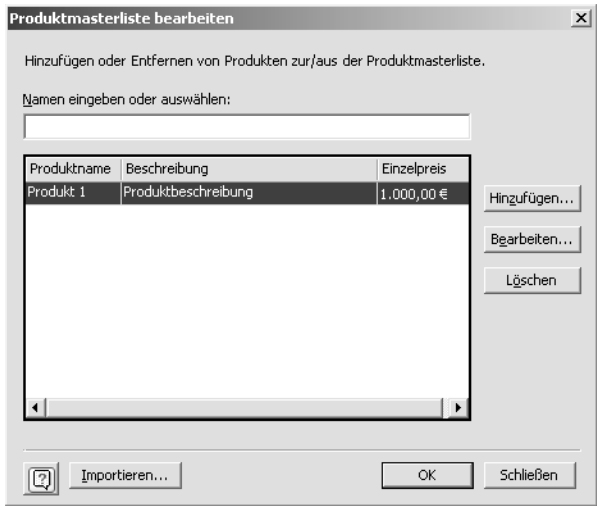


Abbildung 11.4: Das Anlegen der Produktliste

Verkaufschancen

Über VERKAUFSCHANCEN können Sie neue Einträge hinzufügen, die unter AUFGABEN neben den herkömmlichen Outlook-Aufgaben angezeigt werden. Für jede Verkaufschance können Sie umfangreiche Angaben wie den Lead-Ursprung, Mitbewerber, die Vertriebsphase, den erwarteten Umsatz, die Wahrscheinlichkeit, das Enddatum sowie die möglichen Produkte angeben. Zusätzlich können Sie die Verkaufschance mit einer Firma oder einem Geschäftskontakt verknüpfen (siehe Abbildung 11.5).

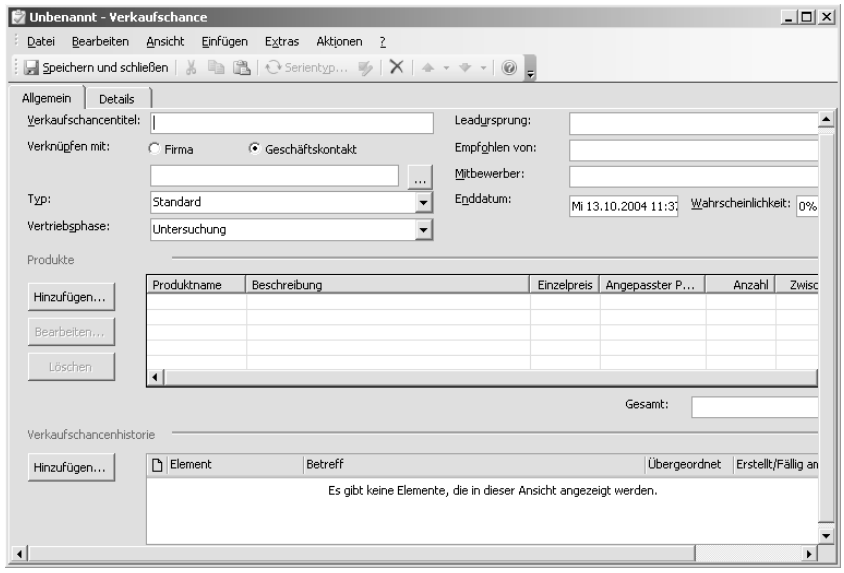


Abbildung 11.5: Die Dateneingabemaske für eine Verkaufschance

11.4.2 Berichte

Berichte können für die vier Bereiche GESCHÄFTSKONTAKTE, FIRMEN, VERKAUFSCHANCEN sowie ANDERE erstellt werden. Dabei können Sie die Berichte nach verschiedenen Kategorien wie Status, Bewertung, Kategorie oder Telefonlisten erstellen. Die VERKAUFSCHANCEN können nach Verkaufstrend, Chancen nach Produkt und Historien aufgelistet werden. Unter ANDERE können Sie Berichte über Lead-Ursprünge sowie Geschäftsaufgabenlisten erstellen.

11.4.3 Weitere Funktionen

Über den Menüpunkt E-MAIL VERKNÜPFEN können Sie eingehende und ausgehende E-Mails automatisch mit der Historie der Firmen- oder Geschäftskontakte verknüpfen. Hierzu wählen Sie die persönlichen Ordner aus, aus denen der BCM die Verknüpfungen herstellen soll. Neben der automatischen Funktion können Sie auch über VORHANDENE E-MAIL VERKNÜPFEN manuell die Ordner auswählen sowie zusätzlich eine Datumsangabe festlegen. So werden alle E-Mails für die Verknüpfung ignoriert, die älter als das angegebene Datum sind. Klicken Sie dann auf STARTEN, um die Verknüpfungen erstellen zu lassen.

Über den Menüpunkt UNTERNEHMENSDIENSTE gelangen Sie auf die Website des BCM. Dort finden Sie Tipps und Tricks für die Arbeit mit dem BCM, Vorlagen für Office sowie weitere Informationen zu dem Produkt.

Unter ANDERE/GESCHÄFTSHISTORIE können Sie die Journalfunktion aufrufen. Der BCM hat hier einen eigenen Eintrag neben dem standardmäßigen Outlook-Journal unter MEINE JOURNALE erstellt.

Weiterhin können Sie über ANDERE/GELÖSCHTE ELEMENTE den Papierkorb des BCM anzeigen. In diesem befinden sich nur die gelöschten Elemente des BCM, nicht jedoch die von Outlook 2003. So ist ein schnelleres Auffinden der Objekte sichergestellt.

12 Eine Sicherheitsstrategie für den SBS 2003

Dieses Kapitel gibt Ihnen eine Übersicht über grundlegende Sicherheitsstrategien, die Sie zum Schutze des SBS 2003-Netzwerks anwenden sollten. Da die verschiedenen Punkte größtenteils bereits im Kontext der einzelnen Kapitel besprochen worden sind, erfolgt hier die Darstellung eher anhand einer Checkliste mit Verweis auf die einzelnen Kapitel.

- Überprüfen Sie Ihre Netzwerktopologie und die daraus resultierende Konfiguration der Firewall.
- Absichern des Routers.
- Überprüfen Sie auf dem SBS 2003 die Netzwerk-, E-Mail-, Firewall- und Webdienste.
- Sorgen Sie mit Hilfe des automatischen Software-Updates für sichere Betriebssysteme des Servers und der Clients.
- Implementieren Sie mit Hilfe der Kennwortrichtlinie sichere Passwörter.
- Sichern Sie den Server, indem Sie den Remote-Zugriff auf den SBS sowie das SBS-Netzwerk steuern.
- Prüfen Sie, ob für die Benutzer auch nur die minimal notwendigen Berechtigungen vergeben worden sind, und beschränken Sie die Benutzerrechte.
- Ändern Sie den Kontonamen für das vordefinierte Administratorkonto, und treffen Sie weitere Sicherheitsmaßnahmen für die Verwendung des Kontos.
- Sichern Sie den Server, auf dem der SBS 2003 ausgeführt wird.
- Überwachen Sie auf dem SBS 2003 die Sicherheits- und Systemereignisse.

12.1 Überprüfen der Netzwerktopologie

Um das Netzwerk effektiv abzusichern, ist zunächst eine Überprüfung der vorhandenen oder aufzubauenden Netzwerkstruktur erforderlich. Dabei ist zu unterscheiden, ob Sie für die Internetverbindung eine Wählverbindung oder eine Breitbandverbindung benutzen. Zum Schutz der Wählverbindung beachten Sie besonders die Hinweise in Kapitel Abbildung 12.3.

Bei Verwendung einer Breitbandverbindung wird danach unterschieden, ob der SBS 2003 über eine Netzwerkkarte für den LAN-Verkehr und einen Router mit Firewall-Funktion für den Internetverkehr verfügt oder ob im SBS 2003 zwei Netzwerkarten vorhanden sind. In letzterem Fall benutzt der Server die interne Firewall, die vom SBS 2003 bereitgestellt wird.

12.1.1 Verwenden eines Routers und einer Firewall für die Breitbandverbindung

Befindet sich im SBS 2003 lediglich eine Netzwerkkarte, sollte die Netzwerktopologie folgendermaßen aussehen (siehe Abbildung 12.1):

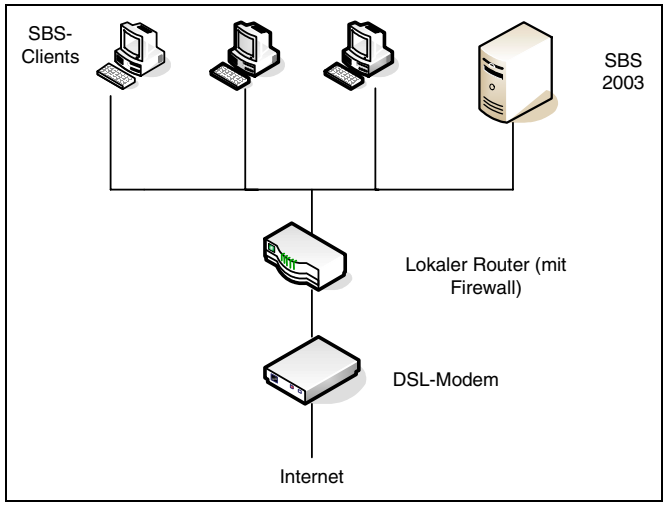


Abbildung 12.1: Einsatz eines Routers und einer Firewall im SBS 2003-Netzwerk

In diesem Szenario können Sie nicht die integrierte Firewall des SBS 2003 benutzen, da der SBS nicht als Gateway zwischen Internet und den Clients fungiert. Deshalb muss entweder der Router über eine Firewall-Funktion verfügen, oder Sie müssen eine externe Firewall einsetzen. Auf der Firewall müssen Sie die Ports öffnen, die für die Funktion des SBS 2003 notwendig sind. Eine Übersicht dieser Ports finden Sie in Tabelle 12.1.

12.1.2 Verwenden der SBS 2003-integrierten Firewall

Verfügt der SBS 2003 über zwei Netzwerkkarten, so muss das Netzwerk folgendermaßen (siehe Abbildung) konfiguriert sein, damit die SBS 2003-integrierte Firewall mit einer Breitbandverbindung korrekt arbeiten kann (siehe Abbildung 12.2).

Für die Nutzung der integrierten Firewall verbinden Sie eine Netzwerkkarte des SBS 2003 über einen Switch oder Hub mit dem lokalen Netzwerk. Die andere Netzwerkkarte wird mit dem Gerät zur Herstellung der Internetverbindung, beispielsweise einem DSL-Modem, verbunden.

Auch in diesem Szenario ist es möglich, zusätzlich zur Firewall des SBS 2003 noch eine externe Firewall einzusetzen. Dabei kann es sich um einen Router mit Firewall-Funktionalität oder um eine reine Firewall handeln. Beachten Sie dabei die Hinweise in Kapitel 12.2.

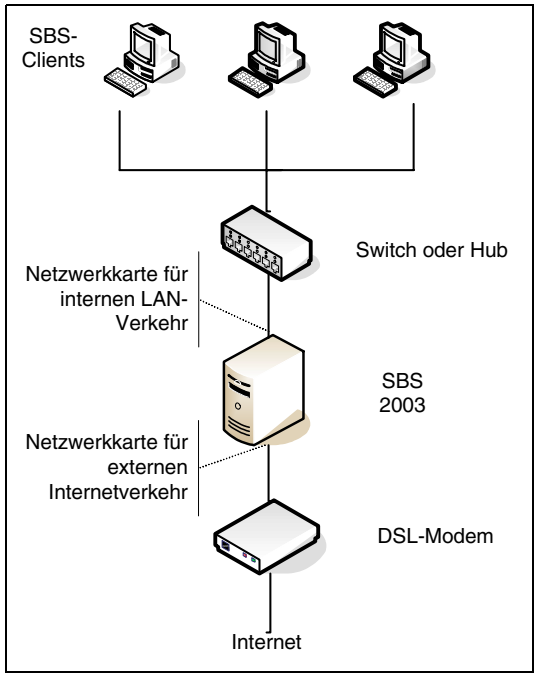


Abbildung 12.2: Verwendung der SBS 2003-integrierten Firewall bei einem SBS mit zwei Netzwerkkarten

Im Assistenten zur Herstellung der Internetverbindung in der Aufgabenliste müssen Sie für dieses Szenario als Verbindungstyp BREITBANDVERBINDUNG (siehe Abbildung 2.19) wählen. Verwenden Sie zusätzlich noch einen Router mit Firewall-Funktionalität, stellen Sie sicher, dass Sie die Option EIN LOKALES ROUTERGERÄT MIT EINER IP-ADRESSE (siehe Abbildung 2.20) wählen.

12.2 Absichern des Routers

Verwenden Sie für die Internetverbindung einen Router, der gleichzeitig noch als Firewall und als Wireless Access Point dient, so müssen Sie eine korrekte, sichere Konfiguration dieses Geräts sicherstellen.

12.2.1 Absichern des Wireless Access Points (Basisstation)

Verfügt der Router zugleich auch über das Feature eines Wireless Access Points und werden in ihrem Unternehmen keine Wireless-Geräte eingesetzt, sollten Sie die Funktionalität des Routers unbedingt abschalten. Ansonsten besteht das Risiko, dass sich fremde Benutzer unautorisiert Zugang zu Ihrem Netzwerk verschaffen können. Genaue Hinweise zum Deaktivieren dieses Features finden Sie in der Dokumentation Ihres Routers. Benutzern Sie hingegen Wireless-Geräte, so müssen Sie den Access Point entsprechend absichern, um den unautorisierten Zugriff auszuschließen oder zumindest stark zu minimieren.

Dazu zählt, dass Sie zunächst ein Passwort für die Konfiguration des Routers vergeben. Dabei sollte es sich nicht um das Standardpasswort handeln, das die Hersteller für ihre Geräte vergeben. Als Nächstes sollten Sie die Verschlüsselung aktivieren. Dazu können Sie entweder die *WEP-Verschlüsselung* (Wired Equivalent Privacy) oder die *802.1x-Authentifizierung* anwenden. Die 802.1x-Authentifizierung ist neuer und sicherer als WEP. Bei beiden Verfahren handelt es sich um ein Sicherheitsprotokoll, bei dem die Daten bei der Übertragung über die Radiowellen von einem Gerät zum anderen verschlüsselt werden. Bei der WEP-Verschlüsselung müssen Sie manuell einen Sicherheitsschlüssel erstellen, der dann zwischen dem Access Point und den Wireless-Geräten ausgetauscht wird. Unter 802.1x wird dieser Sicherheitsschlüssel automatisch generiert. Wenn Sie bei der WEP-Verschlüsselung die Wahl zwischen einem 64-Bit- und einem 128-Bit-Schlüssel haben, sollten Sie immer den längeren Schlüssel benutzen.

Für weitere Sicherheit sollten Sie die MAC-Filterung (Media Access Control) aktivieren. Hierzu müssen Sie die MAC-Adressen der im Netzwerk verwendeten Wireless-Karten herausfinden und die Liste der Adressen im Router eintragen. Damit wird sichergestellt, dass nur die Karten mit den aufgelisteten MAC-Adressen Zugriff auf den Access Point haben.

Um die MAC-Adresse einer Netzwerkkarte auszulesen, geben Sie an der Eingabeaufforderung den Befehl ipconfig /all ein. Die MAC-Adresse wird unter Physikalische Adresse (siehe Abbildung) angezeigt.

Abbildung 12.3: Das Ermitteln der MAC-Adresse einer Wireless-Netzwerkkarte

Haben Sie die MAC-Filterung aktiviert, müssen Sie die Liste auf dem Router aktualisieren, sobald Sie eine neue Wireless-Karte im Netzwerk hinzufügen oder eine Karte entfernen.

12.2.2 Die Firewallkonfiguration auf dem Router

In diesem Kapitel wird die Konfiguration einer Firewall für den Einsatz mit SBS 2003 beschrieben. Auf dem SBS 2003 werden automatisch sämtliche Ports konfiguriert, nachdem Sie in der Aufgabenliste den Assistenten HERSTELLEN DER INTERNETVERBINDUNG abgeschlossen haben.

Das Öffnen von Ports auf einer Firewall wird in den entsprechenden Dokumentationen auch als Port Forwarding oder Weiterleitung bezeichnet. Im Folgenden finden Sie eine Übersicht über die im SBS 2003-Netzwerk möglicherweise benötigten Ports. Wird ein Port nicht benötigt, so sperren Sie diesen auf der Firewall des Routers.

Sofern Sie nicht die Premium Edition des SBS 2003 erworben haben und somit nicht den ISA Server 2000 als Firewall einsetzen, dürfte in den meisten kleineren Unternehmen ein separates Firewall-Gerät vorhanden sein. Dieses kann unter bestimmten Umständen auch gemeinsam mit der in den SBS 2003 integrierten Firewall betrieben werden. Oftmals handelt es sich dabei um eine Kombination aus Firewall und DHCP-Server.

Ist dieses Gerät UPnP-fähig (Universal Plug & Play), so wird die Konfiguration der verschiedenen vom SBS 2003 benötigten Ports über den Assistenten E-Mail und Internetverbindung vorgenommen. Ist das Gerät nicht UPnP-fähig, so müssen Sie die Konfiguration der Firewall manuell durchführen.

Dient die Firewall zusätzlich auch als Router und ist der SBS über eine Netzwerkkarte mit dem lokalen Netzwerk, über die andere mit dem Internet verbunden, so können Sie sowohl die Firewall des SBS 2003 oder die Firewall-Funktionalität des Kombigeräts oder auch beide gemeinsam nutzen.

Tabelle 12.1 zeigt Ihnen eine Übersicht über die vom SBS 2003 für die verschiedenen Dienste genutzten Portnummern. Bei sämtlichen Diensten handelt es sich um TCP-Protokolle.

Portnummer	Dienst	Beschreibung
21	FTP (File Transfer Protocol)	Bevor Sie den Server als FTP-Server einrichten, müssen Sie zunächst den FTP-Dienst hinzufügen und einrichten.
25	E-Mail	Maileingang und -ausgang über das SMTP-Protokoll (Simple Mail Transfer Protocol).
80 (http)	Webserver	Internetzugriff, Outlook Web Access (OWA), Outlook Mobile Access (OMA), Aufruf von Leistungs- und Nutzungsberichten des SBS, Firmenwebseite (wwwroot) sowie Outlook-Zugriff über das Internet (RPC) ohne VPN-Verbindung.
443 (https)	Webserver; Remote-Webarbeitsplatz	http-Anfragen über SSL (Secure Sockets Layer); Webarbeitsplatz siehe die betreffende Spalte dieser Tabelle.
444	SharePoint Services-Intranet-Webseite	Sicherung der Client-Server-Kommunikation beim Zugriff auf die Intranet-Webseite der Firma sowie weitere unter *http://companyweb* bereitgestellte Seiten.
1723	VPN (Virtual Private Network)	Aufbau einer sicheren Verbindung von Remote-Clients zum Firmennetzwerk.

Portnummer	Dienst	Beschreibung
3389	Terminaldienste	Benutzung der Terminaldienste des SBS 2003 durch Remote-Clients.
4125	Remote-Webarbeits-platz	Verbindung über Outlook Web Access (OWA) zum lokalen Netzwerk, Remote-Desktop-Verbindung zu Clients des lokalen Netzwerks, Zugriff auf die Intranet-Webseite der SharePoint Services sowie Herunterladen des Verbindungsmanagers für die Konfiguration des Remote-Zugriffs.

Tabelle 12.1: Übersicht über die im SBS 2003-Netzwerk erforderlichen Ports

Benötigen Sie für bestimmte Applikationen weitere Ports, so müssen Sie diese ebenfalls auf der Firewall freischalten. Eine Übersicht über alle verfügbaren und von bestimmten Applikationen oder Diensten benutzten Ports finden Sie unter *http://www.iana.org/assignments/port-numbers*.

Sofern der Router auch die Funktionalität des Loggings unterstützt, sollten Sie dieses ebenfalls aktivieren und die Log-Dateien auswerten.

12.3 Prüfen der Internet-, E-Mail-, Netzwerk- und Firewall-Dienste auf dem SBS 2003

Ein weiteres Sicherheitsrisiko stellen nicht optimal konfigurierte Internet-, E-Mail-, Netzwerk- und Firewall-Dienste dar.

12.3.1 Prüfen der Firewall-Konfiguration

Für die Konfiguration der Firewall-Fähigkeit des SBS 2003 wird ein Assistent verwendet. In der Standardversion des SBS wird der Standard-Firewall-Dienst im Routing- und RAS-Dienst konfiguriert, in der Premium-Version der ISA-Server.

Bei der Auswahl der verfügbaren Dienste sollten Sie auch immer daran denken, nur die notwendigsten zuzulassen. Wenn Sie beispielsweise den Benutzern den Remote-Webarbeitsplatz zur Verfügung stellen, sollten Sie darüber nachdenken, ob Sie parallel dazu überhaupt noch eine VPN-Verbindung anbieten sollten.

Wenn Sie über den Assistenten zur Herstellung der Internetverbindung entweder den Zugriff über das Internet auf die Firmenwebsite (wwwroot) oder die Intranetsite der Windows SharePoint-Dienste (siehe Abbildung) gestatten, kann es passieren, dass die Anmeldeseite für den Remote-Webarbeitsplatz in Internetsuchmaschinen wie beispielsweise Google aufgelistet wird.

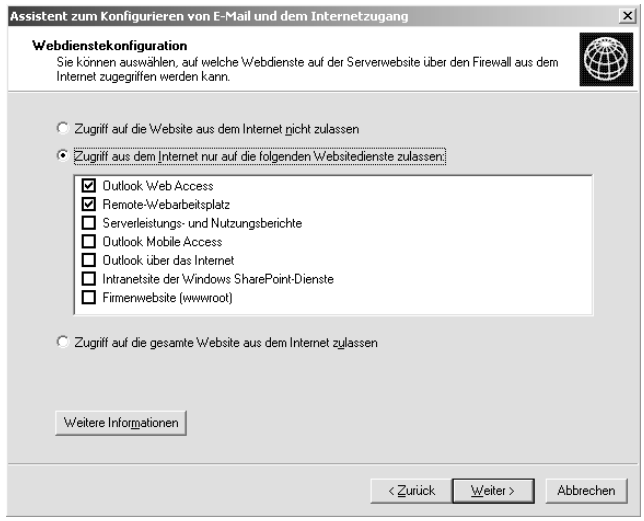


Abbildung 12.4: Auswahl der Komponenten, auf die über das Internet zugegriffen werden darf

Sobald Sie also die Firmenwebsite für den Zugriff über das Internet bereitgestellt haben, können so genannte Web Robots automatisch nach Websites und Dokumenten suchen, indem Sie auf den veröffentlichten Seiten den Hyperlinks folgen.

Um den Web Robots die Suche und Katalogisierung der Websites oder Teilen daraus zu untersagen, müssen Sie eine bestimmte Textdatei namens *robots.txt* mit einem beliebigen Texteditor erstellen und im Verzeichnis der Standardwebsite speichern.

Damit die Web Robots die Datei *robots.txt* lesen können, müssen Sie im Assistenten zur Herstellung der Internetverbindung die Firmenwebsite wwwroot veröffentlichen.

Das folgende Listing zeigt den Inhalt der *robots.txt*, so dass von den Web Robots nur noch der Inhalt der Firmenwebsite, jedoch nicht mehr der internen Websites wie z.B. dem Remote-Webarbeitsplatz angezeigt wird.

```
User-agent: *
Disallow:  /_vti_bin/
Disallow:  /clienthelp/
Disallow:  /exchweb/
Disallow:  /remote/
Disallow:  /tsweb/
Disallow:  /aspnet_client/
Disallow:  /images/
Disallow:  /_private/
Disallow:  /_vti_cnf/
Disallow:  /_vti_log/
Disallow:  /_vti_pvt/
Disallow:  /_vti_script/
Disallow:  /_vti_txt/
```

Listing 12.1: Beispiel für die Datei robots.txt

12.3.2 E-Mail-Anhänge verwalten

Weiterhin sollten Sie das Feature des Exchange Servers 2003 anwenden, das es ermöglicht, bestimmte Dateitypen aus E-Mail-Anhängen automatisch zu entfernen, bevor der Benutzer diesen Anhang öffnen und damit möglicherweise ein Sicherheitsrisiko provozieren kann. Dieses Feature stellen Sie ebenfalls über den Assistenten zur Herstellung der Internetverbindung ein (siehe Abbildung).

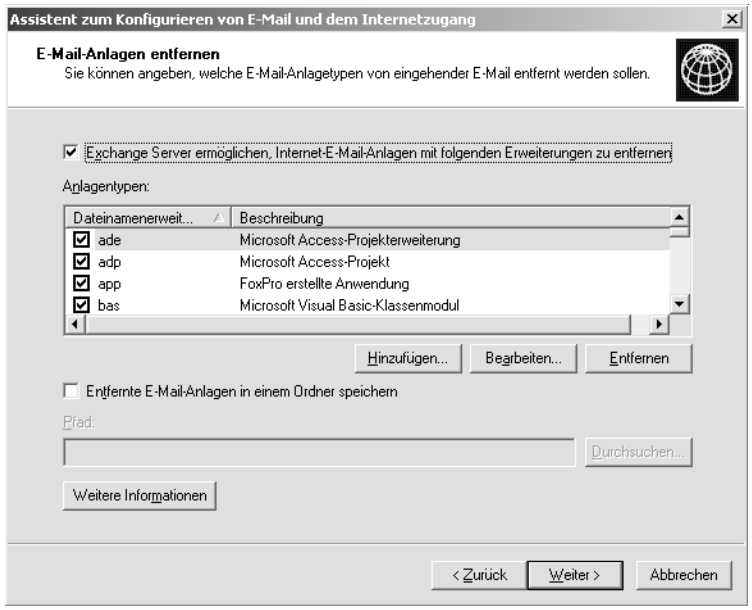


Abbildung 12.5: Die Auswahl von Dateitypen, die als Dateianhang nicht an den Benutzer weitergeleitet werden sollen

Die Einstellungen der Dateitypen können Sie jederzeit ändern, indem Sie den Assistenten erneut starten.

12.3.3 Konfiguration der TCP/IP-Filterung

Die TCP/IP-Filterung wird verwendet, um eingehende Zugriffe zu steuern. Diese Methode ist aus Sicherheitsaspekten sehr empfehlenswert, da sie im Kernelmodus abläuft. Andere Steuermechanismen, wie z.B. IPSec-Richtlinienfilter oder Routing- und RAS-Server, werden im Benutzermodus oder Arbeitsstations- und Serverdienst ausgeführt.

Da mit Hilfe der TCP/IP-Filterung nur der eingehende TCP/IP-Zugriff gesteuert werden kann, sollten Sie dieses Verfahren mit IPSec-Filterung sowie RAS-Paketfilterung für den ausgehenden Zugriff kombinieren.

Die Microsoft-Empfehlung lautet, bei der Verwendung des SBS 2003 mit zwei Netzwerkkarten die Firewall-Funktion zu aktivieren und auf der externen Netzwerkkarte die entsprechenden Ports zu öffnen.

Zur Konfiguration der TCP/IP-Filterung führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Systemsteuerung und wählen aus dem Kontextmenü von NETZWERKVERBINDUNGEN den Eintrag ÖFFNEN.
2. Markieren Sie die Netzwerkverbindung, die für die Steuerung des eingehenden Zugriffs konfiguriert werden soll, und klicken in deren Kontextmenü auf EIGENSCHAFTEN.
3. Auf der Registerkarte ALLGEMEIN klicken Sie unter VERBINDUNGSEIGENSCHAFTEN VON [NAME DES ADAPTERS] auf INTERNETPROTOKOLL (TCP/IP) und EIGENSCHAFTEN.
4. Im Fenster EIGENSCHAFTEN VON INTERNETPROTOKOLL (TCP/IP) klicken Sie auf ERWEITERT und dann auf die Registerkarte OPTIONEN.
5. Klicken Sie auf TCP/IP-FILTER und EIGENSCHAFTEN.
6. Markieren Sie hier die Checkbox TCP/IP-FILTER AKTIVIEREN (ALLE ADAPTER). Hiermit ist zwar die TCP/IP-Filterung für alle Adapter aktiviert, die Filterkonfiguration muss jedoch für jeden Adapter separat durchgeführt werden. Zur Konfiguration können Sie entweder die Option ALLE ZULASSEN wählen oder nur für bestimmte IP-Protokolle, TCP- und UDP-Ports eingehende Verbindungen gestatten.

Beispiel: Wird für die externe Netzwerkkarte nur der Port 80 für eingehenden Verkehr zugelassen, so wird von ihm nur der Internetverkehr zugelassen. Ist für die interne Netzwerkkarte die Option ALLE ZULASSEN gewählt, so ist auf dieser Karte eine uneingeschränkte Kommunikation möglich.

7. Für die TCP/IP-Filterung können Sie die folgenden drei Spalten konfigurieren: TCP-PORTS, UDP-PORTS und IP-PROTOKOLLE. Für jede dieser drei Spalten können Sie die Option ALLE ZULASSEN oder NUR ZULASSEN auswählen. Im zweiten Fall können Sie den TCP- und UDP-Verkehr beschränken. Klicken Sie dazu auf HINZUFÜGEN und tragen im Fenster FILTER HINZUFÜGEN die Portnummer oder die Protokollnummer ein. Haben Sie lediglich die Option NUR ZULASSEN aktiviert, jedoch keine Eintragungen in die Liste vorgenommen, ist keine Kommunikation der Netzwerkkarte möglich. Dies gilt gleichermaßen für interne wie für externe Verbindungen.

Folgende Blockierungen sind jedoch nicht möglich:

TCP- und UDP-Verkehr können nicht blockiert werden, indem Sie für die Spalte IP-Protokolle die Option NUR ZULASSEN wählen und dann die Protokollnummern 6 (TCP, Transfer Control Protocol) und 17 (UDP, User Datagramm Protocol) eintragen.

ICMP-Meldungen (Internet Control Message) können generell nicht blockiert werden, auch nicht, indem Sie für die Spalte IP-Protokolle die Option NUR ZULASSEN wählen und dann die Protokollnummer 1 eintragen.

Die hier eingestellten Filteroptionen beziehen sich nur auf den eingehenden Verkehr. Um den ausgehenden Verkehr ebenfalls zu kontrollieren, verwenden Sie am besten IPSec-Richtlinien oder RAS-Paketfilterung.

12.4 Software-Updates für die Betriebssysteme

Ein weiterer Schritt zur Sicherung des Netzwerks ist die rechtzeitige Aktualisierung der Betriebssystem-Software durch die von Microsoft bereitgestellten Service Packs, Updates und Patches, um bekannte Sicherheitslücken zu schließen. Dieses gilt gleichermaßen für den SBS 2003 selbst als auch für die einzelnen Clientcomputer.

Der beste Weg hierzu ist der Einsatz der Software Update Services (siehe Kapitel 9). Alternativ dazu können Sie auch das automatische Windows-Update verwenden, das ebenfalls in Kapitel 9 beschrieben wird. Weiterhin sollten Sie auch darauf achten, dass Sie auch Applikationen wie Microsoft Office oder auch andere Applikationen anderer Hersteller regelmäßig auf Updates hin prüfen und sich für diese eine Verteilstrategie überlegen. Für Microsoft Office-Produkte wird die automatische Verteilung der Updates in die Version 2.0 der Software Update Services implementiert. Für ein automatisches Update verwenden Sie den Link *http://office.microsoft.com/OfficeUpdate/default.aspx*. Für das Update werden ausschließlich die Office-Versionen 2000, XP und 2003 unterstützt. Um nach Updates für weitere Applikationen zu suchen, schauen Sie auf den entsprechenden Websites nach oder lassen sich automatisch über neue Updates informieren, sofern der Hersteller dieses anbietet.

12.4.1 Updates der Betriebssysteme und Applikationen

Auch bei Clients, die noch unter Windows 9x oder NT 4.0 oder früher betrieben werden, sollten Sie über ein Update auf Windows 2000 oder XP Professional nachdenken. Diese Betriebssysteme garantieren eine bessere Leistung und Sicherheit im SBS 2003-Netzwerk. Zudem erfordert beispielsweise das im SBS 2003 enthaltene Outlook 2003 Windows 2000 Professional mit mindestens Service Pack 3 oder Windows XP und ist unter früheren Windows-Versionen nicht lauffähig.

12.5 Implementieren sicherer Kennwörter

Das Implementieren sicherer Kennwörter, welche die Windows-Komplexitätsanforderungen erfüllen, ist ein weiterer Schritt zur Sicherung des Netzwerks. Neben der Implementierung der entsprechenden Richtlinien ist hier auch die Schulung der Benutzer im Umgang mit dem Kennwort erforderlich. Es soll ja immer noch genügend Benutzer geben (selbst Administratoren), die ihr Kennwort auf einem Zettel unter der Tastatur oder an den Monitor geklebt aufbewahren. Insbesondere der Nutzen des regelmäßigen Änderns des Kennworts sowie der Anforderungen sollten den Benutzern eingehend nahe gebracht werden. Erklären Sie den Benutzern, dass sie ihr Kennwort genauso geheim halten sollten wie beispielsweise die PIN ihrer Kreditkarte.

Für die Wahl des Passworts sollten die Benutzer keine Begriffe wählen, die ein potenzieller Angreifer entweder durch persönliche Kenntnis des Benutzers oder durch andere Suchmethoden herausfinden könnte. Dazu zählen die folgenden Begriffe:

- Der Name von Kindern, Ehegatte, Haustier oder Freunden
- Ein beliebiges Wort, das sich in einem Wörterbuch finden lässt

- Ein Geburtsdatum, eine Telefonnummer oder weitere persönliche Nummern wie Kfz-Kennzeichen oder Kontonummer
- Ebenso wenig sollte ein Kennwort wieder benutzt werden, das bereits früher benutzt worden ist.

Sie erhalten den Hinweis für die Implementierung sicherer Kennwörter, nachdem Sie den Assistenten für die Herstellung der Internetverbindung abgeschlossen haben. Die Implementierung der Anforderungen wurde bereits ausführlich in Kapitel 2.7.2 Schritt 14 beschrieben.

12.6 Remote-Zugriff auf das Netzwerk

Für den Remote-Zugriff können Sie entweder den Remote Webarbeitsplatz oder eine VPN-Verbindung konfigurieren. Die einfachere Lösung ist die Implementierung des Remote-Webarbeitsplatzes, so dass sich nur autorisierte Benutzer mit dem Netzwerk verbinden können. In beiden Fällen sollten Sie den Benutzern beibringen, dass sie sich grundsätzlich sofort abmelden sollen, wenn sie die Verbindung nicht mehr benötigen.

Über den Remote-Webarbeitsplatz können die Benutzer von außerhalb des lokalen Netzwerks eine Verbindung zu ihrem Computer am Arbeitsplatz herstellen, E-Mails empfangen, auf die interne Website zugreifen und Applikationen verwenden. Über den Connection Manager können sich die Benutzer auch mit dem SBS 2003-Netzwerk verbinden.

Um sich mit einem Computer im lokalen Netzwerk über den Remote-Webarbeitsplatz zu verbinden, muss dieser Windows XP Professional oder Windows Server 2000 ausführen. Ist auf dem Remote-Computer ein anderes Betriebssystem installiert, müssen Sie für den Zugriff eine VPN-Verbindung oder Wahlverbindung konfigurieren.

Wird der Remote-Webarbeitsplatz nicht benötigt, sollten Sie dieses Feature deaktivieren.

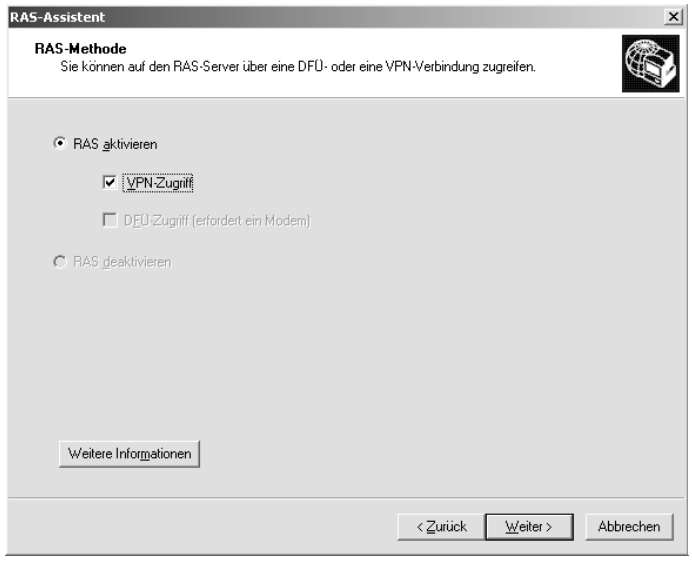


Abbildung 12.6: Auswahl der RAS-Zugriffsmethode

Möchten oder können Sie den Remote-Webarbeitsplatz nicht einrichten, so verwenden Sie wiederum den Assistenten für die Herstellung der Internetverbindung. Mit Hilfe des Assistenten können Sie eine VPN-Verbindung und/oder eine DFÜ-Verbindung einrichten (siehe Abbildung). Bei einer VPN-Verbindung stellt der Remote-Benutzer zunächst eine Verbindung zum Internet her und verbindet sich dann über einen Tunnel mit dem Firmennetzwerk. Bei einer DFÜ-Verbindung wird die Verbindung über die Telefonleitung mit einem Modem auf dem SBS 2003 hergestellt.

Ist die Option RAS AKTIVIEREN nicht verfügbar, so ist der RAS-Dienst auf dem SBS 2003 nicht aktiviert. Werden diese Verbindungstypen nicht benötigt, sollten Sie diese auch nicht einrichten.

12.7 Einschränken der Benutzerrechte

Indem den Benutzern zu hohe Berechtigungen zugewiesen werden, besteht eine Gefahr in zweierlei Weise. So können einerseits die Benutzer selbst ohne böse Absicht oder besseres Wissen schnell Schaden anrichten. Zudem besteht auch die Gefahr, dass im Falle des unberechtigten Zugriffs auf das Konto der Angreifer bereits über umfassende Berechtigungen verfügt.

Beim Erstellen der Benutzerkonten sollten Sie darauf achten, den Benutzern die korrekten Benutzervorlagen zuzuweisen. Weiterhin sollten die Benutzerkonten der Vorlagen Administrator und Power User nicht für die tägliche Arbeit benutzt werden. So ist es über die Benutzervorlagen einem normalen Benutzer nicht möglich, remote auf das Netzwerk zuzugreifen. Um diese Berechtigung bereitzustellen, verwenden Sie für die entsprechenden Benutzer die Vorlage Mobile Users. Auch für Netzwerkfreigaben sollten Sie immer nur die wirklich notwendigen Benutzerrechte und Dateirechte vergeben.

12.7.1 Sicherheitsaspekte für Administratoren

Aus Sicherheitsaspekten sollte der Administrator nur dann unter dem Benutzerkonto Administrator oder unter einem anderen Konto mit Administratorrechten angemeldet sein, wenn er Aufgaben erledigen muss, für die er die entsprechenden Rechte unbedingt benötigt. Ansonsten sollte der Administrator sich mit einem Benutzerkonto mit weniger privilegierten Rechten anmelden. Ist der Administrator mit vollen Admin-Rechten angemeldet und holt sich während eines Internet-Besuches einen Virus oder Trojaner, so werden alle Tätigkeiten des Virus ermöglicht, die dem aktuellen Benutzerkonto möglich sind. Bei Administratorrechten können so Daten gelöscht oder Festplatten formatiert werden. Melden Sie sich deshalb über ein Konto an, dem nur minimale Rechte zugewiesen sind.

Sollte es dabei jedoch vorkommen, dass unvorhergesehen das Ausführen einer bestimmten Aufgabe die Administratorrechte verlangt, so kann diese Aktion dennoch unter dem gerade aktuellen Benutzerkonto ausgeführt werden, ohne dass eine Abmeldung und Neuanmeldung als Administrator am Computer erfolgen muss. Hierzu gibt es die Optionen *Ausführen als* in der grafischen Oberfläche sowie die Kommandozeilenoption *RUNAS*.

12.7.2 Die Option Ausführen als

Sie können jede ausführbare Datei, jede mmc und jedes Element der Systemsteuerung mit der Option *Ausführen als* starten. Dazu müssen Sie lediglich über einen Benutzernamen und ein Passwort verfügen, womit das gewünschte Programm ausgeführt werden darf. Es kann jedoch möglich sein, dass diese Option fehlschlägt, wenn Sie über das Netzwerk ein Programm auf einem anderen Computer ausführen möchten. Dies ist der Fall, wenn das Benutzerkonto, das Sie bei *Ausführen als* angeben, nicht mit dem Konto identisch ist, von dem das Programm ursprünglich gestartet wurde, selbst wenn die Rechte des Ausführen-Kontos ausreichend sind.

Um diese Option zu benutzen, führen Sie die folgenden Schritte aus:

1. Stellen Sie fest, ob unter DIENSTE die Option DIENST AUSFÜHREN ALS aktiviert ist. Falls dies nicht der Fall ist, starten Sie den Dienst manuell.
2. Markieren Sie die Programmdatei, Verknüpfung, mmc oder das Systemsteuerungselement, das Sie ausführen möchten. Halten Sie die Umschalt-Taste (⇧) gedrückt und wählen dann aus dem Kontextmenü AUSFÜHREN ALS.
3. Geben Sie nun an, unter welchem Konto Sie das Programm ausführen möchten. Dazu sind Angaben über Benutzername, Kennwort und Domäne notwendig (siehe Abbildung 12.7).

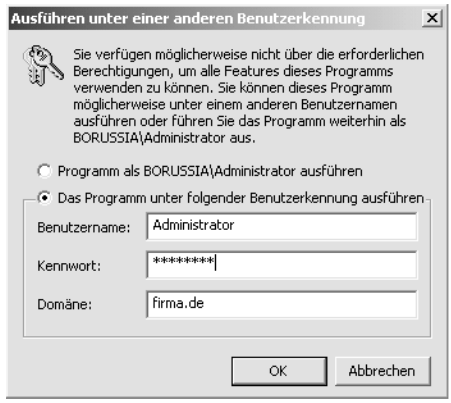


Abbildung 12.7: Die Option AUSFÜHREN ALS

12.7.3 Verwenden von RUNAS

Das Programm RUNAS wird von der Kommandozeile aus gestartet. Es erfüllt denselben Zweck wie das eben beschriebene *Ausführen als.* Prüfen Sie auch hier zuvor, ob unter DIENSTE der Dienst DIENST AUSFÜHREN ALS gestartet ist. RUNAS bietet die folgenden Optionen:

```
runas [/profile] [/env] [/netonly] /user:Kontoname Programmpfad
```

Die optionalen Parameter haben folgende Bedeutung:

`/profile`: Profilpfad des Benutzerkontos, nur nötig, wenn ein Profil geladen werden muss.

`/env`: wenn die Netzwerkumgebung statt der lokalen Umgebung verwendet werden soll.

`/netonly`: wenn die Benutzerinformationen nur für den Remote-Zugriff gültig sind.

`/user`: im Format Computername\Konto bzw. unter 2000 Konto@Computername.

Programmpfad: Pfad zur ausführbaren Datei. Befinden sich Leerzeichen im Programmpfad, müssen die Angaben in Anführungszeichen gesetzt werden.

Eine RUNAS-Befehlszeile könnte folgendermaßen aussehen:

```
runas /user: Administrator@hippokrates.firma.de "mmc %windir%\system32\
Konsole1.msc" ↵
```

Das Passwort für das Konto können Sie nach der Aufforderung eingeben.

Weiterhin sollten für die Benutzung des Administratorkontos folgende, eigentlich selbstverständliche Regeln gelten:

- Benutzen Sie auf jeden Fall ein sicheres Kennwort für das Konto.
- Geben Sie das Kennwort niemals weiter, und notieren Sie dieses nicht in der Nähe des Computers.
- Melden Sie sich für tägliche Aufgaben nicht mit dem Administratorkonto an.
- Lassen Sie den Computer nicht unbeaufsichtigt, wenn Sie unter dem Administratorkonto angemeldet sind. Sperren Sie den Computer, wenn Sie ihn auch nur kurzzeitig verlassen.

12.7.4 Sichern der Netzwerkfreigaben

Bei sämtlichen Netzwerkfreigaben, die bei der Installation des SBS 2003 eingerichtet werden, sind die Berechtigungen automatisch sehr restriktiv gesetzt, um die Unternehmensdaten vor unberechtigtem Zugriff zu schützen. Diesem Prinzip sollten Sie auch bei allen weiteren Freigaben treu bleiben.

Um zu ermitteln, welche Freigaben auf dem Server vorhanden sind, geben Sie an der Eingabeaufforderung den Befehl \\Servername ein. Die folgenden Freigaben werden beim Setup des Servers automatisch erstellt:

- Servername.log
- Address
- ClientApps
- Clients
- Drucker und Faxgeräte
- Faxclient
- Netlogon
- Sysvol

- Tsclient
- Tsweb
- Users

Bei allen anderen möglicherweise aufgelisteten Freigaben handelt es sich um selbst erstellte Freigaben, deren Berechtigungen Sie überprüfen sollten. Öffnen Sie dazu über die EIGENSCHAFTEN die Registerkarte SICHERHEIT und prüfen die Berechtigungen, die den Benutzern und Gruppen für die Freigabe zugewiesen worden sind, und schränken diese notfalls ein.

12.7.5 Ändern des Administratorkontonamens

Ein weiterer Schritt zur Absicherung des Administratorkontos ist das Umbenennen des vordefinierten Kontos Administrator. Da das Administratorkonto nicht gesperrt werden kann, während mit denselben Berechtigungen ein anderes Konto benutzt wird, kommt nur ein Umbenennen des Kontos in Frage. So hat ein potenzieller Angreifer keine Chance, wenn er sich mit dem Konto Administrator anmeldet und versucht, das Kennwort zu erraten, da es ein Konto diesen Namens nicht mehr gibt.

Nachdem Sie das Administratorkonto umbenannt haben, müssen Sie sich unbedingt neu am SBS 2003 anmelden, da Ihnen ansonsten der Zugriff auf Verwaltungswerkzeuge oder weitere Ressourcen verweigert wird, solange Sie noch unter dem alten Administratorkonto angemeldet sind.

1. Um den Kontonamen zu ändern, öffnen Sie in der Serververwaltung den Eintrag BENUTZER. Wählen Sie aus dem Kontextmenü die EIGENSCHAFTEN und öffnen die Registerkarte ALLGEMEIN. Im Textfeld ANZEIGENAME tragen Sie den neuen Namen für das Konto ein.
2. Wechseln Sie dann auf die Registerkarte KONTO und tragen unter BENUTZERANMELDENAME denselben neuen Kontonamen ein. Dieser Name muss auch unter BENUTZERANMELDENAME (PRÄ-WINDOWS 2000) eingetragen werden. Klicken Sie dann auf OK.

Weiterhin können Sie auch auf den Clients das lokale Administratorkonto umbenennen.

1. Unter Windows 2000 und XP öffnen Sie SYSTEMSTEUERUNG/VERWALTUNG/COMPUTERVERWALTUNG.
2. Öffnen Sie in der Konsole LOKALE BENUTZER UND GRUPPEN und darunter BENUTZER. Wählen Sie aus dem Kontextmenü von Administrator den Eintrag UMBENENNEN und ändern den Namen.

Um auf sämtlichen Clientcomputern den Namen des Administratorkontos zu ändern, verwenden Sie die GPMC (Group Policy Management Console).

12.8 Absicherung des SBS 2003

Eine Absicherung des SBS 2003 muss auf zweierlei Ebenen erfolgen. Zunächst einmal muss der Server selbst physikalisch abgesichert werden. Dazu muss der Server auch hinsichtlich der Software sicher gestaltet werden.

12.8.1 Physikalische Absicherung des Servers

Zur physikalischen Absicherung zählt, dass sich der Server in einem abgeschlossenen Raum befindet, so dass kein Zugriff auf den Server erfolgen kann. Die Schlüssel für diesen Raum sollte nur der Personenkreis der Administratoren erhalten. Ansonsten besteht die Gefahr, die Festplatte des Servers zu entfernen und auszulesen, den Computer mit einer Diskette zu starten und die Festplatte zu formatieren oder auch die Tastatur durch eine speziell präparierte Tastatur auszutauschen, die sämtliche Eingaben inklusive des Passworts aufzeichnen kann. Achten Sie also darauf, das Gehäuse des Servers immer verschlossen zu halten und den Schlüssel an einem sicheren Ort zu deponieren. Zusätzlich sollten Sie das BIOS des Servers mit einem Passwort schützen.

Weiterhin sollten Sie die Backup-Bänder des SBS grundsätzlich an einem anderen Ort als dem Standort des Servers aufbewahren. Auch der Einsatz einer USV (Unterbrechungsfreie Stromversorgung) kann den Server vor Schäden bei einem Stromausfall schützen.

12.8.2 Softwareinstallation auf dem Server

Als Grundregel sollte für einen Server immer gelten, dass Sie auf diesem nicht mehr Applikationen als notwendig installieren. Keinesfalls darf der SBS bezüglich der Softwareinstallation wie ein Clientcomputer behandelt werden. Somit schließen Sie aus, dass ein Angreifer über mögliche Sicherheitslücken in den installierten Applikationen Zugriff auf den Server erhält.

Auf jeden Fall sollten Sie auf dem Server ein Backup-Programm ausführen, sofern Sie nicht das integrierte Windows Backup benutzen. Weiterhin sollte es selbstverständlich sein, dass auf dem Server auch ein Antivirenprogramm installiert ist. Dabei müssen Sie entscheiden, ob Sie sich für eine serverbasierte Lösung entscheiden, die sämtliche Clients im Netzwerk ebenfalls vor Viren schützt, oder ob Sie für jeden Client einzeln eine Antivirensoftware einsetzen möchten.

12.9 Überwachen des SBS 2003

Auf dem SBS 2003 sollten Sie die Überwachung sicherheitsbezogener Vorgänge aktivieren. Sie können die Inhalte der Überwachungsreporte sowohl über die Serververwaltungskonsole lesen als auch per E-Mail an einer beliebigen Adresse empfangen.

Wenn Sie die Berichte als E-Mail-Anhang empfangen, finden Sie dort eine chronologische Übersicht über System-, Anwendungs- und Sicherheitsereignisse sowie den IIS. Bedenken Sie jedoch, dass die Reporte als E-Mail-Anhang relativ groß werden können. Übersteigt die Größe eines Reports die Grenze von 5 MB, so wird der Report nicht als Anhang versendet. Bedenken Sie auch, ob eine eventuelle Größenbeschränkung des Postfachs bei Ihrem Mailprovider besteht.

Zusätzlich sollten Sie die Überwachung für das Fehlschlagen von Anmeldungen sowie das Sperren von Konten aktivieren. Standardmäßig ist das Auditing für diese beiden Arten von Ereignissen unter SBS 2003 aktiviert. Sofern innerhalb von zehn Minuten 50 ungültige Anmeldeversuche für ein Benutzerkonto erfolgen, wird das Konto dann auto-

matisch für zehn Minuten gesperrt. Im Ereignisprotokoll des SBS 2003 erfolgt bei jeder ungültigen Anmeldung ein Eintrag. Zusätzlich wird im Leistungsbericht des SBS 2003 vermerkt, wenn ein Konto aufgrund der ungültigen Anmeldeversuche gesperrt wurde. Haben Sie zusätzlich die Option aktiviert, eine E-Mail zu erhalten, wird diese bei jeder Sperrung eines Kontos an die hinterlegte Adresse versendet.

13 Troubleshooting beim Small Business Server 2003

In diesem Kapitel werden verschiedene Fehlerszenarien und Probleme des SBS 2003 vorgestellt und umfassende Lösungsvorschläge gegeben. Zur besseren Übersicht sind die einzelnen Probleme zu den thematischen Gruppen Server, Benutzer, Internet, Intranet, E-Mail und Fax, Überwachung sowie mobile Geräte zusammengefasst.

13.1 Probleme mit dem Server

Dieses Kapitel beschreibt die Probleme, die der Administrator direkt am Small Business Server 2003 ermittelt und die direkt an diesem behoben werden.

13.1.1 Plötzliches Beenden von Diensten beim Herunterfahren und Neustart des SBS 2003

Problem: Beim Herunterfahren oder Neustarten des SBS 2003 kann es zu einem plötzlichen Abbruch der ausgeführten Dienste kommen, bevor diese ordnungsgemäß vom System beendet worden sind. Dabei kann es zu Datenverlusten kommen.

Ursache: Dieses Problem liegt in einem Fehler der Registry. Darin ist für den Wert *WaitToKillServiceTimeout* der falsche Typ REG_DWORD anstelle des korrekten Typs REG_SZ gesetzt. Somit wird der für *WaitToKillServiceTimeout* gesetzte Wert grundsätzlich als Zeitlimit von null Millisekunden interpretiert, und sämtliche laufenden Dienste werden sofort beendet.

Lösung: Um das Problem zu lösen, öffnen Sie unter AUSFÜHREN mit dem Befehl *regedit* den Registry-Editor.

1. Navigieren Sie in diesem zum Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.
2. Wählen Sie aus dem Kontextmenü des Eintrags *WaitToKillServiceTimeout* den Eintrag LÖSCHEN und bestätigen dieses.
3. Wählen Sie dann aus dem Kontextmenü von CONTROL den Eintrag NEU und ZEICHENFOLGE. Erstellen Sie den folgenden neuen Wert: Name: WaitToKillServiceTimeout, Werttyp: REG_SZ, Wert: 120000. Damit ist eine Wartezeit für das Beenden der Dienste von 120000 Millisekunden gesetzt.
4. Beenden Sie dann den Registry-Editor und starten den SBS 2003 neu.

13.1.2 Probleme mit dem Dienst Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)

Problem: Nachdem Sie einen Windows Server 2000 auf SBS 2003 upgedatet haben, können Sie feststellen, dass der Dienst Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS) unerwartet startet und wieder endet.

Ursache: Dieses Phänomen tritt auf, wenn die Internetverbindungsfreigabe auf dem Windows Server 2000 aktiviert war. Deshalb startet dieser Dienst auch nach dem Update auf SBS 2003, obwohl die Internetverbindungsfreigabe nicht im SBS 2003 vorhanden ist.

Lösung: Dieses Problem können Sie lösen, indem Sie den Dienst deaktivieren. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie START/PROGRAMME/VERWALTUNG/DIENSTE.
2. Wählen Sie aus dem Kontextmenü des Dienstes INTERNETVERBINDUNGS-FIREWALL/INTERNETVERBINDUNGSFREIGABE den Eintrag EIGENSCHAFTEN.
3. Wählen Sie auf der Registerkarte ALLGEMEIN unter STARTTYP den Eintrag DEAKTIVIERT und klicken auf OK.

13.1.3 Anstelle einer Benutzer-E-Mail-Adresse wird nur die GUID angezeigt

Problem: In der Serververwaltung unter BENUTZER wird nicht der Benutzername für die E-Mail-Adresse, sondern nur dessen GUID (Globally Unique Identifier) angezeigt.

Ursache: Dieses Problem tritt auf, wenn im Benutzernamen Unicode-Zeichen enthalten sind.

Lösung: Um das Problem zu beheben, ändern Sie die SMTP-E-Mail-Adresse für das Benutzerkonto. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie in der SERVERVERWALTUNG den Eintrag ERWEITERTE VERWALTUNG und darin ACTIVE DIRECTORY-BENUTZER UND COMPUTER.
2. Doppelklicken Sie dort den Namen des SBS und öffnen den Ordner USERS oder BUILTIN, je nachdem, wo der Benutzer gespeichert ist.
3. Aus dem Kontextmenü des Benutzers wählen Sie EIGENSCHAFTEN und wechseln auf die Registerkarte E-MAIL-ADRESSEN.
4. Unter TYP wählen Sie den Eintrag SMTP und klicken auf BEARBEITEN. Ersetzen Sie dann die angezeigte GUID durch die korrekte E-Mail-Adresse des Benutzers und klicken auf OK.
5. Wechseln Sie dann auf die Registerkarte EXCHANGE – ALLGEMEIN. Im Textfeld ALIAS ersetzen Sie die GUID durch das korrekte E-Mail-Alias. Klicken Sie dann auf OK.

13.2 Probleme der Benutzer

Im Folgenden finden Sie eine Reihe typischer Probleme und Fehlerszenarien, die auf Seiten des Benutzers auftreten können.

13.2.1 Ein Benutzer kann sein Kennwort nicht ändern

Problem: Wenn der Benutzer versucht, sein Kennwort zu ändern, erhält er die Fehlermeldung, dass dieses nicht geändert werden kann.

Ursache: Ein Kennwort kann nicht geändert werden, wenn das neue Kennwort des Benutzers nicht den Kennwortrichtlinien entspricht, die der Administrator festgelegt hat.

Lösung: Teilen Sie dem Benutzer mit, welche Anforderungen bezüglich Länge und Komplexität erforderlich sind.

13.2.2 Das Konto eines Benutzers ist gesperrt

Problem: Ein Benutzer kann sich nicht mehr anmelden, da sein Konto gesperrt ist.

Ursache: Ein Benutzerkonto wird aus Sicherheitsgründen automatisch gesperrt, wenn zu viele seiner Anmeldeversuche fehlgeschlagen sind.

Lösung: Um sein Konto wieder zu entsperren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der SERVERVERWALTUNG den Eintrag BENUTZER und wählen den Eintrag EIGENSCHAFTEN aus dem Kontextmenü des betroffenen Benutzers.
2. Öffnen Sie die Registerkarte KONTO und deaktivieren dort die Checkbox KONTO IST GESPERRT. Der Benutzer kann sich jetzt wieder anmelden.

Über die Kontosperrungsrichtlinien wird festgelegt, dass standardmäßig eine Kontosperrung nach 50 fehlgeschlagenen Versuchen eintritt. Die Sperrdauer beträgt zehn Minuten.

13.2.3 Ein neuer Benutzer kann sich nicht anmelden

Problem: Ein neu erstellter Benutzer versucht sich unmittelbar nach der Erstellung des Kontos an der Domäne anzumelden. Dieses schlägt jedoch fehl.

Ursache: Sobald ein Benutzerkonto erstellt wurde, wird dieses nicht sofort vom Active Directory erkannt und kann deshalb noch nicht verwendet werden. Standardmäßig dauert es 15 Minuten, bis das Konto erkannt ist.

Lösung: Teilen Sie dem Benutzer mit, ca. 15 Minuten zu warten (und in der Zwischenzeit vielleicht eine Tasse Kaffee zu trinken).

13.2.4 Die erstmalige Anmeldung an einem Client dauert sehr lange

Problem: Sobald sich der Benutzer das erste Mal am Client anmeldet, sobald dieser zur SBS-Domäne hinzugefügt wurde, dauert die Anmeldung sehr lange.

Ursache: Die Umleitung des Ordners Eigene Dateien auf den Server wurde aktiviert. Bei der ersten Anmeldung muss der Inhalt des lokalen Ordners mit dem Server synchronisiert werden. Je größer der Inhalt des Ordners ist, desto länger dauert der Synchronisationsvorgang und somit auch die Anmeldung. Ab der zweiten Anmeldung werden nur die Änderungen des Ordners synchronisiert, so dass die Anmeldung schneller erfolgt.

Lösung: Da es sich um keinen Fehler handelt, ist auch keine Lösung vorgesehen.

13.2.5 Ein Benutzer kann keine Daten in den freigegebenen Ordnern des Servers speichern

Problem: Ein Benutzer kann keine Daten mehr auf den freigegebenen Ordnern des Servers speichern.

Ursache: Er hat das Limit des für die Benutzer zugewiesenen Datenträgerkontingents zum Speichern von Daten überschritten.

Lösung: Sie können ihn zunächst auffordern, die Daten auf seinem lokalen Computer zu speichern. Tritt das Problem aber bei mehreren Benutzern auf, sollten Sie darüber nachdenken, die Größe des Datenträgerkontingents zu ändern. Bedenken Sie jedoch, dass Sie das Kontingent nicht für jeden Benutzer individuell, sondern nur für eine gesamte Festplattenpartition ändern können.

13.2.6 Benutzer können keine vorhergehende Dateiversion wiederherstellen

Problem: Die Benutzer können keine vorhergehende Version ihrer Dateien wiederherstellen, da die Registerkarte VORHERIGE VERSIONEN unter den Eigenschaften des Ordners Eigene Dateien fehlt.

Ursache: Der Ordner Eigene Dateien wurde erst vor kurzem an einen neuen Speicherort umgeleitet, so dass der durchzuführende Snapshot noch nicht erstellt wurde. Die Speicherplatzzuweisung für gelöschte Dateien muss auch weiterhin aktiv sein.

Lösung: Die Registerkarte ist verfügbar, sobald der nächste Snapshot erstellt ist. Dies geschieht um 7:00 h sowie 12:00 h. Weitere Maßnahmen sind nicht erforderlich.

13.2.7 Der Ordner Eigene Dateien wird nicht mit dem Server synchronisiert

Problem: Es erfolgt keine Synchronisation der Inhalte des Ordners Eigene Dateien mit denen auf dem Server.

Ursache: Die Größe des Datenträgerkontingents wurde überschritten, so dass keine weiteren Dateien des Benutzers auf dem Server gespeichert werden können.

Lösung: Sie können entweder dem Benutzer mitteilen, dass er nicht mehr benötigte Daten aus dem Ordner Eigene Dateien löschen möge, oder alternativ das Datenträgerkontingent erhöhen. Bedenken Sie jedoch, dass sich das Erhöhen des Kontingents auf sämtliche Benutzer bezieht.

13.2.8 Nach der Migration von Benutzerprofilen ist kein Zugriff auf umgeleitete Ordner mehr möglich

Problem: Nachdem Sie die Benutzerprofile auf den SBS 2003 migriert haben, können die Benutzer nicht mehr auf die umgeleiteten Ordner zugreifen.

Ursache: Bei privaten Benutzerprofilen werden die administrativen Credentials von den Benutzerordnern auf den Clientcomputern entfernt. Die Benutzer benötigen jedoch diese Credentials, um auf die Ordner zuzugreifen, die an den Server umgeleitet worden sind. Nach der Migration der Benutzerprofile, zu denen auch die umgeleiteten Ordner gehören, können die Benutzer möglicherweise nicht mehr auf die Daten auf dem Server zugreifen.

Lösung: Um das Problem zu beheben, müssen Sie auf dem Clientcomputer manuell den Zugriff für die Benutzerordner wiederherstellen. Führen Sie dazu die folgenden Schritte durch:

1. Auf dem Clientcomputer öffnen Sie STARTMENÜ/PROGRAMME/VERWALTUNG/EREIGNISANZEIGE. Öffnen Sie dort den Eintrag ANWENDUNG.
2. Suchen Sie in der Liste nach einer Fehlermeldung, die als Quelle ORDNERUMLEITUNG angibt, und doppelklicken diesen Eintrag.
3. Notieren Sie sich das Ziel- und Quellverzeichnis, das in der Ereignisbeschreibung angegeben ist.
4. Die nächsten Schritte werden auf dem Server durchgeführt. Navigieren Sie dort über den Windows Explorer zu dem in Schritt 3 notierten Benutzerordner.
5. Wählen Sie aus dem Kontextmenü des Ordners den Eintrag FREIGABE UND SICHERHEIT und wählen die Registerkarte BERECHTIGUNGEN. Prüfen Sie, dass der Name des Benutzers dort nicht in der Liste Berechtigungseinträge vorhanden ist. Ist der Ordner leer, so löschen Sie ihn.
6. Ab hier werden die Schritte wieder auf dem Client ausgeführt. Navigieren Sie dort über den Windows Explorer zu dem in Schritt 3 notierten Benutzerordner. Wählen Sie aus dem Kontextmenü des Ordners den Eintrag FREIGABE UND SICHERHEIT und klicken auf der Registerkarte SICHERHEIT auf ERWEITERT.
7. Im Fenster ERWEITERTE SICHERHEITSEINSTELLUNGEN wählen Sie die Registerkarte BENUTZER. Klicken Sie dort auf den Benutzernamen und aktivieren die Checkbox BESITZER DER OBJEKTE UND UNTERGEORDNETEN CONTAINER ERSETZEN. Klicken Sie auf ÜBERNEHMEN.
8. Auf der Registerkarte BERECHTIGUNGEN sollte der Name des Benutzers in der Liste BERECHTIGUNGSEINTRÄGE vorhanden sein. Ist dies nicht der Fall, müssen Sie über HINZUFÜGEN den Benutzer in die Liste aufnehmen. Weisen Sie diesem die Berechtigung VOLLZUGRIFF für diesen Ordner zu. Klicken Sie dann auf OK.
9. Melden Sie sich anschließend vom Clientcomputer ab und danach wieder neu an.

13.2.9 Nach dem Upgrade auf SBS 2003 stehen nicht mehr alle Applikationen zur Verfügung

Problem: Auf den Clients sind nach dem Upgrade lediglich die unter SBS 2003 verfügbaren Applikationen vorhanden, nicht jedoch die bereits vorher installierten.

Ursache: Es werden nur die standardmäßigen Applikationen auf den Clientcomputern installiert. Andere Applikationen werden nicht aktualisiert.

Lösung: Installieren Sie die Applikationen auf dem SBS 2003. Sie werden auf dem Clientcomputer installiert, nachdem das Upgrade abgeschlossen ist. Die Kommandozeilen für die Installation der Applikationen auf den Clients finden Sie in der Registry des SBS 2003 unter dem Schlüssel:

```
HKEY_LOCAL_MACINE\SOFTWARE\Microsoft\SmallBusinessServer\clientsetup\sbs2k_
archive\Client Applications\
```

Öffnen Sie dann in der Serververwaltung CLIENTCOMPUTER und CLIENTCOMPUTERN ANWENDUNGEN HINZUFÜGEN. Geben Sie dort die jeweiligen Kommandozeilen für die Installation der Applikationen an.

13.2.10 Es kann keine Remote-Verbindung hergestellt werden

Problem: Ein Benutzer kann keine Remote-Verbindung zu einem Computer unter Windows XP herstellen.

Ursache 1: Das Benutzerkonto verfügt nicht über die Berechtigung, um sich per Remote-Desktop anzumelden.

Lösung 1: Um dem Benutzer diese Berechtigung zu gewähren, öffnen Sie in der Serververwaltung den Eintrag BENUTZER. Aus dem Kontextmenü des betreffenden Benutzers wählen Sie den Eintrag EIGENSCHAFTEN. Auf der Eigenschaftsseite wechseln Sie auf die Registerkarte TERMINALDIENSTPROFILE und aktivieren dort die Checkbox TERMINALSERVERANMELDUNG ZULASSEN.

Ursache 2: Der Clientcomputer ist nicht für die Verwendung des Remote-Desktops eingerichtet.

Lösung 2: Um den Clientcomputer zu konfigurieren, führen Sie die folgenden Schritte durch:

1. Öffnen Sie SYSTEMSTEUERUNG/SYSTEM und dort die Registerkarte REMOTE.
2. Aktivieren Sie dort die Checkbox BENUTZERN ERLAUBEN, EINE REMOTE-DESKTOP-VERBINDUNG HERZUSTELLEN und klicken auf OK.

Ursache 3: Der Clientcomputer ist so konfiguriert, dass der Remote-Zugriff durch den Benutzer nicht zugelassen wird.

Lösung 3: Um den Clientcomputer für das Zulassen von Remote-Zugriffen zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie SYSTEMSTEUERUNG/SYSTEM und dort die Registerkarte REMOTE.
2. Klicken Sie auf REMOTE-BENUTZER AUSWÄHLEN. In dem dann erscheinenden Fenster REMOTE-DESKTOP-BENUTZER klicken Sie auf HINZUFÜGEN.

3. Im Fenster BENUTZER ODER GRUPPEN WÄHLEN wählen Sie unter OBJEKTTYPEN den gewünschten Objekttyp, z.B. Benutzer. Unter PFADE geben Sie den Suchpfad für den gewählten Objekttyp an. Unter GEBEN SIE DIE ZU VERWENDENDEN OBJEKTNAMEN EIN geben Sie den Namen des Benutzer- oder Gruppenobjekts an und klicken dann auf NAMEN ÜBERPRÜFEN.
4. Wird der Name gefunden, bestätigen Sie mit OK. Der Name wird nun in der Liste der zugelassenen Benutzer im Fenster REMOTE-DESKTOP-BENUTZER angezeigt.

13.3 Probleme mit dem Internet

Hier finden Sie einige typische Szenarien bezüglich der Probleme mit den Internetverbindungen und internetspezifischen Einstellungen.

13.3.1 Es ist kein VPN-Zugriff möglich

Problem: Ein Benutzer kann nicht über VPN auf das SBS 2003-Netzwerk zugreifen.

Ursache: Der Benutzer verfügt über keine Berechtigungen für den Zugriff über VPN oder DFÜ auf den SBS 2003.

Lösung: Damit der Benutzer die notwendigen Berechtigungen erhält, müssen Sie den Benutzer zur Gruppe Mobile Users hinzufügen oder über den Assistenten zum Ändern der Benutzerberechtigungen auf den Benutzer die Vorlage MOBILE USER anwenden.

13.3.2 SBS 2003 Standard und USB-Geräte für das Wählen bei Bedarf

Problem: In der Standardversion ist ein USB-Gerät für die Internetverbindung für das Wählen bei Bedarf nicht nutzbar.

Ursache: Die Standardedition des SBS 2003 unterstützt keine Internetverbindungen für das Wählen bei Bedarf, die ein Netzwerkgerät benutzen, das über den USB-Bus verbunden ist, wie z.B. ein USB-Modem oder ein USB-DSL-Adapter.

Lösung: Bei der Konfiguration von E-Mail und Internetverbindung über den Assistenten müssen Sie in der Standardversion ein nicht-USB-basiertes Netzwerkgerät auswählen oder aber die Enterprise-Version des SBS 2003 verwenden, die nicht von dieser Einschränkung betroffen ist.

Für die Standardversion des SBS 2003 gibt es keine Lösung dieses Problems. Sie können in diesem Fall kein USB-Gerät verwenden.

13.4 Probleme mit dem Intranet

Hier finden Sie eine Reihe von Fehlerszenarien, die in Verbindung mit der Intranetnutzung, insbesondere bei der Verwendung der SharePoint Services auftreten können.

13.4.1 Die Installation der Intranetkomponente bzw. die Verbindung mit http://companyweb schlägt fehl

Problem: Während der Installation der Intranetkomponente erhalten Sie eine Fehlermeldung, dass ein Fehler bei der Installation der SharePoint Services und beim Erstellen der Intranetseite aufgetreten ist. Sofern Sie nach der Installation des SBS 2003 auf die Firmenwebsite zugreifen möchten, erhalten Sie den Hinweis, dass Sie nicht berechtigt sind, auf die Seite zuzugreifen.

Ursache: Diese Symptome treten nicht auf, wenn der SBS 2003 vor dem 24. November 2003 installiert worden ist, es sei denn, es wurden größere Änderungen an den SharePoint Services wie etwa das Erstellen einer neuen Top-Level-Website vorgenommen. Das eigentliche Problem liegt in der Validierung von DLLs. Einige DLLs werden von der Installationsroutine fälschlicherweise als ungültig betrachtet.

Lösung: Um dieses Problem zu beheben, hat Microsoft einen Patch für die SharePoint Services und die SQL Server 2000 MSDE bereitgestellt. Sie finden diesen beiden Patches auf der Begleit-CD sowie weitere Informationen dazu im Microsoft KB-Artikel 832880 und 833019.

Die fehlerhaften Installationsdateien der Installations-CD 3 wurden zwischenzeitlich ausgetauscht. Kunden, die noch die alte CD besitzen, können sich kostenlos die berichtigte CD zusenden lassen. Das entsprechende Bestellformular finden Sie unter *https://microsoft.order-4.com/sbsrtmcd/*.

Sind bereits vor der Installation dieses Patches Benutzer hinzugefügt worden, öffnen Sie in der Serververwaltung den Eintrag BENUTZER und starten den Assistenten zum Zuweisen von Benutzerrechten. Erteilen Sie den bereits angelegten Benutzern Zugriffsrechte für die Website.

Wurde die Website vor dem Einspielen des Patches veröffentlicht, starten Sie nach Einspielen des Patches den Assistenten für E-Mail und Internetzugang erneut, um die Website im Internet bereitzustellen.

13.4.2 Beim Zugriff auf die Firmenwebsite muss ein Benutzer seine Anmeldeinformationen eingeben

Problem: Sobald ein Benutzer versucht, auf die interne Firmenwebsite zuzugreifen, wird er aufgefordert, seine Anmeldeinformationen einzugeben.

Ursache: Da die interne Firmenwebsite auf den SharePoint Services beruht, muss der Benutzer Mitglied einer SharePoint Services-Websitegruppe sein. Ist er Mitglied dieser Gruppe, muss er keine Anmeldeinformationen eingeben.

Lösung: Wenn Sie ein Benutzerkonto auf Basis einer der Benutzervorlagen erstellen, sind die Benutzer automatisch für den Zugriff ohne weitere Anmeldeinformationen auf die Firmenwebsite konfiguriert.

13.4.3 Die Suchfunktion auf der internen Website ist nicht verfügbar

Problem: Auf der internen Firmenwebsite steht keinerlei Suchfunktion zur Verfügung.

Ursache: Die Funktionalität der Volltextsuche ist nicht verfügbar, wenn auf dem SBS 2003 die MSDE ausgeführt wird. Dafür ist eine Instanz des SQL Servers 2000 erforderlich.

Lösung: Um die Volltextsuche nutzen zu können, müssen Sie die MSDE auf eine Instanz von SQL Server 2000 aktualisieren. Mit Hilfe einer Evaluierungsversion des SBS 2003 ist kein Update der MSDE durchführbar.

13.4.4 Es können keine Dokumente der Firmenwebsite bearbeitet werden

Problem: Es ist nicht möglich, die Dokumente der internen Firmenwebsite zu bearbeiten oder zu speichern.

Ursache: Um Dokumente der Firmenwebsite bearbeiten und speichern zu können, muss auf dem Clientcomputer Microsoft Office XP oder Microsoft Office 2003 installiert sein. Mit älteren Office-Versionen können die Dokumente nicht bearbeitet werden.

Lösung: Aktualisieren Sie die entsprechenden Office-Anwendungen auf den Clients der Benutzer.

13.4.5 Die Webseite des SBS 2003 kann nicht über den FQDN erreicht werden

Problem: Sobald Sie versuchen, von einem internen Client aus auf den SBS 2003 über seinen öffentlich registrierten FQDN (Fully Qualified Domain Name/Vollqualifizierter Domänenname) zuzugreifen, erhalten Sie die Fehlermeldung: DNS-FEHLER. DIE SEITE KANN NICHT ANGEZEIGT WERDEN.

Ursache: Dieses Problem tritt auf, wenn der öffentlich registrierte FQDN zur externen Seite eines NAT-Geräts (Network Address Translation) hin aufgelöst wird, das mit dem Internet verbunden ist und dieses an den internen Server zurückgibt. In diesem Moment versucht der Internet Explorer, den öffentlich registrierten FQDN zu erreichen, die Verbindung wird jedoch blockiert, und es erscheint die Fehlermeldung. Die Anfrage wird dabei vom Router so interpretiert, als würde sie von einer IP-Adresse aus gestellt werden, die sich innerhalb des internen Netzwerks befindet. Der Router sieht die Anfrage deswegen als gefälscht an (Spoofing) und bearbeitet das Paket nicht weiter. Der Client jedoch, der sich in Wirklichkeit ja im externen Netz befindet, enthält anstatt einer Antwort lediglich die Fehlermeldung.

Lösung 1: Zur Lösung des Problems können Sie zunächst versuchen, für den Router ein aktuelles Firmware-Update einzuspielen.

Lösung 2: Ist dieses bereits vorhanden oder kann dadurch das Problem auch nicht gelöst werden, so können die Clients versuchen, den SBS zu erreichen, indem Sie innerhalb der URL den NetBIOS-Namen benutzen.

Lösung 3: Die dritte Lösung besteht darin, eine zusätzliche DNS-Forward-Lookup-Zone einzurichten. Diese Zone muss denselben Namen haben wie der externe Domänenname. Um diese DNS-Zone einzurichten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie über den Befehl *dnsmgmt.msc* die DNS-Verwaltungskonsole.
2. Doppelklicken Sie hier den DNS-SERVER und wählen in der rechten Fensterhälfte aus dem Kontextmenü von FORWARD LOOKUP-ZONE den Eintrag NEUE ZONE. Klicken Sie dann auf WEITER.
3. Wählen Sie dann den Eintrag PRIMÄRE ZONE und klicken auf WEITER.
4. Im Fenster ACTIVE DIRECTORY… klicken Sie ebenfalls auf WEITER.
5. Auf der Seite ZONENNAME geben Sie den FQDN der externen Domäne an. Dieser Name kann beispielsweise *www.externername.de* lauten. Klicken Sie danach auf WEITER.
6. Im Fenster DYNAMISCHE UPDATES wählen Sie die Option KEINE DYNAMISCHEN UPDATES ZULASSEN und klicken auf WEITER und dann auf FERTIG STELLEN.
7. Markieren Sie nun die eben angelegte DNS-Zone und wählen aus deren Kontextmenü den Eintrag NEUER HOST (A).
8. Im Fenster NEUER HOST tragen Sie nichts in das Feld NAME ein. Sofern der FQDN das www beinhaltet, tragen Sie dieses in das Feld NAME ein. Im Feld IP-ADRESSE tragen Sie die lokale IP-Adresse des SBS ein. Klicken Sie dann auf HOST HINZUFÜGEN.

Es besteht auch die Möglichkeit, auf dem SBS einen DNS-Eintrag zu erstellen, der den externen FQDN zur internen IP-Adresse des SBS auflöst. Hiervon ist jedoch nicht die IP-Adresse betroffen, welche die Clients im Internet für eine Verbindung zum FQDN des SBS benutzen.

Um diesen zusätzlichen DNS-Eintrag zu erstellen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie die DNS-Administrationskonsole und wählen aus dem Kontextmenü des DNS-Servers den Eintrag NEUE ZONE. Klicken Sie auf WEITER.
2. Wählen Sie als Zonentyp eine PRIMÄRE ZONE und klicken dann auf WEITER.
3. Als Active Directory-Replikationsbereich wählen Sie die Option AN ALLE DOMÄNEN-CONTROLLER DER ACTIVE DIRECTORY-DOMÄNE. Klicken Sie dann auf WEITER.
4. Wählen Sie dann als Zonentyp eine FORWARD LOOKUP-ZONE aus und klicken auf WEITER.
5. Unter ZONENNAME tragen Sie den externen FQDN ein, z.B. *www.externername.de*. Klicken Sie auf WEITER.
6. Im Fenster DYNAMISCHE UPDATES wählen Sie die Option KEINE DYNAMISCHEN UPDATES ZULASSEN und klicken auf WEITER und dann auf FERTIG STELLEN.
7. Markieren Sie dann unter dem Eintrag FORWARD LOOKUP-ZONEN die eben erstellte Zone und wählen aus deren Kontextmenü NEUER HOST (A).
8. Im Fenster NEUER HOST tragen Sie im Feld NAME keinen Wert ein und im Feld IP-ADRESSE die interne IP-Adresse des SBS. Klicken Sie dann auf HOST HINZUFÜGEN.
9. Auf den Clientcomputern (Windows 2000 und XP) muss nun der DNS-Auflösungscache gelöscht werden. Geben Sie dazu an der Eingabeaufforderung der Clients den Befehl ipconfig /flushdns ein.

13.4.6 Interne Clients können sich nicht mit dem externen FQDN des SBS verbinden

Problem: Beim Zugriffsversuch eines internen Clients auf den SBS 2003 erhalten Sie die folgenden Fehlermeldung: Die Seite kann nicht angezeigt werden. Am Ende der Seite wird auf mögliche DNS-Probleme hingewiesen.

Ursache: Dieses Problem tritt auf, wenn der SBS 2003 nur über eine Netzwerkkarte verfügt und sich hinter einem Router befindet. Der Benutzer des internen Clients versucht dabei auf den SBS zuzugreifen, indem er dessen externen FQDN verwendet. Das Problem betrifft jedoch nicht sämtliche dieser Szenarien, sondern nur bei bestimmten Routermodellen und Firmware-Versionen dieser Router. Im Einzelnen sind die folgenden Routermodelle von diesem Problem betroffen:

- 3Com OfficeConnect Cable/DSL Gateway 3C855
- D-Link Broadband VPN Router DI-804
- Microsoft Wireless Basisstation MN-500
- Microsoft Basisstation MN-100

In der Regel werden die internen Netzwerkbenutzer den SBS nicht über den externen FQDN ansprechen. Jedoch müssen die Benutzer des Outlook Mobile Access (OMA) auf den externen Domänennamen des SBS zugreifen, um ihre mobilen Geräte mit Outlook synchronisieren zu können.

Lösung: Um das Problem zu umgehen, erstellen Sie eine DNS-Zone für den externen FQDN des Servers, so dass der FQDN zur internen IP-Adresse des SBS aufgelöst wird. Führen Sie dazu die folgenden Schritte durch:

1. Öffnen Sie die DNS-Administrationskonsole und wählen aus dem Kontextmenü des DNS-Servers den Eintrag FORWARD LOOKUP-ZONE und dann NEUE ZONE. Klicken Sie auf WEITER.
2. Wählen Sie als Zonentyp eine PRIMÄRE ZONE und klicken dann auf WEITER.
3. Unter ZONENNAME tragen Sie den externen FQDN ein, z.B. *www.externername.de*. Klicken Sie auf WEITER.
4. Im Fenster DYNAMISCHE UPDATES wählen Sie die Option NUR GESICHERTE UPDATES ZULASSEN und klicken auf WEITER und dann auf FERTIG STELLEN.
5. Markieren Sie dann unter dem Eintrag FORWARD LOOKUP-ZONEN die eben erstellte Zone und wählen aus deren Kontextmenü NEUER HOST (A).
6. Im Fenster NEUER HOST tragen Sie im Feld NAME keinen Wert ein und im Feld IP-ADRESSE die interne IP-Adresse des SBS.
7. Markieren Sie die Checkbox FÜR DIESEN EINTRAG EINEN PTR-EINTRAG ERSTELLEN und klicken dann auf HOST HINZUFÜGEN.
8. Sie erhalten dann eine Meldung, dass der PTR-Eintrag erfolgreich hinzugefügt wurde. Bestätigen Sie diese mit OK.

13.5 Probleme mit E-Mail und Fax

Im Folgenden finden Sie eine Auflistung typischer Probleme im Zusammenhang mit dem Senden und Empfangen von E-Mails und Faxen.

13.5.1 Es können keine E-Mails mehr gesendet und empfangen werden

Problem: Nach einer Weile tritt bei einem Benutzer das Problem auf, dass er keine E-Mails mehr senden und empfangen kann.

Ursache: Dies geschieht, wenn der Benutzer das Limit für die Postfach-Größenbeschränkung erreicht hat.

Lösung: Sie können zunächst die E-Mails in einem lokalen Ordner auf dem Client des Benutzers speichern. Sofern das Problem bei einem Benutzer wiederholt auftritt, sollten Sie darüber nachdenken, für sein Postfach die Größenbeschränkung heraufzusetzen. Die Anleitung dazu finden Sie in Kapitel 8.x.

13.5.2 An die Exchange-Postfächer werden unerwünschte E-Mails geschickt

Problem: An die Postfächer des Exchange Servers werden unerwünschte Nachrichten (Spam) gesendet.

Ursache: Für den Exchange Server wurde der Verbindungsfilter nicht konfiguriert.

Lösung: Konfigurieren Sie den Verbindungsfilter, der auf Grundlage von Sperrlisten unerwünschte E-Mails nicht an den Exchange Server sendet.

13.5.3 Mehrere vorhandene E-Mail-Domänen können nicht unter dem Assistenten für E-Mail und Internetzugang angegeben werden

Problem: Auf der Seite des Assistenten für die Konfiguration von Internet und E-Mail kann nur ein E-Mail-Domänenname angegeben werden (siehe Abbildung 2.28), obwohl mehrere verschiedene E-Mail-Domänen benutzt werden sollen.

Ursache: Auf der Seite des Assistenten wird nur eine E-Mail-Domäne angegeben, da Sie hier die Antwortadressen für die Domäne konfigurieren.

Lösung: Um mehrere E-Mail-Domänen zu verwenden, erstellen Sie nach Abschluss des Assistenten unter Exchange eine benutzerdefinierte Empfängerrichtlinie für eine zweite E-Mail-Domäne. Über diese Richtlinie werden die E-Mail-Adressen für die Benutzer der zweiten E-Mail-Domäne erstellt. Weitere Hinweise dazu finden Sie in Kapitel 4.4.6.

13.5.4 Probleme beim Download von externen POP3-E-Mails über den POP3-Connector

Problem: Auf dem SBS 2003 befindet sich eine große Anzahl unerwarteter E-Mails in der Exchange SMTP-Warteschlange. Diese E-Mails sind ausschließlich an Empfänger außerhalb der SBS-E-Mail-Domäne gerichtet. Dieses Symptom tritt auf, wenn der POP3-Connector nach dem Download der E-Mails vom externen POP3-Server fälschlicherweise die E-Mails an die Empfänger zurücksenden will, die nicht Mitglied der SBS 2003-E-Mail-Domäne sind.

Ursache: Dieses Problem tritt nicht auf, wenn die E-Mails mit Hilfe des Exchange Servers intern gehostet werden.

Lösung: Bei diesem Symptom handelt es sich um ein Problem des SBS 2003. Zu diesem Zweck sollten Sie das Update KB835734 einspielen. Dieses Update finden Sie auf der Begleit-CD im entsprechenden Verzeichnis.

13.5.5 Es kann keine Verbindung zu den POP3- und IMAP4-Diensten des SBS hergestellt werden

Problem: Beim Start des Exchange System Managers auf dem SBS 2003 werden die beiden Dienste POP3 virtueller Server sowie IMAP4 virtueller Server angehalten. Beim Versuch, die beiden Dienste über den Exchange System Manager neu zu starten, erhalten Sie eine Fehlermeldung.

Da die beiden Dienste beendet sind, können auch von Microsoft Outlook und Outlook Express aus keine Verbindungen mehr zum SBS 2003 hergestellt werden. Sie erhalten bei den Verbindungsversuchen zum POP3-Server oder IMAP4-Server entsprechende Fehlermeldungen.

Ursache: Dieses Problem liegt darin begründet, dass unter SBS 2003 standardmäßig der Microsoft Exchange POP3-Dienst sowie der Microsoft Exchange IMAP4-Dienst ausgeschaltet sind.

Lösung: Um diese Dienste zu aktivieren sowie die Firewall für diese beiden Dienste zuzulassen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie STARTMENÜ/PROGRAMME/VERWALTUNG/DIENSTE und doppelklicken den Dienst MICROSOFT EXCHANGE POP3.
2. Wählen Sie aus der Listbox STARTTYP den Eintrag AUTOMATISCH. Klicken Sie dann auf ÜBERNEHMEN und klicken unter DIENSTSTATUS auf STARTEN.
3. Wiederholen Sie diesen Schritt für den Dienst MICROSOFT EXCHANGE IMAP4 und schließen danach das Fenster DIENSTE.
4. Öffnen Sie dann die Serververwaltung und erweitern die AUFGABENLISTE. In der rechten Fensterhälfte klicken Sie auf MIT DEM INTERNET VERBINDEN.
5. Folgen Sie den Anweisungen des Assistenten, bis Sie zur Seite FIREWALL gelangen. Klicken Sie hier auf FIREWALL AKTIVIEREN und WEITER.

6. Klicken Sie auf HINZUFÜGEN und tragen in das Textfeld DIENSTNAME Microsoft Exchange POP3 ein. Unter PROTOKOLL tragen Sie TCP und unter PORT 110 ein. Klicken Sie dann auf OK.
7. Klicken Sie nochmals auf HINZUFÜGEN und tragen den DIENSTNAMEN Microsoft Exchange IMAP4, das PROTOKOLL TCP und den PORT 143 in die entsprechenden Felder ein und klicken auf OK.
8. Klicken Sie auf WEITER und beenden den Assistenten.

13.5.6 Die Fehlermeldung 5120 im Ereignisprotokoll

Problem: Im Ereignisprotokoll findet sich eine Fehlermeldung mit der Ereignis-ID 5120. Diese tritt auf, wenn ein- oder ausgehende E-Mails Anhänge enthalten. Allerdings müssen die Anhänge MIME-Felder enthalten, deren Typ *multipart/alternative* lautet. Standardmäßig lautet der MIME-Typ *multipart/mixed*. Bei E-Mail-Anhängen vom MIME-Typ *multipart/alternative* handelt es sich in der Regel um E-Mail-Würmer.

Ursache: Die Fehlermeldung kann auch auftreten, wenn ein Antivirenprogramm auf Dateiebene alle Ordner, darunter auch den Exchange-Ordner, scannt. Bei dem Virenscan auf Dateiebene können möglicherweise infizierte E-Mail-Anhänge bereits entfernt werden, bevor dieser Anhang vom SBS 2003 selbst gelöscht werden kann.

Lösung: Bei dieser Ereignismeldung handelt es sich also um keine Fehlermeldung im eigentlichen Sinne. Möglicherweise sollten Sie auf ein anders Antivirenprogramm umsteigen, das keinen Scan auf Dateiebene durchführt.

13.5.7 Probleme beim Senden von E-Mails via SMTP beim Einsatz eines Smart Host Servers

Problem: Beim Senden von E-Mails über den SMTP-Connector tritt das Problem auf, dass die Mails in der Warteschlange des Postausgangs verbleiben und nicht gesendet werden. Zusätzlich müssen die folgenden drei Bedingungen erfüllt sein, damit das Problem auftritt:

- Alle E-Mails werden an einen Smart Host-Server weitergeleitet.
- Der Smart Host-Server ist nicht identisch mit dem Mailserver Ihres Internet-Providers, auf dem die E-Mails gespeichert sind.
- Für das Abrufen der E-Mails wird die TURN-Authentifizierung angewendet.

Diese Konstellation trifft zu, wenn Sie im E-Mail- und Internetverbindungs-Assistenten die folgenden Einstellungen konfiguriert haben:

- Im Fenster E-MAIL-SENDEMETHODE klicken Sie auf ALLE E-MAILS AN DEN MAILSERVER DES ISP WEITERLEITEN. In das Textfeld MAILSERVER tragen Sie den Namen eines Smart Host-Servers ein.
- Im Fenster E-MAIL-SENDEMETHODE sind folgende Einstellungen vorgenommen: Markieren Sie die Checkbox EXCHANGE BENUTZEN. Klicken Sie auf E-MAIL WIRD BEIM ISP VORGEHALTEN, BIS MEIN SERVER EIN SIGNAL SENDET.

- Im Feld E-MAIL-SERVER, AN DEN DAS SIGNAL GESENDET WERDEN SOLL, geben Sie den Namen des Servers an. Hier handelt es sich um den Mailserver des ISP, an den Ihr Exchange-Server ein Signal sendet. Dieser Server unterscheidet sich vom Smart Host Server. Sie klicken auf TURN NACH AUTHENTIFIZIERUNG.
- Im Fenster INFORMATIONEN ZUR TURN-AUTHENTIFIZIERUNG geben Sie den Benutzernamen und das Kennwort für das Konto an, über das sich der Exchange Server gegenüber dem Mailserver des ISP authentifiziert.

Ursache: In dieser Konstellation schlägt die Authentifizierung fehl, wenn E-Mails über den SMTP-Connector gesendet werden sollen. Bei der Authentifizierung des SMTP-Connectors am Smart Host-Server verwendet er die Konteneinstellungen für ausgehende Verbindungen, die Sie für die TURN-Authentifizierung angegeben haben. Diese Konteneinstellungen sind für den Server konfiguriert, von dem der SBS die eingehenden E-Mails empfängt, und nicht für den Smart Host Server. Somit können Sie aufgrund des Authentifizierungsproblems nur Internet-E-Mails empfangen, jedoch nicht senden.

Lösung: Um die Konteneinstellung für ausgehende SMTP-Verbindungen zu ermitteln, öffnen Sie im Exchange System Manager den Eintrag CONNECTOREN und wählen aus dem Kontextmenü von SMALLBUSINESS SMTP-CONNECTOR den Eintrag EIGENSCHAFTEN. Auf der Registerkarte ERWEITERT klicken Sie auf AUSGEHENDE SICHERHEIT.

13.5.8 Es ist kein Faxempfang möglich

Problem: Es ist kein Empfang von Faxen möglich, obwohl das Faxmodem korrekt installiert ist und auch im Ereignisprotokoll keine Fehlermeldungen vorhanden sind.

Ursache: Das Modem muss zurückgesetzt werden.

Lösung: Um das Modem zurückzusetzen, ziehen Sie den Stecker des Modems und schließen es danach wieder neu an. Weitere Hinweise zum Zurücksetzen finden Sie möglicherweise in der Dokumentation des Geräts.

13.5.9 Die Weiterleitung von Faxen in die Dokumentenbibliothek ist nicht verfügbar

Problem: Weder im Faxkonfigurations-Assistenten noch in der Faxverwaltungskonsole ist die Option verfügbar, Faxe an die Dokumentenbibliothek weiterzuleiten.

Ursache: Wahrscheinlich sind die Faxdienste unter SYSTEMSTEUERUNG/SOFTWARE/WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN deinstalliert worden. Die Option zur erneuten Installation ist dort unter SBS 2003 nicht verfügbar.

Lösung: Sie müssen die Faxdienste erneut installieren.

1. Öffnen Sie dazu SYSTEMSTEUERUNG/SOFTWARE/WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN und deaktivieren die Checkbox FAXDIENSTE. Klicken Sie dann auf FERTIG STELLEN.
2. Wechseln Sie dann unter SOFTWARE zu ZURZEIT INSTALLIERTE PROGRAMME. Wählen Sie dort MICROSOFT WINDOWS SMALL BUSINESS SERVER 2003 und klicken auf ÄNDERN/ENTFERNEN.

3. Auf der Seite KOMPONENTENAUSWAHL wählen Sie unter AKTION den Eintrag FAX-DIENSTE und klicken auf INSTALLIEREN. Klicken Sie dann auf WEITER und folgen den weiteren Hinweisen des Assistenten.

13.6 Probleme mit der Überwachung

Dieses Kapitel stellt einige Probleme vor, die im Zusammenhang mit der Überwachung und den Leistungs- und Nutzungsberichten auftreten können.

13.6.1 Es werden keine Überwachungswarnungen mehr übermittelt

Problem: Es werden keine Überwachungswarnungen mehr übermittelt, nachdem eine Konfiguration des Health-Monitors importiert worden ist.

Ursache: Bei dem Import der Health-Monitor-Konfiguration mit Hilfe des Assistenten kommt es zu Problemen mit den importierten Aktionen, wenn die Aktionen immer noch auf den Computer verweisen, von dem sie importiert worden sind. So kann beispielsweise ein eingetragener SMTP-Server oder ein falscher Dateipfad nicht mehr gültig sein und zu Problemen führen.

Lösung: Damit die Überwachungswarnungen wieder korrekt funktionieren, müssen Sie die eingetragenen Daten der Aktionen aktualisieren. Öffnen Sie dazu in der Verwaltung den HEALTH MONITOR und klicken auf AKTIONEN. Wählen Sie dann aus dem Kontextmenü einer Aktion den Eintrag EIGENSCHAFTEN und prüfen die Einstellungen auf allen jeweils verfügbaren Registerkarten.

13.6.2 Laut Warnungsbenachrichtigung wurde ein Benutzerkonto angegriffen

Problem: In der Warnungsbenachrichtigung wird der Angriff auf ein Benutzerkonto mitgeteilt.

Ursache 1: Diese Benachrichtigung wird auch dann gesetzt, wenn der Benutzer die in der Anzahl der ungültigen Anmeldungen überschreitet, die in der Kontensperrungsschwelle festgelegt ist.

Ursache 2: Es hat tatsächlich ein Angriff auf das Benutzerkonto stattgefunden oder wird immer noch vorgenommen.

Lösung 1: Finden Sie also heraus, ob der Benutzer tatsächlich eine Reihe ungültiger Anmeldungen durchgeführt hat, da er sein Kennwort vergessen hat. In diesem Fall setzen Sie das Kennwort des Benutzerkontos zurück und teilen ihm das neue Kennwort mit.

Lösung 2: Hat tatsächlich ein Angriff stattgefunden oder läuft dieser immer noch, führen Sie die folgenden Schritte durch:

1. Prüfen Sie im Ereignisprotokoll unter SICHERHEIT unter den überwachten Anmeldeereignissen, ob bereits ein Angriff auf das lokale Netzwerk erfolgt ist.
2. Ermitteln Sie die IP-Adresse des angreifenden Computers und versuchen, über den Internetdienstanbieter nähere Informationen über diese IP-Adresse zu erhalten.
3. Schauen Sie in der SERVERVERWALTUNG unter BENUTZER nach, ob dort unbekannte Benutzerkonten vorhanden sind.
4. Setzen Sie das Kennwort des betroffenen Kontos unverzüglich zurück und deaktivieren dieses Konto, bis der Angriff beendet ist. Zusätzlich sollten Sie auch das Administrator-Kennwort zurücksetzen.
5. Trennen Sie den SBS 2003 von seiner Internetverbindung, bis der Angriff beendet ist.

13.6.3 In den Serverleistungs- und Nutzungsberichten sind nicht alle gewählten Protokolldaten enthalten

Problem: Im Serverleistungs- und Nutzungsbericht sind nicht alle Daten enthalten, die für die Protokollierung ausgewählt worden sind.

Ursache: Dem Bericht werden nur Daten als Anlagen hinzugefügt, wenn sich die zu protokollierenden Daten seit dem letzten Bericht geändert haben. Auch bei Anwendungen, die mehrere Protokolldateien erzeugen, wie z.B. die Internetinformationsdienste, werden keine neuen Anlagen für die Berichte versendet, wenn keine neuen Daten vorliegen.

Lösung: Da es sich um keinen Fehler handelt, sind auch keine weiteren Schritte erforderlich.

13.6.4 In den Servernutzungsberichten befinden sich keine Informationen über die Internetnutzung

Problem: In den Servernutzungsberichten sind zwar Daten enthalten, jedoch umfassen diese nicht die Informationen über die Internetnutzung.

Ursache 1: Wenn Sie die Firewall-Funktion des ISA-Servers verwenden, ist der SBS 2003 nicht in der Lage, die Firewall-Statistik des ISA-Servers zu überwachen.

Lösung 1: Sie müssen die Überwachung und Berichterstattung auf dem ISA-Server und nicht auf dem SBS 2003 einrichten.

Ursache 2: Sie verwenden einen Hardware-Router als Firewall. Auch in diesem Fall ist der SBS 2003 nicht in der Lage, die entsprechende Statistik des Geräts auszuwerten.

Lösung 2: Fügen Sie dem SBS 2003 eine zusätzliche Netzwerkkarte hinzu. Über den Assistenten für Internetzugang und E-Mail richten Sie dann den Routing- und RAS-Dienst als Firewall auf dem SBS 2003 ein.

13.6.5 Die Serverleistungs- und Nutzungsberichte werden unter Outlook Express nicht empfangen

Problem: Unter Outlook Express ist es nicht möglich, die Serverleistungs- und Nutzungsberichte zu empfangen.

Ursache: Standardmäßig sind unter Outlook Express verschiedene Dateianlagen gesperrt. Damit soll das Risiko minimiert werden, dass möglicherweise gefährliche Anhänge geöffnet werden könnten.

Lösung: Um die Anlagen zuzulassen, öffnen Sie unter Outlook Express im Menü EXTRAS den Eintrag OPTIONEN. Wechseln Sie auf die Registerkarte SICHERHEIT und deaktivieren dort die Checkbox SPEICHERN ODER ÖFFNEN VON ANLAGEN, DIE MÖGLICHERWEISE EINEN VIRUS ENTHALTEN KÖNNTEN, NICHT ZULASSEN.

13.7 Probleme mit mobilen Geräten

In diesem Kapitel werden einige Szenarien vorgestellt, die im Zusammenhang mit der Benutzung mobiler Geräte auftreten können.

13.7.1 ActiveSync kann nicht installiert werden

Problem: Die Applikation ActiveSync kann nicht auf dem Clientcomputer installiert werden.

Ursache: Für die Installation von ActiveSync darf das mobile Gerät nicht an den Clientcomputer angeschlossen sein. Die Installation wird in diesem Fall nicht vollständig abgeschlossen.

Lösung: Um die Applikation erneut zu installieren, trennen Sie das angeschlossene mobile Gerät vom Clientcomputer, melden sich erneut an und starten dann die Installation neu.

13.7.2 Es kann keine Verbindung zwischen dem mobilen Gerät und dem Clientcomputer hergestellt werden

Problem: Es ist nicht möglich, zwischen dem mobilen Gerät und dem Clientcomputer eine Verbindung herzustellen.

Ursache: Höchstwahrscheinlich liegt ein Problem mit der USB-Verbindung der beiden Geräte vor. Möglicherweise ist auch nicht die aktuelle Version von ActiveSync installiert.

Lösung: Prüfen Sie zunächst, ob die aktuelle Version von ActiveSync auf dem Clientcomputer installiert ist. Ist dies der Fall, nehmen Sie das mobile Gerät aus der Basisstation oder trennen die Kabelverbindung. Schalten Sie dann das mobile Gerät aus und erneut wieder ein, bevor Sie es mit dem Clientcomputer verbinden.

13.7.3 Ein angeschlossenes mobiles Gerät kann nicht das Internet durchsuchen, wenn der ISA Server 2000 installiert ist

Problem: Sofern der ISA Server 2000 installiert ist, kann ein Benutzer nicht das Internet mit seinem mobilen Gerät durchsuchen, wenn dieses über die Basisstation oder ein Kabel angeschlossen ist.

Ursache: Ist das mobile Gerät angeschlossen, wird dessen Benutzer wie ein anonymer Benutzer behandelt. Der ISA Server 2000 untersagt jedoch das Durchsuchen des Internets für anonyme Benutzer.

Lösung: Je nach installiertem Betriebssystem auf dem mobilen Gerät müssen Sie unterschiedliche Lösungswege einschlagen. Anschließend müssen noch einige Einstellungen unter ActiveSync vorgenommen werden. Diese sind unabhängig vom Betriebssystem des mobilen Geräts für alle gleich.

Microsoft SmartPhone 2003

1. Öffnen Sie auf dem mobilen Gerät START/EINSTELLUNGEN/DATE CONNECTIONS.
2. Öffnen Sie dann MENU/EDIT CONNECTIONS/PROXY CONNECTIONS.
3. Klicken Sie unter MENU auf HINZUFÜGEN.
4. Unter CONNECTS FROM wählen Sie die Option WORK, unter CONNECTS TO die Option INTERNET.
5. Tragen Sie unter PROXY (NAME:PORT) den Namen und Port des Proxy-Servers ein. Die Portnummer lautet 8080. Geben Sie weiterhin noch Ihren Benutzernamen und das Kennwort ein und klicken dann auf FERTIG STELLEN.

Microsoft Pocket PC Phone Edition 2003

1. Öffnen Sie START/EINSTELLUNGEN. Klicken Sie unter VERBINDUNGEN auf VERBINDUNGEN und dann auf SET UP MY PROXY SERVER.
2. Wechseln Sie auf die Registerkarte PROXY-EINSTELLUNGEN. Aktivieren Sie hier die Checkboxen DIESES NETZWERK STELLT EINE VERBINDUNG MIT DEM INTERNET HER sowie DIESES NETZWERK VERWENDET EINEN PROXY-SERVER. Tragen Sie dann den Namen des Proxy-Servers ein und klicken auf ERWEITERT.
3. Unter ANSCHLUSS tragen Sie die Portnummer 8080 ein. Bestätigen Sie diesen Vorgang mit OK.

Microsoft Pocket PC Phone Edition 2002

1. Öffnen Sie START/EINSTELLUNGEN. Klicken Sie unter VERBINDUNGEN auf VERBINDUNGEN.
2. Unter WORK SETTINGS klicken Sie auf ÄNDERN und wechseln auf die Registerkarte PROXY-EINSTELLUNGEN.
3. Aktivieren Sie hier die Checkboxen DIESES NETZWERK STELLT EINE VERBINDUNG MIT DEM INTERNET HER sowie DIESES NETZWERK VERWENDET EINEN PROXY-SERVER. Tragen Sie dann den Namen des Proxy-Servers ein und klicken auf ERWEITERT.

4. Unter ANSCHLUSS tragen Sie die Portnummer 8080 ein. Bestätigen Sie diesen Vorgang mit OK.

Einstellungen unter ActiveSync

Diese Einstellungen müssen unabhängig davon, welches System Sie verwenden, immer vorgenommen werden.

1. Öffnen Sie unter *ActiveSync* das Menü EXTRAS/OPTIONEN und wechseln auf die Registerkarte REGELN.
2. Wählen Sie unter VERBINDUNG den Eintrag BÜRO.

   Beim ersten Durchsuchen des Internets werden Sie aufgefordert, einen Benutzernamen und ein Kennwort anzugeben. Das anzugebende Benutzerkonto muss Mitglied der Gruppe Internet Users sein.

13.7.4 Die erste Synchronisation zwischen Outlook und dem mobilen Gerät schlägt fehl

Problem: Die erste Synchronisation zwischen Outlook 2003 und dem mobilen Gerät kann nicht durchgeführt werden. Sie erhalten die Fehlermeldung, dass das Profil nicht gefunden werden konnte.

Ursache: Solange der Benutzer Outlook 2003 noch nicht ausgeführt hat, kann Outlook kein Profil anlegen. ActiveSync ist nicht in der Lage, selber ein Profil anzulegen.

Lösung: Starten Sie Outlook und schließen das mobile Gerät über seine Basisstation oder mit einem Kabel an den Clientcomputer an. Achten Sie beim Anschluss des mobilen Geräts auf die folgende Reihenfolge:

1. Starten Sie das Programm *ActiveSync*.
2. Verbinden Sie die Basisstation des mobilen Geräts über das USB-Kabel oder den COM-Anschluss mit dem Clientcomputer. Bei Verwendung des COM-Anschlusses müssen Sie sicherstellen, dass der bei der *ActiveSync*-Installation benutzte COM-Anschluss nicht verwendet wird. Um den COM-Anschluss freizugeben, klicken Sie unter *ActiveSync* im Menü DATEI auf GET CONNECTED.
3. Legen Sie das mobile Gerät in die Basisstation oder verbinden das Kabel. *ActiveSync* stellt automatisch eine Verbindung mit dem mobilen Gerät her.

13.7.5 Die Synchronisation eines angeschlossenen mobilen Geräts ist nicht möglich

Problem: Sobald das mobile Gerät über seine Basisstation oder ein Kabel an den Clientcomputer angeschlossen ist, kann es nicht synchronisiert werden.

Ursache: Auf dem SBS 2003 ist der ISA-Server oder Routing und RAS (RRAS) eingerichtet. Dafür wurde die Option DURCHGANG UNTER ACTIVESYNC nicht korrekt konfiguriert.

Lösung: Öffnen Sie auf dem Client das Programm ActiveSync. Wählen Sie aus dem Menü EXTRAS den Eintrag OPTIONEN und wechseln dort auf die Registerkarte REGELN. Bei der Option VERBINDUNG unter DURCHGANG wählen Sie den Eintrag INTERNET aus.

13.7.6 Probleme mit Outlook Mobile Access (OMA) und SSL

Problem: Auf einigen Geräten mit SmartPhone 2002, Pocket PC 2002 oder WAP 2.0 (Wireless Application Protocol) treten Probleme bei der Verwendung von Outlook Mobile Access in Verbindung mit SSL (Secure Sockets Layer) auf.

Ursache: Einige Geräte werden nicht unterstützt, sofern Sie nicht das signierte Zertifikat des SBS 2003 verwenden.

Lösung: Stellen Sie das geeignete signierte Zertifikat bereit.

A SBS 2003 und Firewalls ohne ISA-Server

In diesem Kapitel wird die Konfiguration einer Firewall für den Einsatz mit SBS 2003 beschrieben. Sofern Sie nicht die Premium Edition des SBS 2003 erworben haben und somit nicht den ISA Server 2000 als Firewall einsetzen, dürfte in den meisten kleineren Unternehmen ein separates Firewall-Gerät vorhanden sein. Dieses kann unter bestimmten Umständen auch gemeinsam mit der in den SBS 2003 integrierten Firewall betrieben werden. Oftmals handelt es sich dabei um eine Kombination aus Firewall und DHCP-Server.

Ist dieses Gerät UPnP-fähig (Universal Plug & Play), so wird die Konfiguration der verschiedenen vom SBS 2003 benötigten Ports über den Assistenten E-Mail und Internetverbindung vorgenommen. Ist das Gerät nicht UPnP-fähig, so müssen Sie die Konfiguration der Firewall manuell durchführen.

Dient die Firewall zusätzlich auch als Router und ist der SBS über eine Netzwerkkarte mit dem lokalen Netzwerk, über die andere mit dem Internet verbunden, so können Sie sowohl die Firewall des SBS 2003 oder die Firewall-Funktionalität des Kombigeräts oder auch beide gemeinsam nutzen.

Tabelle A.1 zeigt Ihnen eine Übersicht über die vom SBS 2003 für die verschiedenen Dienste genutzten Portnummern. Bei sämtlichen Diensten handelt es sich um TCP-Protokolle. Eine komplette Aufstellung aller Ports finden Sie im Internet unter der Adresse `http://www.iana.org/assignments/port-numbers`. Dort sind auch sämtliche Ports verzeichnet, die von Applikationen bestimmter Hersteller reserviert sind.

Portnummer	Dienst	Beschreibung
21	FTP (File Transfer Protocol)	Bevor Sie den Server als FTP-Server einrichten, müssen Sie zunächst den FTP-Dienst hinzufügen und einrichten.
25	E-Mail	Maileingang und -ausgang über das SMTP-Protokoll (Simple Mail Transfer Protocol).
80 (http)	Webserver	Internetzugriff, Outlook Web Access (OWA), Outlook Mobile Access (OMA), Aufruf von Leistungs- und Nutzungsberichten des SBS, Firmenwebseite (wwwroot) sowie Outlookzugriff über das Internet (RPC) ohne VPN-Verbindung.
443 (https)	Webserver; Remote-Webarbeitsplatz	http-Anfragen über SSL (Secure Sockets Layer); Webarbeitsplatz siehe die betreffende Spalte dieser Tabelle.

Portnummer	Dienst	Beschreibung
444	SharePoint Services-Intranet-Webseite	Sicherung der Client-Server-Kommunikation beim Zugriff auf die Intranet-Webseite der Firma sowie weitere unter *http://companyweb* bereitgestellte Seiten.
1723	VPN (Virtual Private Network)	Aufbau einer sicheren Verbindung von Remote-Clients zum Firmennetzwerk.
3389	Terminaldienste	Benutzung der Terminaldienste des SBS 2003 durch Remote-Clients.
4125	Remote-Webarbeitsplatz	Verbindung über Outlook Web Access (OWA) zum lokalen Netzwerk, Remote-Desktop-Verbindung zu Clients des lokalen Netzwerks, Zugriff auf die Intranet-Webseite der SharePoint-Services sowie Herunterladen des Verbindungsmanagers für die Konfiguration des Remote-Zugriffs.

Tabelle A.1: Die vom SBS 2003 standardmäßig verwendeten Portnummern

B Konfiguration eines DHCP-Servers für SBS 2003

Im SBS 2003-Netzwerk können Sie entweder den DHCP-Serverdienst (Dynamic Host Configuration Protocol) des SBS 2003 oder den eines anderen DHCP-Servers benutzen. Dabei kann es sich um einen Router mit DHCP-Funktionalität oder um einen separaten DHCP-Server handeln.

Möchten Sie den DHCP-Dienst des SBS 2003 nutzen, so dürfen Sie den ursprünglichen DHCP-Dienst erst dann beenden, wenn das Setup-Programm Sie dazu auffordert. Anderenfalls kann vom Setup-Programm nicht festgestellt werden, welcher IP-Adressbereich bisher verwendet wurde.

Konfiguration eines bestehenden DHCP-Servers

Möchten Sie den DHCP-Dienst auch nach der Installation des SBS von einem anderen Server ausführen lassen, so müssen Sie sicherstellen, dass der Dienst auch korrekt konfiguriert ist.

Öffnen Sie auf dem DHCP-Server die *dhcp.mmc*, sofern es sich um einen Windows-basierten DHCP-Server handelt. Verwenden Sie beispielsweise einen Unix-basierten Server, nehmen Sie die im Folgenden beschriebenen Einstellungen in der jeweiligen Konfigurationsdatei vor.

1. Erstellen Sie einen neuen DHCP-Bereich. Die Details der Bereichsoptionen finden Sie in der Tabelle XXX. Stellen Sie zudem sicher, dass in dem Bereich eine ausreichende Anzahl von IP-Adressen für sämtliche Clients und andere Netzwerkgeräte mit eigener IP-Adresse vorhanden ist. Sie müssen auch IP-Adressen für alle geplanten RAS-Server und Remote-Benutzer hinzufügen.
2. Unter xx schließen Sie die eigene IP-Adresse des DHCP-Servers für das lokale Netzwerk aus der Liste der zu vergebenden Adressen aus. Schließen Sie auch die Adressen aus, die von Geräten mit einer statischen IP-Adresse belegt sind. Um auf der sicheren Seite zu sein, sollten Sie ca. fünf oder mehr Adressen ausschließen, so dass Sie später weitere Netzwerkgeräte mit einer statischen IP-Adresse konfigurieren können.

Tabelle B.1 gibt die zu konfigurierenden DHCP-Bereichsoptionen an. Diese sind auf einem Windows-basierten DHCP-Server verfügbar und sollten es auch auf dem von Ihnen verwendeten sein, wenn dieser nicht Windows-basiert ist.

DHCP-Bereichsoption	Beschreibung
Router (Standard-Gateway)	Ist der SBS als Gateway eingerichtet und besitzt zwei Netzwerkkarten, tragen Sie hier die Adresse der Karte für die Verbindung mit dem lokalen Netzwerk ein. Verfügt der SBS 2003 nur über eine Netzwerkkarte und wird die Internetverbindung über einen Router hergestellt, tragen Sie hier die interne IP-Adresse des Routers ein.
DNS-Server	Tragen Sie hier die Adresse der Netzwerkkarte für die Verbindung zum lokalen Netzwerk ein. Wird der DNS-Dienst auf einem separaten Server ausgeführt, tragen Sie dessen IP-Adresse hier ein.
DNS-Domänenname	Tragen Sie hier den vollständigen Namen (FQDN, Fully Qualified Domain Name) der internen Domäne ein, z.B. *sbs2003.local*. Dieser Name wird automatisch den Clients zugewiesen.
WINS-Server	Tragen Sie hier ebenfalls die IP-Adresse des SBS 2003 ein, sofern Sie keinen anderen WINS-Server im Einsatz haben. Die WINS-Unterstützung ist lediglich für Clients der Betriebssysteme Windows NT 4.0 sowie Windows 9x erforderlich.
WINS-Knotentyp	Tragen Sie als Knotentyp den Wert hybrid oder H-Knoten (0x8) ein. Durch Setzen des WINS-Knotentyps wird im Netzwerk unnötiger Broadcast-Verkehr unterbunden.

Tabelle B.1: Die Bereichsoptionen eines DHCP-Servers konfigurieren

Stichwortverzeichnis

C

D

E

H

I

K

L

M

N

O

P

Q

R

S

Copyright

Zusatzdaten

Möglicherweise liegt dem gedruckten Buch eine CD-ROM mit Zusatzdaten bei. Die Zurverfügungstellung dieser Daten auf der Website ist eine freiwillige Leistung des Verlags. Der Rechtsweg ist ausgeschlossen.