

Windows Server 2003

Schritt für Schritt zum Profi

UWE BÜNNING JÖRG KRAUSE



WOCHE 1

Tag 1	Einführung	11
Tag 2	Installation	33
Tag 3	Administrationswerkzeuge	67
Tag 4	Fernadministration	125
Tag 5	Massenspeicherverwaltung	159
Tag 6	Dateisysteme	207
Tag 7	Geräte und Dienste	243

WOCHE 2

Tag 8	Wichtige Netzwerkgrundlagen	267
Tag 9	Active Directory-Einführung	305
Tag 10	Active Directory installieren	343
Tag 11	Active Directory – erste Schritte	369
Tag 12	Dateiserver-Funktionen	397
Tag 13	Druckserver-Funktionen	439
Tag 14	DHCP und DNS	467

WOCHE 3

Tag 15	Clientsysteme administrieren	507
Tag 16	Ausbau des Verzeichnisses	551
Tag 17	Weitere Serverfunktionen	571
Tag 18	Internet-Informationsdienste	607
Tag 19	Weitere IIS-Funktionen	641
Tag 20	Scripting	671
Tag 21	Reparatur und Datensicherung	697



Administrations- werkzeuge



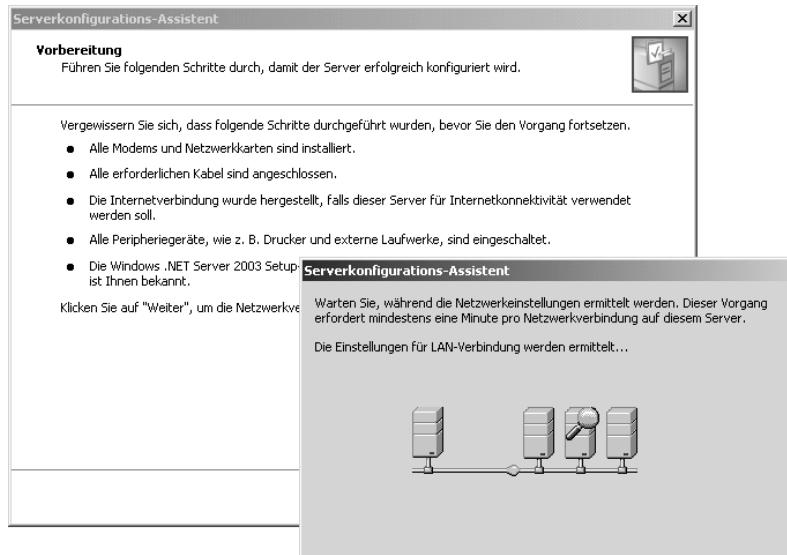
Windows Server 2003 liefert ein umfassendes Arsenal an Dienstprogrammen und Assistenten, mit deren Hilfe Sie alle Administrationsaufgaben schnell und effizient erledigen können. Am heutigen Tag lernen Sie die wichtigsten Werkzeuge und deren wesentlichen Bedienschritte kennen.

3.1 Überblick

In diesem Abschnitt werden die wichtigsten Gruppen von Administrationswerkzeugen vorgestellt.

Die Windows-Assistenten

Für den Administrator eine nicht zu unterschätzende Hilfe sind die Assistenten, die an vielen Stellen die Arbeit stark vereinfachen. Zusätzlich können Sie damit eine höhere Sicherheit Ihres Systems erreichen, wenn Sie beispielsweise einen Assistenten dann konsequent einsetzen, wenn Sie mit den Details zu der betreffenden Funktion nicht 100%ig vertraut sind. Die durch einen Assistenten vorgenommenen Standardeinstellungen werden in aller Regel auf eine maximale Sicherheit hin ausgerichtet sein.



*Abbildung 3.1:
Der Serverkonfigurations-Assistent erlaubt das schrittweise Hinzufügen oder Entfernen von Funktionen*

Viele Assistenten erklären sich selbst, sodass sie nicht separat in diesem Buch behandelt werden müssen. Allerdings ist es nützlich zu wissen, welche Assistenten für die wichtigsten Aufgaben überhaupt verfügbar sind und was sie »anrichten«. Deshalb werden diese in Abschnitt *Wichtige Assistenten* ab Seite 71 vorgestellt und im Verlaufe des Buches immer wieder in die Betrachtungen mit einbezogen.



Für Standard-Einrichtungsaufgaben sollten Sie, wenn möglich, immer auf einen der Assistenten zurückgreifen. Das erspart Ihnen unter Umständen viel Zeit und führt in der Regel zu einer funktionierenden Grundkonfiguration, die Sie nachträglich an konkrete Erfordernisse anpassen können.

Die Microsoft Managementkonsole

Vorab die wichtigste Information zur Beruhigung: Für jede wichtige Funktion gibt es ein grafisches Dienstprogramm – und was noch besser ist, die Mehrzahl dieser Programme gleicht sich in der Bedienung. Das ist vor allem dem konsequent durchgesetzten Konzept der Microsoft Managementkonsole (MMC; von engl. *Microsoft Management Console*) zu verdanken.

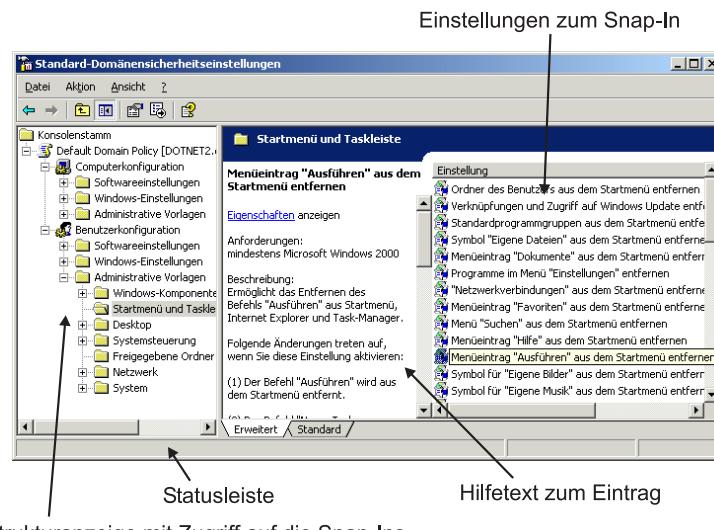


Abbildung 3.2:
Die Managementkonsole Computerverwaltung

Strukturansicht mit Zugriff auf die Snap-Ins

Die Managementkonsole ist selbst eine Windows-Anwendung, in welche so genannte Snap-Ins eingebunden werden. Diese Snap-Ins sind die eigentlichen grafischen Werkzeuge, die dank der Managementkonsole über ein einheitliches Bedienschema verfügen. Windows Server 2003 bringt für alle wichtigen Aufgaben bereits Snap-Ins mit, die in einer Reihe vorgefertigter Managementkonsolen zusammengefasst worden sind.



Neben den vorgefertigten Managementkonsolen können Sie auch Ihre eigenen Konsolen entwerfen. Diese lassen sich dann mit grafischen Mitteln sogar so gestalten, dass die Bedienung noch weiter vereinfacht werden kann.

Weitere wichtige grafische Dienstprogramme

Neben den als Snap-Ins ausgeführten Dienstprogrammen gibt es weitere, konventionell als Windows-Anwendungen implementierte Tools. Dies sind beispielsweise der für die direkte Serverüberwachung wichtige Task-Manager oder die mitgelieferte Datensicherungslösung.

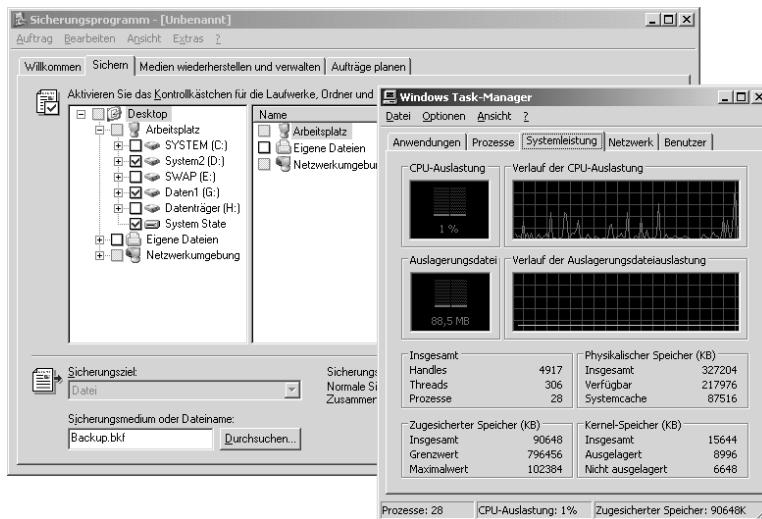


Abbildung 3.3:
Wichtige grafische
Dienstpro-
gramme, die nicht
als MMC-Snap-
Ins ausgelegt sind

Die wichtigsten Programme werden am heutigen Tag näher vorgestellt.

Tools für den Einsatz an der Eingabeaufforderung

An die Verfechter der Eingabeaufforderung oder Unix-Umsteiger wurde ebenfalls gedacht. Wie die ersten Windows-Versionen verfügt Windows Server 2003 über eine Kommandozeile, über die Sie Dienstprogramme mit all ihren notwendigen Parametern starten können. Für alle wesentlichen Administrationsaufgaben, die Sie mit den grafischen Dienstprogrammen erledigen können, gibt es ein passendes Kommandozeilen-Tool. Dazu wurden dem Lieferumfang von Windows Server 2003 viele nützliche Programme hinzugefügt, die für die Windows 2000 Serversysteme nur gegen Aufpreis im Ressource Pack enthalten waren.



```
c:\ Eingabeaufforderung
C:\Dokumente und Einstellungen\Administrator>dir /w
Datenträger in Laufwerk C: ist SYSTEM
Volumeseriennummer: 500F-2376

Verzeichnis von C:\Dokumente und Einstellungen\Administrator

[.]      [..]      [Desktop]      [Eigene Dateien]
[Favoriten]  [Startmenü]  Sti_Trace.log
              1 Datei(en)  0 Bytes
              6 Verzeichnis(se),  2.537.791.488 Bytes frei

C:\Dokumente und Einstellungen\Administrator>fsutil
---- Unterstützte Befehle ----

behavior      Steuert das Dateisystemverhalten
dirty         Verwaltet fehlerhafte Bits auf dem Volume
file          Dateispezifische Befehle
fsinfo        Datenstrukturinformationen
hardlink      Hardlinkverwaltung
objectid      Objektkennungswartung
quota         Kontingenzpunktwartung
reparsepoint  Analysepunktwartung
sparse        Steuert geringe Dateidatendichte
usn          USN-Verwaltung
volume        Volumeverwaltung

C:\Dokumente und Einstellungen\Administrator>
```

Abbildung 3.4:
An der Eingabeaufforderung können prinzipiell ebenfalls alle Administrationsaufgaben erledigt werden

Damit ist Windows Server 2003 das erste Windows-Serverbetriebssystem von Microsoft, welches standardmäßig komplett von der Kommandozeile aus administriert werden kann.

Automatisierung und eigene Tools

Neben diesen »fertigen« Hilfsmitteln können Sie sich auch eigene Tools schaffen. Dazu lassen sich die integrierten Programmierungsmöglichkeiten nutzen. Im Mittelpunkt stehen aus Sicht des Administrators sicherlich die Scripting-Funktionen, mit deren Hilfe Sie den Aufruf bestehender Dienstprogramme automatisieren oder sogar gänzlich neue Tools erstellen können. Diesem Thema haben wir aufgrund der Komplexität einen ganzen Tag gewidmet – den Tag 20.

3.2 Wichtige Assistenten

Für zentrale Administrationsaufgaben gibt es einige Assistenten, die Sie kennen sollten. Sie werden in diesem Abschnitt vorgestellt.

Serverkonfigurations-Assistent

Den Serverkonfigurations-Assistent können Sie folgendermaßen starten:

1. Wählen Sie den entsprechenden Eintrag im Menü VERWALTUNG, welches Sie über das Startmenü öffnen können.
2. Geben Sie an der Eingabeaufforderung den Befehl Cys.exe ein.



Der Assistent arbeitet dann wie folgt:

1. Prüfung aller Netzwerkverbindungen auf korrekte Konfiguration

In Abbildung 3.1 auf Seite 68 sehen Sie diesen Assistenten in dieser ersten Phase in Aktion. Wird beispielsweise erkannt, dass eine Netzwerkverbindung getrennt ist, erhalten Sie eine entsprechende Mitteilung. Sie können dann entscheiden, ob der Assistent fortfahren oder abbrechen soll.

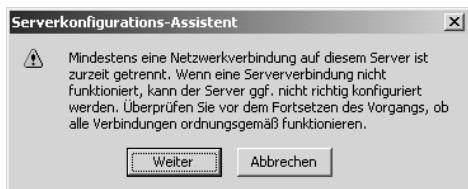


Abbildung 3.5:
Ein Fehler in einer Netzwerkverbindung wurde festgestellt

Ein Server, der über mehrere Netzwerkadapter verfügt, kann für die erste Einrichtung vielleicht noch nicht vollständig an das Netzwerk angeschlossen sein. Dann ist es hilfreich, dass Sie den Assistenten mit einem Klick auf WEITER trotzdem fortfahren lassen können.

2. Einrichten von Serverfunktionen

Nach dieser ersten Überprüfung werden Sie zur Einrichtung der Serverfunktionen geführt. Einen Überblick über diese Funktionen haben Sie bereits in Abschnitt *Funktionen stehen im Mittelpunkt* ab Seite 63 kennen gelernt.

Serverfunktionen automatisch oder benutzerdefiniert einrichten

Die Serverfunktionen lassen sich auf zwei verschiedenen Wegen einrichten. Der Assistent bietet Ihnen im nächsten Dialogfenster folgendes an:

■ STANDARDKONFIGURATION FÜR EINEN ERSTEN SERVER

Der Assistent übernimmt vollautomatisch die erste Einrichtung des Servers. Dabei wird eine neue Active Directory-Domäne eingerichtet. Der Server fungiert dann als erster Domänencontroller dieser Domäne. Hinzu kommen weitere Einrichtungsschritte, um beispielsweise einen Internetzugang über den Server im gesamten Netzwerk nutzen zu können.



Sie sollten den Assistenten mit diesem automatischen Modus nur dann einsetzen, wenn Sie ein Netzwerk neu einrichten wollen. Sie müssen dabei wissen, was der Verzeichnisdienst Active Directory ist und wie die einzelnen Komponenten bis hin zum DNS mit diesem zusammenspielen. Unbedingt vermeiden sollten Sie den Assistenten, wenn Sie den Server in eine bestehende Netzwerkstruktur einbinden wollen – ob mit oder ohne Domäne.

Wenn Sie sich neu mit dem Windows Server 2003 vertraut machen, brechen Sie den Assistenten an dieser Stelle zunächst ab. An den nächsten Tagen erhalten Sie das notwendige »Rüstzeug«, mit dessen Hilfe Sie Ihren Server optimal als Domänencontroller in einer Active Directory-Domäne einrichten können. Sie können danach entscheiden, ob Sie dazu diesen Assistenten benutzen oder andere Wege gehen wollen.

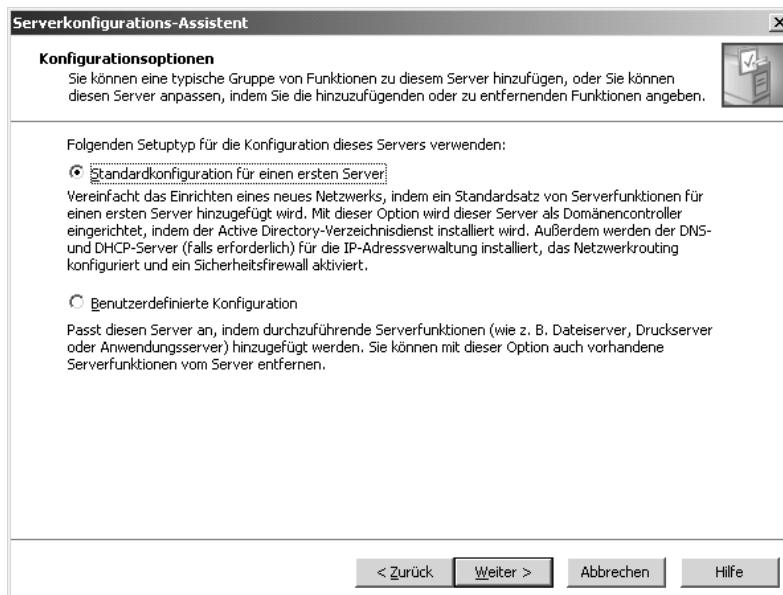


Abbildung 3.6:
Auswahl zwischen einer vollautomatischen Standardeinrichtung und der benutzerdefinierten Konfiguration



Dieser automatische Assistent und damit das Auswahlfenster (siehe Abbildung 3.6) erscheinen nur dann, wenn

- ▶ der Server noch nicht einer Domäne angeschlossen oder als Domänencontroller eingerichtet ist,
- ▶ Sie das Programm direkt am Server, also nicht über eine Terminalsession aufrufen, und
- ▶ der Server nicht als DNS-, DHCP- oder RAS-Server eingerichtet ist.

Weitere Voraussetzungen sind, dass mindestens ein Laufwerk mit dem Dateisystem NTFS formatiert sowie das Protokoll TCP/IP eingerichtet ist. Zu letzterer Bedingung ist zu beachten, dass eine feste IP-Adresse eingerichtet sein muss. Erhält der Server über einen DHCP-Server seine IP-Adresse, wird dieses Dialogfenster ebenfalls nicht eingeblendet.



■ BENUTZERDEFINIERTE KONFIGURATION

Die zweite Option startet ein Dialogfenster mit einer Liste der Serverfunktionen. Um eine bestimmte Funktion, die noch nicht konfiguriert ist, einzurichten, markieren Sie diese und klicken auf WEITER. Es startet dann der entsprechende Assistent, der Sie durch die weiteren Schritte führt.

Zum Verwalten von bereits eingerichteten Funktionen werden im rechten Bereich weiterführende Links angeboten, mit denen Sie die entsprechenden Administrationswerkzeuge aufrufen können.

Wollen Sie dem Server eine bestimmte Funktion wieder entziehen, reicht es aus, auf die Schaltfläche WEITER zu klicken.

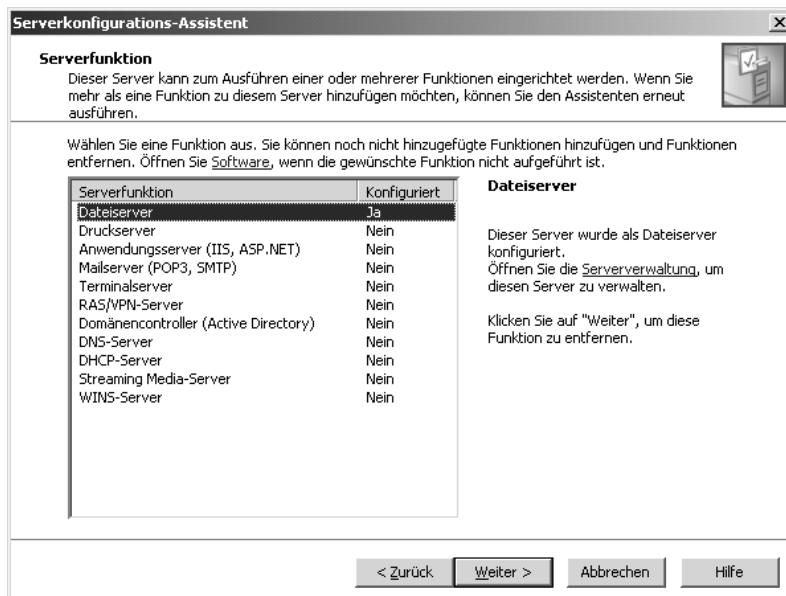


Abbildung 3.7:
Die einzelnen
Serverfunk-
tionen benutzer-
definiert
einrichten

An dieser Stelle sollten Sie noch keine weiteren Einrichtungsschritte unternehmen. Wenn Sie dennoch einen Assistenten testen wollen, wählen Sie die Funktionen *Dateiserver* oder *Druckserver*. Die Einstellungen, die Sie darüber vornehmen, sind unkritisch und beeinflussen nicht das gesamte Systemverhalten des Servers.

Anders sieht es aus, wenn Sie beispielsweise einen DNS-Server oder einen Domänencontroller mit Hilfe des Assistenten einrichten. Hierbei sollten Sie genau wissen, was der Assistent im Hintergrund alles so einrichtet. Das gilt umso mehr, wenn Sie den Server in eine bereits bestehende Netzwerklandschaft einbinden wollen.



Assistent zum Installieren von Active Directory

Für die Ersteinrichtung eines Servers für den Betrieb mit dem Verzeichnisdienst Active Directory sollten Sie generell diesen Assistenten einsetzen. Der Assistent hilft Ihnen unter anderem bei diesen Aufgaben:

- *Anlegen einer neuen, ersten Active Directory-Domäne*: Dabei wird der Server zum ersten Domänencontroller heraufgestuft und die Verzeichnisdatenbank eingerichtet.
- *Einrichten eines zusätzlichen Domänencontrollers für eine bestehende Domäne*: Der Server wird zum Domänencontroller (DC) heraufgestuft und in eine bestehende Domäne integriert. Dabei erhält er eine Kopie der Verzeichnisdatenbank. Nach dem Vorgang ist der neue Domänencontroller ein gleichberechtigtes Mitglied in der Reihe der DCs dieser Domäne. Allerdings sollten Sie danach bestimmte Optimierungen an der Konfiguration der DCs vornehmen. Zwar sind im Active Directory alle DCs gleich, einige Rollen sind dennoch zwischen ihnen aufgeteilt.
- *Anlegen einer neuen, untergeordneten Domäne*: Domänen können im Active Directory hierarchisch aufgebaut werden. Allerdings sollten Sie gute Gründe haben, mit mehreren Domänen in Ihrem Netzwerk zu arbeiten. Für kleine bis mittlere Netzwerke, um die es im vorliegenden Buch primär geht, sind solche Konstruktionen in aller Regel nicht geeignet. Im Normalfall reicht es aus, eine einzige Domäne anzulegen und in dieser alle weiteren Untergliederungen mit Hilfe von Organisationseinheiten vorzunehmen.

Komplexe Gebilde wie *Gesamtstrukturen* (engl. *Forest*) oder *Domänenstrukturen* (engl. *Tree*), die sich aus Konfigurationen mit mehreren Domänen ergeben können, werden deshalb in diesem Buch praktisch nicht weiter erörtert.

Die erste Einrichtung einer Active Directory-Domäne und damit eines Domänencontrollers ist dank dieses leistungsfähigen Assistenten in wenigen Minuten erledigt. Allerdings sollten Sie dabei einige Grundlagen wissen, welche am Tag 9 behandelt werden.



Ist die Domäne erst einmal angelegt, lassen sich viele Einrichtungsdetails, seien es auch nur die Namen für die Domäne oder die Domänencontroller, nur noch mit viel Aufwand nachträglich ändern. Eine gute Planung ist deshalb unverzichtbar.

Sicherungs- oder Wiederherstellungs-Assistent

Das Thema *Datensicherung*, in kleineren Netzwerken oft sträflich vernachlässigt, wird mit einigen neuen Werkzeugen und Funktionen in Windows Server 2003 relativ leicht beherrschbar. Schon mit den Bordmitteln, wie dem bereits aus Windows NT 4 bekannten,



aber grundlegend renovierten Tool *Ntbackup.exe*, können Sie vollautomatisch und zuverlässig Datensicherungen auf Magnetbandgeräte (*Streamer*) oder in Sicherungsdateien anfertigen lassen.

Zwei neue Funktionen haben im Zusammenhang mit einer möglichst 100%igen Datensicherung und einer schnellen Wiederherstellung im Falle eines Serverausfalls eine entscheidende Bedeutung:

- **Volumenschattenkopie:** Anders als unter Windows 2000 Server können jetzt Dateien gesichert werden, die gerade durch ein anderes Programm geöffnet sind. Gesichert wird natürlich nicht die Fassung, die in diesem Moment im Arbeitsspeicher, beispielsweise an einem Clientcomputer, geladen ist. Aber es wird auf die letzte Version zugegriffen, die auf der Festplatte des Servers abgelegt ist. Für das Sicherungsprogramm gibt es also keine Dateien mehr, die nicht gesichert werden können. Das betrifft damit alle Systemdateien.

Die Volumenschattenkopie-Technologie kann darüber hinaus dazu benutzt werden, gezielt Kopien von geänderten Dateien »aufzuheben«. Benutzer sind dann in der Lage, auf frühere Versionen von Dateien zurückzugreifen. Dazu muss der Administrator nicht eingreifen. Ohne diese Technologie bleibt dem Administrator nur der herkömmliche Weg über das Suchen und Zurückspielen der Dateien aus einer Datensicherung.

Am Tag 12 wird die Volumenschattenkopie-Technologie näher vorgestellt.

- **Automatische Systemwiederherstellung:** Diese mit ASR (*Automated System Recovery*) bezeichnete Funktion kann dazu benutzt werden, ein Serversystem im Notfall fast vollautomatisch wiederherstellen zu können. Benötigt wird dazu eine entsprechende Datensicherung, die mit Hilfe der oben beschriebenen Funktion *Volumenschattenkopie* alle Dateien zuverlässig sichern kann. Beim Beginn des Systemstarts kann dann die ASR-Funktion für die Wiederherstellung über einen Druck auf **[F2]** in Gang gesetzt werden.

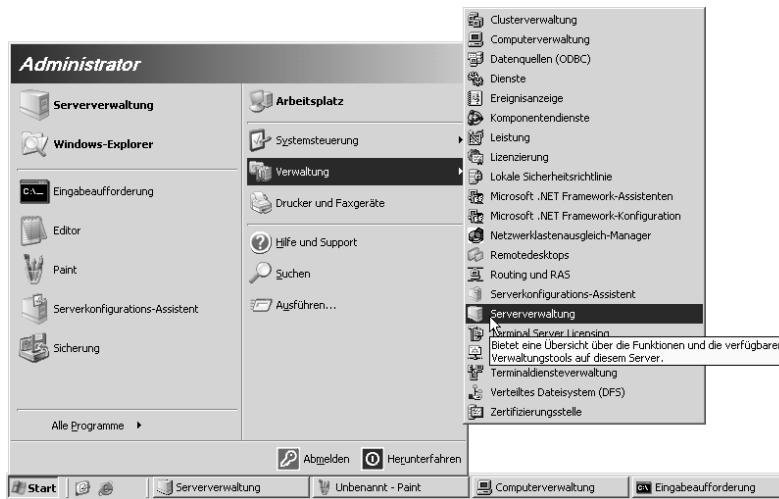
Sowohl die Datensicherung als auch die ASR-Funktionen sind dank ausgefeilter Assistenten relativ leicht beherrschbar. Am Tag 21 werden Sie diese ausführlich kennenlernen.

3.3 Die Microsoft Managementkonsole (MMC)

Nicht für jeden Einrichtungsschritt ist ein Assistent verfügbar oder sinnvoll. Die überwiegende Zahl der grafischen Administrationswerkzeuge sind aber einheitlich strukturiert und damit in ihrer Bedienung schnell beherrschbar, da sie nicht als eigenständige Programme, sondern als Snap-Ins für die Microsoft Managementkonsole vorliegen.

Aufruf der vorkonfigurierten MMCs

Nach dem lokalen Anmelden am Server finden Sie eine Reihe von vorkonfiguriertem Managementkonsolen im Startmenü, wenn Sie auf VERWALTUNG klicken.



*Abbildung 3.8:
Hier sind neben
anderen Pro-
grammen die
vorgefertigten
MMCs zu
finden*

Abhängig von den tatsächlich installierten beziehungsweise aktivierten Funktionen sind hier verschiedene MMCs zu sehen. Die Konsole DNS wird beispielsweise erst dann in das Menü eingebunden, wenn Sie den DNS-Server tatsächlich einrichten.

In den nächsten Abschnitten finden Sie eine Aufstellung der wichtigsten vorkonfigurierten MMCs, die Sie wahrscheinlich am häufigsten für die Administration eines Windows Server 2003 einsetzen werden. Neben den vorkonfigurierten MMCs sind im Bereich VERWALTUNG des Startmenüs Einträge für den Start von verschiedenen Assistenten eingerichtet.

MMCs für die allgemeine Verwaltung

Für die Verwaltung des Serversystems selbst, also seiner Hardware und der sie steuernden Betriebssystemkomponenten, stehen im Wesentlichen diese MMCs zur Verfügung:

■ COMPUTERVERWALTUNG

In dieser MMC ist eine Reihe von Snap-Ins zusammengefasst worden, welche für die tägliche Arbeit des Administrators besonders wichtig sind.



Sie erreichen die MMC COMPUTERVERWALTUNG besonders schnell, wenn Sie im Kontextmenü des ARBEITSPLATZ-Symbols im Startmenü (sekundäre Maustaste klicken) den Punkt VERWALTEN wählen.

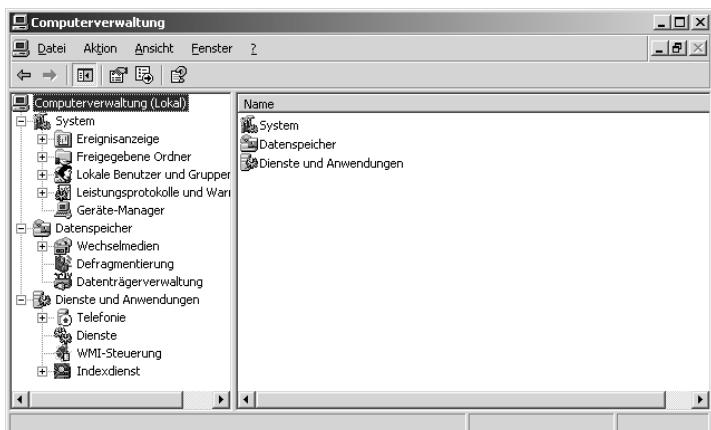


Abbildung 3.9:
Die MMC Computerverwaltung

Im Abschnitt SYSTEM sind dies diese Einträge:

- ▶ EREIGNISANZEIGE: (siehe nachfolgender Abschnitt)
- ▶ FREIGEGBENE ORDNER: Hier verwalten Sie alle Ordner-Freigaben auf diesem Server. Dieses Thema wird am Tag 11 näher behandelt.
- ▶ LOKALE BENUTZER UND GRUPPEN: Damit verwalten Sie die lokal an diesem Server gültigen Benutzer- und Gruppenkonten. Diese sind direkt vergleichbar mit den Konten auf einem Windows 2000 Professional- oder XP Professional-System. Richten Sie den Server als Domänencontroller im Active Directory ein, so werden diese Konten nicht mehr hier verwaltet, sondern in der MMC ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
- ▶ LEISTUNGSPROTOKOLLE UND WARNUNGEN: (siehe nachfolgender Abschnitt)
- ▶ GERÄTE-MANAGER: Hier finden Sie detaillierte Informationen zur eingesetzten Hardware und zum Status der dafür installierten Treiber. In Abschnitt *Geräte-Manager* ab Seite 247 wird dies näher behandelt.

Im Abschnitt DATENSPEICHER sind Snap-Ins für die Verwaltung der Datenträger (Festplatten, Wechseldatenträger etc.) zusammengefasst:

- ▶ WECHSELMEDIEN: Diese Anwendung kann für die Verwaltung von Wechselseiten wie Bändern für Sicherungs-Bandlaufwerke (*Streamer*) eingesetzt werden. Dabei sind Funktionen für die Ansteuerung automatisch arbeitender Bandwechselsysteme integriert.



- ▶ **DEFragmentierung:** Die Festplatten-Datenträger sind neben Prozessorleistung und RAM die wichtigsten Leistungsträger eines Serversystems. Mit diesem Programm können Sie diese einer Defragmentierung unterziehen.
- ▶ **DATENTRÄGERVERWALTUNG:** Das ist das zentrale Administrationstool für die Verwaltung von Datenträgern und logischen Volumes.

Diese und weitere wichtige Werkzeuge für die Datenträgerverwaltung des Windows Server 2003 werden am Tag 5 eingehend unter die Lupe genommen.

Im Bereich DIENSTE UND ANWENDUNGEN sind diese Snap-Ins untergebracht:

- ▶ **TELEFONIE:** Hier sind Snap-Ins für die Einrichtung und Verwaltung von Kommunikationsfunktionen des Servers gemäß TAPI (*Telephony Application Programming Interface*) zu finden. In diesem Buch werden diese Funktionen allerdings nicht behandelt.
- ▶ **WMI-STEUERUNG:** Hier finden Sie einige spezielle Konfigurationsfunktionen für die WMI-Schnittstelle Ihres Serversystems (*Windows Management Instrumentation*). Diese sind für die normale Arbeit des Administrators kaum relevant und werden deshalb ebenfalls nicht weiter behandelt.
- ▶ **INDEXDIENST:** Für das schnellere Auffinden von Informationen können Sie den Indexdienst aktivieren und gezielt einrichten. Dies wird am Tag 17 ausführlich gezeigt.
- **DIENSTE:** Mit diesem Snap-In konfigurieren Sie die Dienste des Serversystems. Am Tag 7 wird dies näher erläutert.

MMCs für die Überwachung des Servers

Da einem Server eine zentrale Rolle im Netzwerk zukommt, ist eine Überwachung der wesentlichen Systemfunktionen besonders wichtig. So können Fehlfunktionen, die vielleicht zu einem baldigen Ausfall führen, frühzeitig erkannt oder gezielte Optimierungs-Maßnahmen bei einer zu geringen Leistung ergriffen werden.

Die folgenden Snap-Ins stehen in vorkonfigurierten Managementkonsolen zur Verfügung:

- **EREIGNISANZEIGE:** Das ist eines der wichtigsten Werkzeuge für den Administrator, da hiermit alle Ereignisse, welche die Systemkomponenten, die Sicherheit und Anwendungen betreffen, protokolliert werden können. In Abschnitt *Die Ereignisanzeige* ab Seite 92 finden Sie dazu ausführliche Informationen.
- **LEISTUNG:** Für eine Analyse des Systemzustandes kommen Systemmonitore zum Einsatz. Damit kann grafisch angezeigt werden, wie einzelne Komponenten belastet sind.



- LEISTUNGSPROTOKOLLE UND WARNUNGEN: Die im Systemmonitor verwendeten Leistungsindikatoren, beispielsweise zur CPU-Last oder zur Auslastung von Datenträgern, können hiermit protokolliert beziehungsweise mit Warnschwellen versehen werden. Damit erhalten Sie ein Instrument, welches Sie rechtzeitig auf bestimmte Zustände hinweisen kann und so hilft, Fehlfunktionen vorzubeugen.

MMCs für die Netzwerk-Verwaltung

Für die umfangreichen Netzwerkfunktionen eines Windows Server 2003-Systems stehen vor allem diese MMCs bzw. Snap-Ins zur Verfügung:

- DHCP: Die Vergabe von IP-Adressen im Netzwerk kann mit Hilfe des *Dynamic Host Configuration Protocol* (DHCP) automatisiert werden. Dadurch wird die Netzwerkverwaltung wesentlich vereinfacht. An den Tagen 8 und 14 werden wir uns diesem Thema umfassend widmen.
- DNS: Grundlage eines Active Directory-Netzwerks ist ein funktionierendes *Domain Name System* (DNS). Im Normalfall wird diese wichtige Funktion ebenfalls der Windows Server 2003 übernehmen. Am Tag 14 wird dieses Thema vertieft.
- ROUTING UND RAS: Mit dieser MMC richten Sie Funktionen zum Verbinden von Netzwerken oder zum Anschluss an das Internet ein. Am Tag 17 wird dieses Thema behandelt.

MMCs für die Verwaltung des Active Directory

Die für die Verwaltung des Active Directory-Verzeichnisdienstes am meisten eingesetzte MMC heißt ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Diese benutzen Sie beispielsweise für das Einrichten von Benutzerkonten und zur Strukturierung des Verzeichnisses mit Organisationseinheiten. Das konkrete Vorgehen dazu ist unter anderem Inhalt am Tag 10.



Die MMC ACTIVE DIRECTORY-BENUTZER UND -COMPUTER steht erst dann am Server zur Verfügung, wenn dieser zu einem Domänencontroller heraufgestuft worden ist. Sie können dieses Snap-In aber auch nachträglich auf einem Mitgliedsserver oder einer Arbeitsstation einsetzen, wenn Sie hier die Server-Verwaltungstools installieren. Dies wird in Abschnitt *Server-Verwaltungsprogramme installieren* ab Seite 89 beschrieben.

An einem Domänencontroller steht das Snap-In LOKALE BENUTZER UND GRUPPEN übrigens nicht mehr zur Verfügung. Der Zugriff auf lokale Benutzerkonten wird damit unterbunden. Eine besondere Rolle spielt nur das lokale Administratorkonto, welches Sie im



Abbildung 3.10:
Die wichtigste
MMC für die
Verwaltung des
Active Directory

Notfall einsetzen, um beispielsweise die Verzeichnis-Datenbank reparieren zu können. Weiterführende Informationen finden Sie zu diesem Thema am letzten Tag.

Diese beiden MMCs stehen für spezielle Verwaltungsaufgaben am Active Directory ebenfalls zur Verfügung:

- ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN
- ACTIVE DIRECTORY-STANDORTE UND -DIENSTE

Diese MMCs werden vor allem für die Verwaltung komplexerer Active Directory-Strukturen benötigt, die aus mehreren Domänen zusammengesetzt sind oder sich über mehrere geografische Standorte erstrecken.



Wenn Sie die Server-Verwaltungstools nachträglich installieren, wie im nachfolgenden Abschnitt gezeigt, finden Sie eine Managementkonsole ACTIVE DIRECTORY-VERWALTUNG, in der diese drei MMCs sowie die MMC DNS zusammengefasst sind.

MMCs für die Sicherheitsrichtlinien

Neben der Steuerung der Zugriffsrechte auf Daten und Programme über die Benutzerkonten und Sicherheits-Gruppenzugehörigkeiten gibt es seit Windows 2000 ein weiteres mächtiges Administrationswerkzeug: Mit den Gruppenrichtlinien, speziell den Sicherheitsrichtlinien, können Sie unter anderem festlegen, welche Einstellungen an bestimmten Systemkomponenten oder dem Windows-Desktop vorgenommen werden sollen. So können Sie beispielsweise im Startmenü den Eintrag AUSFÜHREN ausblenden, wenn Sie verhindern wollen, dass Benutzer eigenmächtig darüber Programme aufrufen.

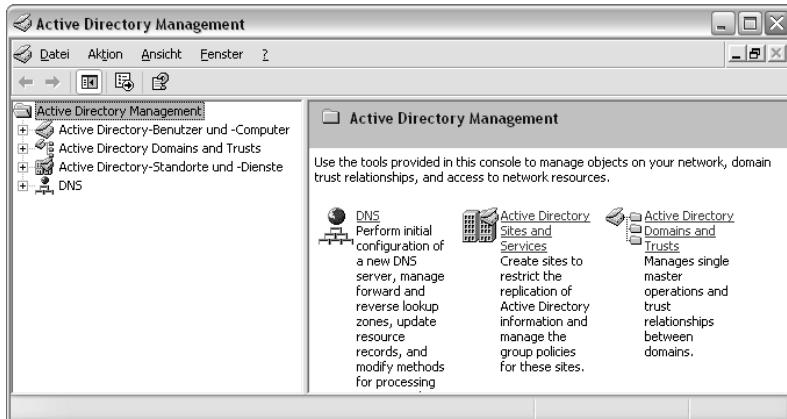


Abbildung 3.11:
Die vorkonfigurierte MMC
Active Directory-Verwaltung

Die folgenden MMCs stehen vorkonfiguriert zur Verfügung:

- **LOKALE SICHERHEITSRICHTLINIE:** Für die lokale Absicherung des Serversystems besitzt dieses Snap-In eine besondere Bedeutung. Wird der Server allerdings in eine Active Directory-Domäne integriert, ob als Mitgliedsserver oder als Domänencontroller, haben die Richtlinien auf Domänenebene stets Vorrang.
- **SICHERHEITSRICHTLINIE FÜR DOMÄENEN:** Betreiben Sie ein Netzwerk mit einer Active Directory-Domäne, können Sie hier die Richtlinien definieren, die global auf Ebene der Domäne gelten sollen. Beachten Sie, dass diese Einstellungen Priorität gegenüber allen lokal festgelegten Richtlinien haben.
- **SICHERHEITSRICHTLINIE FÜR DOMÄNENCONTROLLER:** Speziell der Absicherung von Domänencontrollern dient diese MMC. Da diese eine besondere Bedeutung für den Betrieb des Netzwerks haben, sollten sie auch speziell abgesichert werden.

Dieses Thema wird in Abschnitt *Gruppenrichtlinien* ab Seite 529 vertieft.

Eigene Managementkonsolen anlegen

Sie finden für alle wesentlichen Administrationsaufgaben bereits vorkonfigurierte Managementkonsolen vor. Sie können aber ebenso Ihre bevorzugten Snap-Ins in einer eigenen Managementkonsole arrangieren und sich damit Ihre Werkzeuge individuell zusammenstellen. Zusätzlich lassen sich sogar grafische Symbole zur Vereinfachung der Benutzung in so genannten *Taskpadansichten* anlegen.



Der grundlegende Aufbau einer MMC

Die Managementkonsolen-Anwendung ist so gestaltet, dass die Bedienung der Snap-Ins einem einheitlichen Schema folgt. Die wichtigsten Elemente werden in der nachfolgenden Abbildung gezeigt.

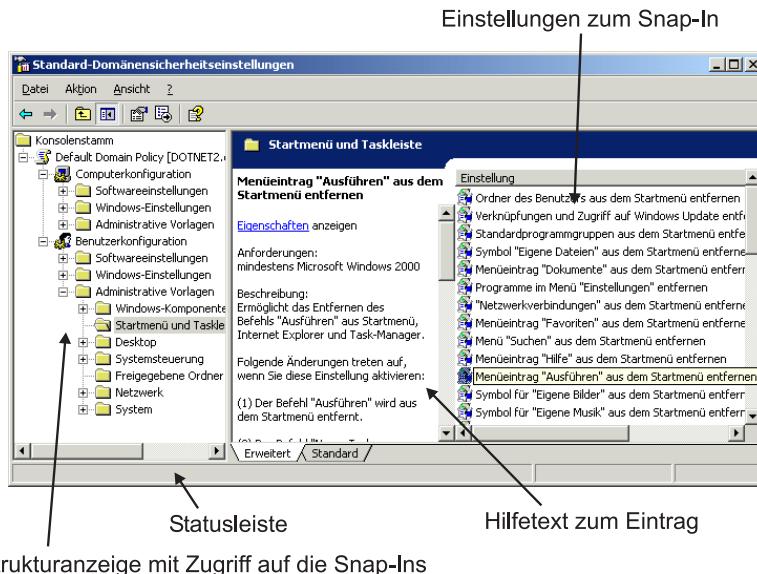


Abbildung 3.12:
Wesentliche
Komponenten
einer Manage-
mentkonsole

Die Strukturanzige können Sie über einen Klick auf das entsprechende Symbol in der Symbolleiste ein- und ausschalten. Die Registerkarte ERWEITERT, über die Sie Hilfetexte zu Einträgen erhalten, ist nur bei bestimmten Snap-Ins verfügbar.

Snap-Ins in eine eigene MMC einbinden

Gehen Sie wie folgt vor, wenn Sie eine eigene Managementkonsole erstellen wollen:

1. Starten Sie eine leere Managementkonsole, indem Sie im Startmenü auf AUSFÜHREN klicken und im dann folgenden Dialogfenster »mmc« eingeben.
2. Über den Punkt SNAP-IN HINZUFÜGEN/ENTFERNNEN des DATEI-Menüs oder über **Strg**+**M** können Sie Snap-Ins einfügen. Die Auswahl treffen Sie aus der Liste der angebotenen Snap-Ins.
3. Wählen Sie das gewünschte Snap-In aus und klicken Sie dann auf die Schaltflächen HINZUFÜGEN. Die meisten Snap-Ins lassen beim Einbinden die Auswahl zu, ob sie für das lokale oder ein entferntes System eingesetzt werden sollen.



Administrationswerkzeuge

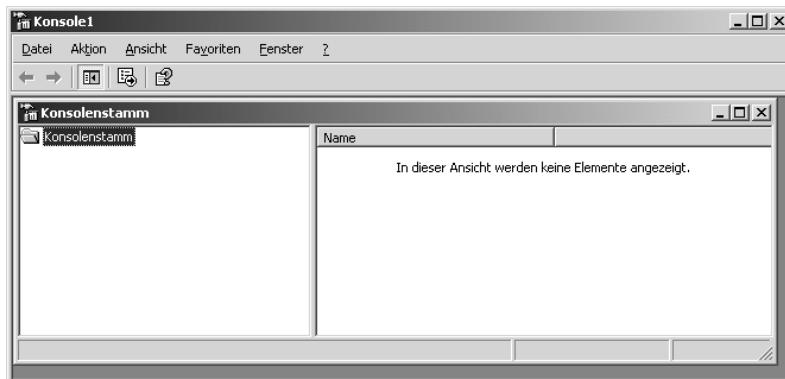


Abbildung 3.13:
Eine leere
Management-
konsole

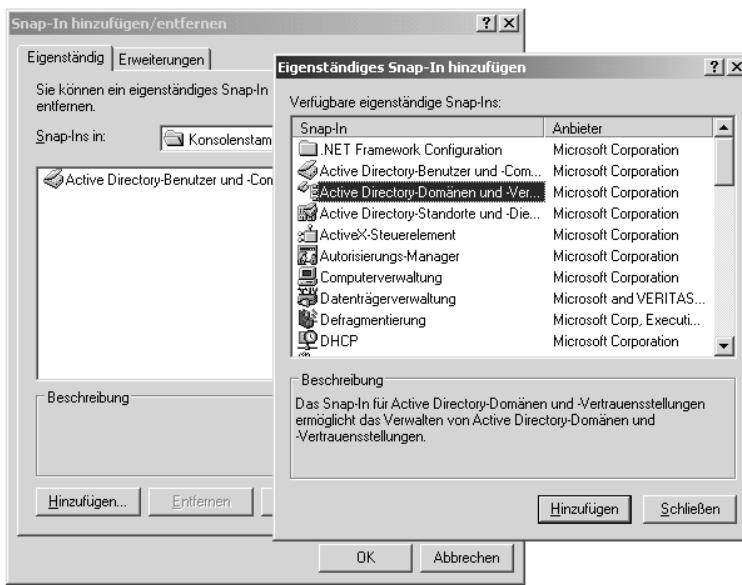


Abbildung 3.14:
Snap-Ins in die
Management-
konsole hinzufü-
gen

4. Soll das Snap-In ein entferntes System verwalten, geben Sie hier den Namen oder die IP-Adresse des betreffenden Systems ein. Weiterführende Informationen finden Sie zu diesem Thema in Abschnitt *Server-MMCs auf einer Arbeitsstation einsetzen* ab Seite 89.

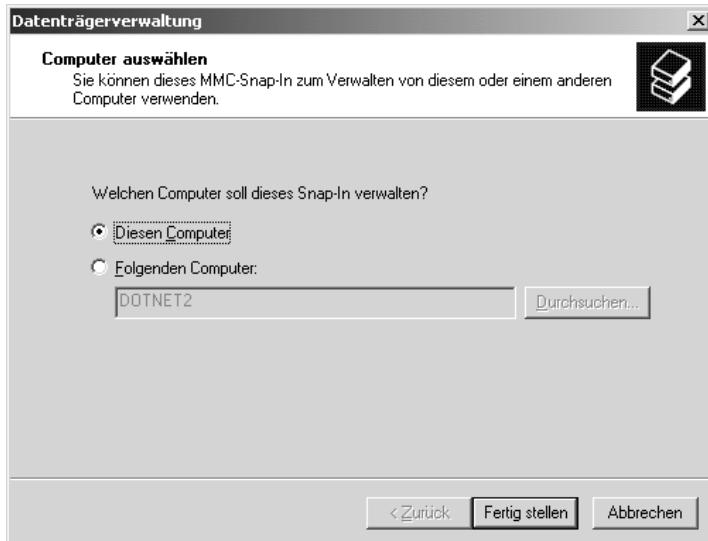


Abbildung 3.15:
Auswahl, ob das Snap-In
das lokale oder ein ent-
ferntes System verwalten
soll

Erweiterungen zu Snap-Ins

Einige Snap-Ins bestehen aus mehreren Komponenten, die Sie gezielt aktivieren oder deaktivieren können. Ein Beispiel dafür ist das Snap-In *Computerverwaltung*, in welchem mehrere eigenständige Snap-Ins zusammengefasst sind. Über die Registerkarte ERWEITERUNGEN des Dialogfensters SNAP-IN HINZUFÜGEN/ENTFERNEN lassen sich diese Snap-Ins ein- und ausschalten.

Wollen Sie beispielsweise aus der *Computerverwaltung* das Snap-In *Defragmentierung* entfernen, deaktivieren Sie zuerst ALLE ERWEITERUNGEN HINZUFÜGEN und danach den Eintrag *DEFRAMENTIERUNG*.

Das macht im Beispiel des Snap-Ins *Computerverwaltung* dann Sinn, wenn Sie damit von einer Arbeitsstation aus den Server administrieren wollen. Die standardmäßig beigelegte Defragmentierungslösung kann nämlich als einzige Komponente dieses Snap-Ins nicht für die Fernadministration eingesetzt werden. Dazu müssten Sie sich erst die Vollversion dieser Software beschaffen.

Modi von Managementkonsolen

Vor dem Abspeichern einer Managementkonsole können Sie noch einen so genannten *Konsolenmodus* einstellen. Standardmäßig können selbst erzeugte MMCs von allen Benutzern geändert werden. Snap-Ins lassen sich damit entfernen, hinzufügen oder hinsichtlich ihrer Erweiterungen anpassen.

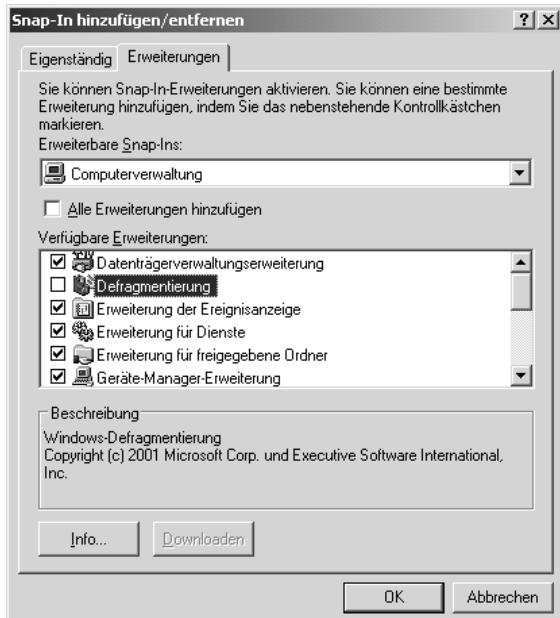


Abbildung 3.16:
Erweiterungen eines Snap-Ins
gezielt auswählen

Über die Auswahl eines passenden Konsolenmodus können Sie dies wirkungsvoll verhindern. Öffnen Sie dazu das Dialogfenster OPTIONEN über das DATEI-Menü.

In diesem Dialogfenster können Sie neben dem Konsolenmodus eine passende Bezeichnung und ein alternatives Symbol festlegen. Ein anderes Symbol erhalten Sie übrigens, indem Sie über die entsprechende Schaltfläche eine beliebige Windows-Anwendung anwählen.

Die folgenden Konsolenmodi stehen zur Verfügung:

- **AUTORENMODUS:** Das ist der Standardmodus. Die MMC kann nachträglich jederzeit geändert werden. Das betrifft sowohl die eingebundenen Snap-Ins, die gelöscht oder um weitere ergänzt werden können, als auch das optische Erscheinungsbild.
- **BENUTZERMODUS – VOLLZUGRIFF, MEHRERE FENSTER:** Die eingebundenen Snap-Ins können nicht mehr modifiziert werden. Der Benutzer hat aber freie Wahl, was das optische Erscheinungsbild der Konsole betrifft. Er kann beliebig Fensteransichten starten und sich frei zwischen allen eingebundenen Snap-Ins bewegen.
- **BENUTZERMODUS – BESCHRÄNKTER ZUGRIFF, MEHRERE FENSTER:** Mit diesem Modus können Sie die Sicht gezielt auf ein einziges oder mehrere ausgewählte Snap-Ins beschränken. Schließen Sie vor dem Speichern alle anderen Fenster von Snap-Ins, die der Benutzer nicht sehen soll. Wenn er diese MMC dann öffnet, kann er nur noch weitere Fenster für bereits bestehende Sichten öffnen.



Abbildung 3.17:
Optionen für die erstellte MMC anpassen

- **BENUTZERMODUS – BESCHRÄNKTER ZUGRIFF, EINZELFENSTER:** Sie beschränken so die Managementkonsole auf genau eine Sicht, die der Benutzer nicht verändern kann. Dieser Modus empfiehlt sich dann, wenn Sie die MMC auf eine ganz bestimmte Administrationsaufgabe festlegen wollen. Es ist nur das Fenster verfügbar, welches beim Abspeichern aktiv gewesen ist. Der Benutzer kann keine weiteren Fenster öffnen. Dieser Modus ist zu empfehlen, wenn Sie eine MMC grafisch mit Taskpad-Ansichten gestalten und sichergehen wollen, dass der Benutzer die Konsole nur über diese Sichten bedient.

Zusätzlich lassen sich für die drei Benutzermodi zwei weitere Optionen festlegen, welche Änderungen und Anpassungen von Ansichten für eine Konsole betreffen:

- **ÄNDERUNGEN FÜR DIESE KONSOLE NICHT SPEICHERN:** Wollen Sie sichergehen, dass die Konsole bei jedem neuen Aufruf immer gleich aussieht, aktivieren Sie dieses Kontrollkästchen. Änderungen, die ein Benutzer vorgenommen hat, werden damit nicht mit abgespeichert.
- **ANPASSEN VON ANSICHTEN DURCH BENUTZER ZULASSEN:** Deaktivieren Sie dieses Kontrollkästchen, und aus dem Menü ANSICHT wird der Punkt ANPASSEN entfernt. Damit werden Elemente wie Statusleiste oder Symbolleisten zu den Snap-Ins genau festgelegt und können nicht mehr verändert werden.



Eine Managementkonsole können Sie jederzeit wieder im Autorenmodus öffnen, um Änderungen an ihr vorzunehmen. Klicken Sie dazu im Windows-Explorer auf die Konsole über die rechte Maustaste und wählen Sie aus dem Kontextmenü **IM AUTORENMODUS ÖFFNEN**. Alternativ können Sie die Konsole über die Kommandozeile starten, indem Sie die Option **/A** mit übergeben:
`mmc MeineKonsole.msc /A`

Speicherung von Managementkonsolen-Dateien

Eine fertig erstellte Managementkonsole könnte zunächst wie folgt aussehen:



Abbildung 3.18:
Eine individuell erstellte MMC

Sie können diese Managementkonsole dann über **DATEI/SPEICHERN** oder **Strg + S** an einem beliebigen Ort ablegen. Damit Sie sie im Startmenü am Server unter **VERWALTUNG** wiederfinden, sollten Sie im Benutzerprofil hier abgelegt werden: **STARTMENÜ / PROGRAMME / VERWALTUNG**.

Die Dateiendung von Managementkonsolen ist **.msc**. Die erzeugten Dateien sind sehr klein, da sie lediglich Verweise auf die enthaltenen Komponenten wie Snap-Ins oder Acti-veX-Controls enthalten. Damit eignen sie sich sehr gut, um beispielsweise über E-Mail weitergegeben zu werden. Allerdings sollten Sie beachten, dass auf dem System, auf welchem sie ausgeführt werden sollen, die betreffenden Komponenten installiert sein müssen. Zur Installation der Snap-Ins für einen Windows Server 2003 auf einer Arbeitsstation finden Sie weitere Informationen in Abschnitt *Server-Verwaltungsprogramme installieren* ab Seite 89.



Server-MMCs auf einer Arbeitsstation einsetzen

Die Technologie der Managementkonsolen und ihrer Snap-Ins ist entwickelt worden, um dem Administrator die Arbeit zu erleichtern. Dazu gehören die ausgefeilten Möglichkeiten zur Fernadministration. Die meisten mitgelieferten Snap-Ins sind so programmiert, dass sie für entfernte Systeme ausgeführt werden können. Das kann ein Windows Server 2003 oder eine andere Windows-Arbeitsstation sein. Eine volle Unterstützung der Managementkonsole und ihrer Technologien wird ab Windows 2000 geboten. Windows NT 4-Systeme lassen dies nur mit Einschränkungen zu.

Nachfolgend finden Sie die notwendigen Informationen, wie Sie eine Arbeitsstation unter Windows 2000 Professional oder Windows XP Professional so einrichten, dass Sie alle wichtigen Administrationswerkzeuge für den Windows Server 2003 von hier aus verwenden können. Damit sparen Sie sich für die meisten Arbeiten den Gang zum Serversystem selbst.



Eine andere Alternative für die Fernadministration besteht darin, die Terminaldienste von Windows Server 2003 zu nutzen. Dieses Thema wird am Tag 4 eingehend behandelt.

Server-Verwaltungsprogramme installieren

Bevor Sie die Server-Managementkonsolen auf Ihrer Arbeitsstation aufrufen können, müssen Sie bestimmte vorkonfigurierte Managementkonsolen und Snap-Ins nachinstallieren. Die MMC *Active Directory-Benutzer und -Computer* beispielsweise steht standardmäßig unter Windows 2000/XP Professional nicht zur Verfügung. Alle zur Verwaltung eines Windows Server 2003 notwendigen MMCs und Snap-Ins und damit die zur Verwaltung von Active Directory-Domänen finden Sie als installierbares MSI-Paket (*Microsoft Installer*) auf der Installations-CD.

Gehen Sie wie folgt vor, um dieses Paket zu installieren:

1. Legen Sie die Installations-CD zum Windows Server 2003 ein und öffnen Sie hier über den Windows-Explorer das Verzeichnis `\i386`.
2. Doppelklicken Sie auf das Windows Installer-Paket `Adminpak.msi`. Nach Bestätigung eines Hinweisfensters beginnt sofort die Installation.

Leider erlaubt dieses Installationsprinzip kein Selektieren einzelner Komponenten. Es werden grundsätzlich »in einem Rutsch« sämtliche MMCs mit den neuen Snap-Ins auf dem Zielsystem installiert und eingerichtet – ob Sie das wollen oder nicht.

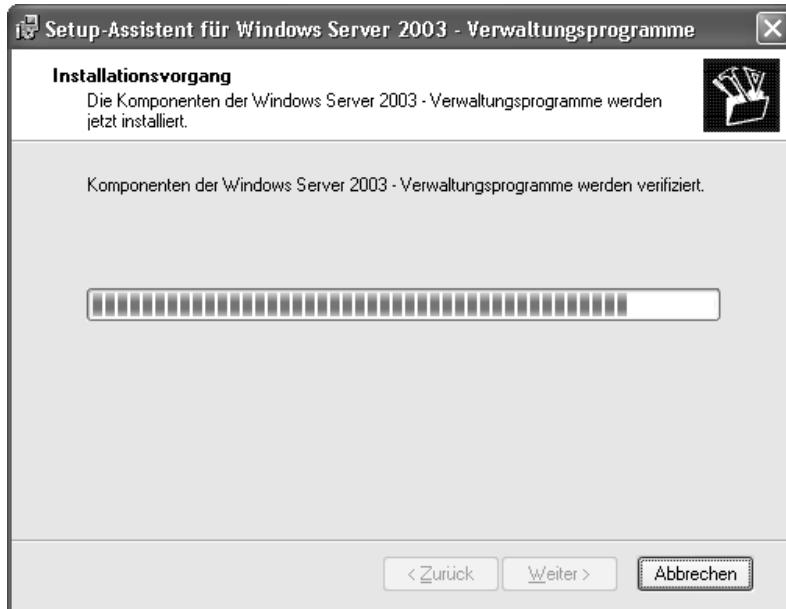


Abbildung 3.19:
Die Verwal-
tungspro-
gramme werden
auf einer Win-
dows XP-Arbeits-
station
installiert

Zur Deinstallation der Verwaltungsprogramme öffnen Sie die SYSTEMSTEUERUNG und wählen Sie das Applet SOFTWARE. Hier finden Sie in der Liste der installierten Programme einen Eintrag WINDOWS SERVER 2003 – VERWALTUNGSPROGRAMME. Markieren Sie diesen und klicken Sie dann auf ENTFERNEN.

Snap-Ins für entfernte Systeme anwenden

So können Sie ein Managementkonsolen-Snap-In mit einem entfernten System verbinden:

1. Markieren Sie in einer gestarteten Managementkonsole das betreffende Snap-In und wählen Sie den Menüpunkt AKTION/VERBINDUNG ZU ANDEREM COMPUTER HERSTELLEN. Sie finden diesen Punkt im Kontextmenü zum Snap-In (rechte Maustaste).
2. Geben Sie im dann erscheinenden Dialogfenster den Namen oder die IP-Adresse des entfernten Systems an.

Wenn die Verbindung hergestellt werden konnte, können Sie die Funktionen des Snap-Ins genauso benutzen, als würden Sie lokal am Server arbeiten.

Damit Sie nicht erst nachträglich eine Verbindung zum Server herstellen müssen, können Sie beim Anlegen einer eigenen Managementkonsole die Snap-Ins gleich mit einem entfernten System »fest« verbinden. Dies wurde bereits in Abschnitt *Snap-Ins in eine eigene MMC einbinden* ab Seite 83 gezeigt.

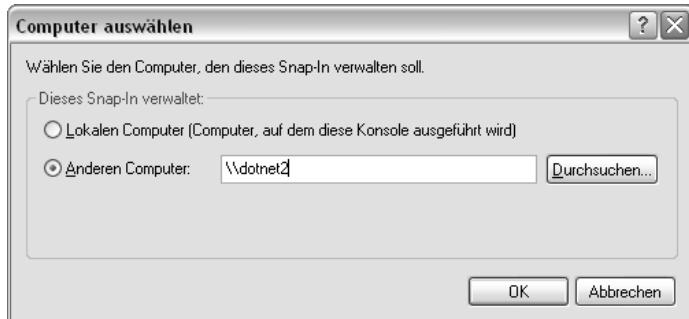


Abbildung 3.20:
Verbindung eines Snap-Ins
zu einem entfernten
System herstellen

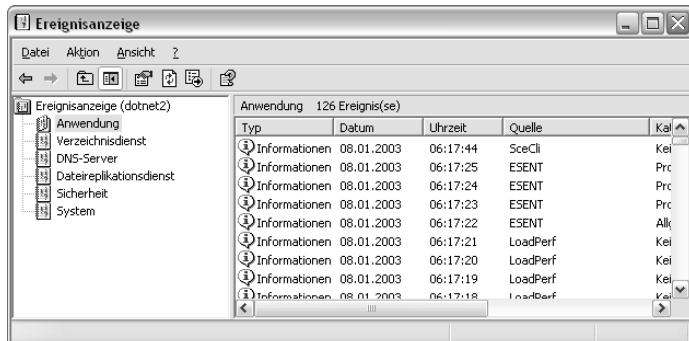


Abbildung 3.21:
Die Managementkonsole
Ereignisanzeige für einen
Windows Server 2003
unter Windows XP
Professional

 Damit Sie vollen Zugriff mit den Snap-Ins auf den Server erhalten, müssen Sie die zugehörige Managementkonsole mit den entsprechenden Administratorrechten ausführen. Dies wird im nachfolgenden Abschnitt näher erläutert.

MMCs mit Administratorrechten ausführen

Um alle Funktionen eines Snap-Ins für ein Serversystem nutzen zu können, müssen Sie dieses als Benutzer mit Administratorrechten aufrufen. Wenn Sie an einer Windows 2000 Professional- oder Windows XP Professional-Arbeitsstation nicht als Administrator angemeldet sind, können Sie dies über den Aufruf der Managementkonsole unter einer anderen Benutzerkennung erreichen, ohne dass Sie sich erst umständlich ab- und wieder anmelden müssen. Sie haben dazu diese beiden Möglichkeiten:

- Klicken Sie im Startmenü unter ALLE PROGRAMME/VERWALTUNG auf den entsprechenden Eintrag für die Managementkonsole mit der alternativen Maustaste und halten Sie dabei die **Shift**-Taste gedrückt. Wählen Sie im dann erscheinenden Kontextmenü den Eintrag AUSFÜHREN ALS. Sie können hier als Benutzer den Administrator mit seinem Kennwort angeben und starten so die Managementkonsole mit dessen Rechten.



- Wenn Sie die Managementkonsole von der Kommandozeile aus starten wollen, können Sie das Dienstprogramm *Runas.exe* verwenden, um es in einem anderen Benutzerkontext laufen zu lassen. Ein Aufruf der Managementkonsole *Ereignisanzeige* könnte beispielsweise so aussehen:

```
Runas /user:Administrator "mmc.exe %SystemRoot%\system32\eventvwr.msc /s"
```



Verschiedene Verwaltungswerkzeuge für das Active Directory funktionieren erst dann von einer Arbeitsstation aus, wenn diese selbst in das Verzeichnis eingebunden ist. Zusätzlich ist es notwendig, dass Sie sich als Domänen-Benutzer mit entsprechenden Administratorrechten angemeldet haben.

3.4 Die Ereignisanzeige

Die Managementkonsole *Ereignisanzeige* ist eines der wichtigsten Administrationswerkzeuge. Wenn Sie Fehlfunktionen oder Störungen am Server vermuten, sollten Sie zuerst einen Blick in eines der hier geführten Protokolle werfen. Sie finden die Ereignisanzeige im Startmenü am Server unter PROGRAMME/VERWALTUNG sowie als Teil der Managementkonsole COMPUTERVERWALTUNG, die Sie über das Kontextmenü zum Symbol ARBEITSPLATZ starten können. Wie bereits beschrieben, können Sie das Snap-In *Ereignisanzeige* auch in eine eigene Managementkonsole einbinden.

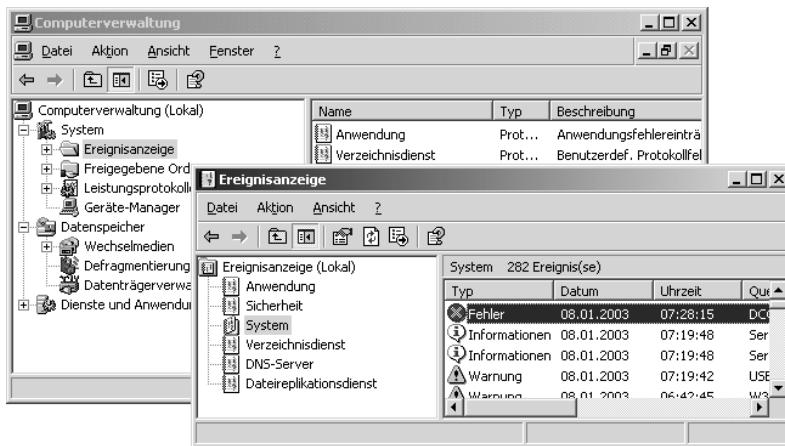


Abbildung 3.22:
Das Snap-In
Ereignisanzeige
in einer eigenen
MMC sowie als
Teil der Computerverwaltung

Das von Windows NT bekannte Programm *Eventvwr.exe* können Sie unter Windows Server 2003 ebenfalls aufrufen. Allerdings wird damit die Managementkonsole *Ereignisanzeige* gestartet.



Mit Hilfe des Kommandozeilen-Tools *Eventcreate.exe* können Sie unter Windows Server 2003 sehr einfach eigene Ereignismeldungen erzeugen. Meldungen, die Sie aus Kommandozeilenprogrammen, eigenen Skripts oder zeit- bzw. ereignisgesteuert vorher vielleicht in eine Textdatei (»Logdatei«) geschrieben haben, sind nun in die zentralen Ereignisprotokolle integrierbar. In Abschnitt *Eigene Ereignismeldungen erzeugen* ab Seite 100 finden Sie dazu weiterführende Informationen.

Nicht minder interessant sind zwei weitere neue Tools:

- *Eventtriggers.exe*: Mit diesem Programm können Sie auf bestimmte Ereignisse reagieren wie beispielsweise das Knappwerden von Speicherplatz auf einem Laufwerk. Tritt dieses Ereignis ein, können Sie ein beliebiges Programm oder Skript zur weiteren Behandlung starten.
- *Eventquery.vbs*: Dieses Skript eignet sich, Ereignismeldungen aus einem oder mehreren Protokollen herauszufiltern und zur Anzeige oder zur Speicherung in eine Datei zu bringen.

Die einzelnen Protokolle

Die Ereignisanzeige umfasst bei einem Windows Server 2003 meist diese sechs Protokolle, die nachfolgend näher vorgestellt werden.

Anwendungsprotokoll

Im Anwendungsprotokoll erscheinen Meldungen von Anwendungsprogrammen. Allerdings finden Sie hier bereits Einträge, wenn auf Ihrem Serversystem zusätzlich zum Betriebssystem noch gar keine weiteren Programme installiert sind. Diese Einträge werden also auch von diversen Systemkomponenten generiert. Allein der Programmierer entscheidet, ob eine Meldung seines Programms im System- oder im Anwendungsprotokoll erscheinen soll.

Sicherheitsprotokoll

Dieses Protokoll hat für ein Serversystem eine besondere Bedeutung. Unter Windows 2000 Server müssen erst bestimmte Einstellungen an den Sicherheitsrichtlinien vorgenommen werden, damit das Protokoll geführt wird. Mit Windows Server 2003 ist dies nun anders. Standardmäßig sind hier die wichtigsten Überwachungsfunktionen aktiviert.



Für einen Domänencontroller konfigurieren Sie diese über die Managementkonsole *Sicherheitsrichtlinie für Domänencontroller*, welche Sie am Server direkt über das START-MENÜ/ALLE PROGRAMME/VERWALTUNG aufrufen können.

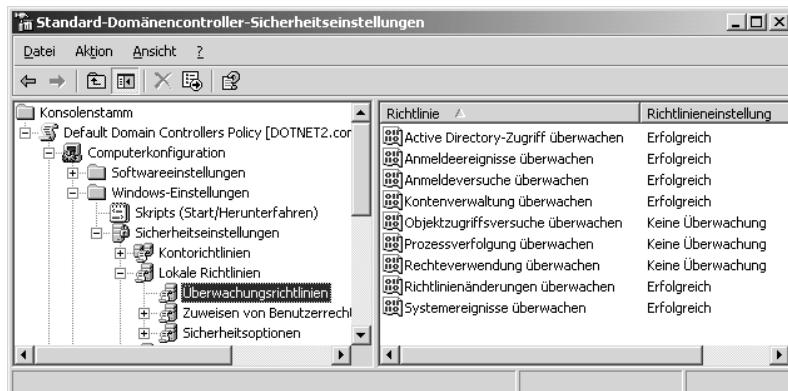


Abbildung 3.23:
Die Standard-Überwachungs-einstellungen für einen Domänencontroller

Ist der Server kein Domänencontroller, finden Sie die zugehörigen Einstellungen in der Managementkonsole *Lokale Sicherheitsrichtlinie*. Hier werden standardmäßig nur Anmeldeereignisse überwacht.

Systemprotokoll

Im Systemprotokoll werden Meldungen von systemnahen Prozessen aufgezeichnet. Dies sind beispielsweise Einträge zu Gerätetreibern. Hier finden Sie Meldungen zu Starts oder zum Herunterfahren des Servers (Quelle: *eventlog*).

Verzeichnisdienst-Protokoll

Ist der Server ein Domänencontroller, so finden Sie hier Meldungen, die den Verzeichnisdienst Active Directory betreffen. Umfassend wird dieses Thema an den Tagen 10 und 11 behandelt.

DNS-Server-Protokoll

Wird auf dem Server der DNS-Serverdienst betrieben, wie dies bei einer Standard-Installation eines alleinstehenden Domänencontrollers der Fall ist, so werden die entsprechenden Meldungen hier aufgezeichnet.



Dateireplikationsdienst-Protokoll

In diesem Protokoll werden die Meldungen des Dateireplikationsdienstes erfasst. Dieser Dienst ist für den Betrieb des Verzeichnisdienstes Active Directory erforderlich. Er wird aber auch für andere Funktionen, wie beispielsweise für die Replikation von Daten im *Verteilten Dateisystem*, eingesetzt.

Ereignismeldungen im Detail

In diesem Abschnitt werden die Ereignismeldungen selbst unter die Lupe genommen. Damit lernen Sie, wie Sie die hier angezeigten Informationen richtig deuten. Über einen Doppelklick öffnet sich ein Detailfenster zur betreffenden Ereignismeldung.

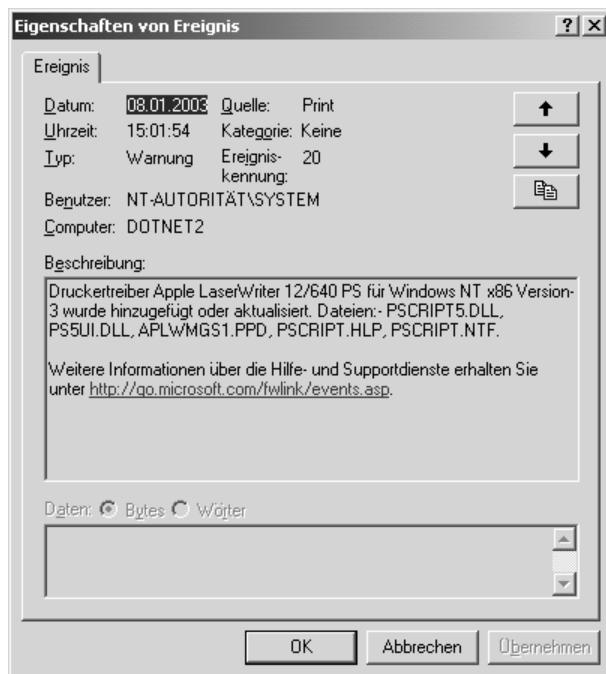


Abbildung 3.24:
Eigenschaften-Fenster einer Ereignismeldung; hier zur Installation eines neuen Druckers

Über die beiden Pfeil-Schaltflächen können Sie sich im Protokoll auf- und abwärts bewegen. Darunter befindet sich eine Schaltfläche, über die Sie den Inhalt des gesamten Fensters als Text in die Zwischenablage kopieren können. So können Sie eine Meldung schnell in ein Textdokument oder eine E-Mail übertragen, um sie beispielsweise an einen Kollegen weiterzuleiten.



Weitergehende Informationen von Microsoft erhalten

Seit Windows XP wird in Ereignismeldungen im Feld **BESCHREIBUNG** ein zusätzlicher Link angezeigt, über den Sie weiterführende Informationen zu dieser Meldung bei Microsoft abrufen können. Allerdings sind die angefragten Informationen derzeit (Anfang 2003) nach wie vor entweder nicht verfügbar oder sagen nicht mehr aus als das, was Sie ohnehin in der Beschreibung vorfinden.

Typen von Ereignissen

Die Meldungen im Ereignisprotokoll werden hinsichtlich ihrer Bedeutung nach verschiedenen Typen unterteilt. Diese reichen von einfachen *Informationen* bis hin zu *Fehlern*, die unter Umständen Ihrer besonderen Aufmerksamkeit bedürfen. Die Bedeutungen der einzelnen Typen werden nachfolgend kurz erläutert:

- **Informationen:** Die meisten Einträge, die einen ordnungsgemäßen Verlauf oder Abschluss eines Prozesses kennzeichnen sollen, werden mit diesem Typ gekennzeichnet.
- **Warnungen:** Damit werden Meldungen herausgehoben, um auf besondere Ereignisse aufmerksam zu machen. Diese müssen nicht immer einen kritischen Status haben. So wird die korrekte Installation eines neuen Druckers am Server ebenfalls von einer Warnmeldung begleitet.
- **Fehler:** Einträge mit diesem Typ weisen meist auf ernst zu nehmende Probleme am Serversystems hin. Finden Sie hier beispielsweise Fehlermeldungen, die wichtige Gerätetreiber wie die für das Festplatten-Interface betreffen, sollten Sie schnellstmöglich die Ursache für den Fehler finden.
- **Erfolgsüberwachung:** Diesen Typ werden Sie im Sicherheitsprotokoll finden. Er weist Sie auf einen Vorgang (Spalte: **KATEGORIE**) hin, der überwacht wird und erfolgreich abgeschlossen worden ist. Das kann beispielsweise ein Anmeldevorgang sein. Mit dessen Aufzeichnung im Protokoll können Sie erreichen, dass Sie genau nachvollziehen können, wer sich wann am System zuletzt angemeldet hat.
- **Fehlerüberwachung:** Im Gegensatz zum zuvor erläuterten Typ werden damit Ereignisse gekennzeichnet, die fehlgeschlagen sind. So können im Falle der Überwachung von Anmeldevorgängen Einbruchsversuche ermittelt werden, bei denen versucht wird, das Kennwort zu erraten.



Bedeutungen weiterer Felder in der Meldung

- **Quelle:** Hier werden die Anwendung oder der Prozess angezeigt, durch welche die betreffende Meldung ausgelöst worden ist.
- **Kategorie:** Verschiedene Meldungen verfügen über einen Eintrag in diesem Feld, durch den sie weiter eingeordnet werden können.
- **Ereigniskennung:** Jeder Ereignismeldung liegt eine Fehlernummer zugrunde, die hier angezeigt wird. Diese kann helfen, um beispielsweise in der Knowledge Base bei Microsoft nach weiteren Informationen zu einer Meldung zu fahnden. Dabei hilft die Kennung weiter, um in der weit umfangreicherer englischsprachigen Datenbasis fündig zu werden. Teile des deutschen Beschreibungstextes sind dort als Suchbegriffe nicht anwendbar.
- **Benutzer:** In diesem Feld wird, wenn diese Information vorliegt, das Benutzerkonto angezeigt, welches mit dem Auslösen des Ereignisses in Zusammenhang steht. Dabei müssen Sie allerdings beachten, dass dies nur die Konten betrifft, die direkt mit dem auslösenden Prozess oder der Anwendung zu tun haben.
- **Computer:** In diesem Feld wird der Name des Computers angegeben, auf dem dieses Ereignis ausgelöst worden ist.

Ereignisse sortieren und filtern

Eine umfangreiche Liste von Ereignismeldungen kann schnell sehr unübersichtlich werden. Deshalb haben Sie verschiedene Möglichkeiten, die Liste zu sortieren oder nur bestimmte Meldungen herauszufiltern. Sie können nach einer bestimmten Spalte wie im Windows Explorer gewohnt sortieren, indem Sie auf den Spaltenkopf klicken.

Zum Filtern von Meldungen gehen Sie über das Menü ANSICHT/FILTERN. Sie müssen dabei das betreffende Protokoll angeklickt haben. Sie erhalten dann das EIGENSCHAFTEN-Dialogfenster zu diesem Protokoll mit dem Fokus auf der Registerkarte FILTER.

Hier können Sie den EREIGNISTYP festlegen, der angezeigt werden soll. Wollen Sie nach ganz bestimmten Ereignissen suchen, können Sie die Anzeige weiter einschränken, indem Sie zuerst die EREIGNISQUELLE und dann gegebenenfalls noch eine KATEGORIE dazu auswählen.

Über die Schaltfläche WIEDERHERSTELLEN machen Sie alle gesetzten Filtereinstellungen mit einem Mausklick wieder rückgängig.

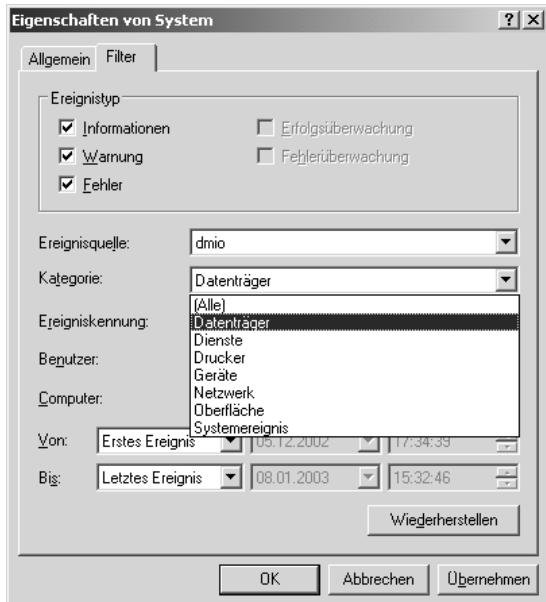


Abbildung 3.25:
Filtereinstellungen für ein Protokoll
(hier: System) festlegen

Die Protokollierung konfigurieren

Die standardmäßigen Voreinstellungen zur Protokollierung wie maximale Protokollgrößen oder deren Speicherorte sind für viele Anwendungsfälle sicherlich ausreichend. Trotzdem kann es nicht schaden zu wissen, wie sich wichtige Parameter im Bedarfsfall ändern lassen.

Eigenschaften eines Protokolls

Das Eigenschaften-Dialogfenster zu einem Protokoll erhalten Sie, indem Sie das Kontextmenü zu diesem Protokoll aufrufen (rechte Maustaste) und dort den Eintrag EIGENSCHAFTEN wählen.

Die MAXIMALE PROTOKOLLGRÖSSE können Sie in 64-Kbyte-Schritten einstellen. Der Voregewert ist in der Regel ausreichend. Wird die maximale Größe erreicht, können Sie das Systemverhalten mit den folgenden drei Optionen bestimmen:

- **EREIGNISSE NACH BEDARF ÜBERSCHREIBEN:** Damit werden die ältesten Ereignisse soweit gelöscht, wie Platz für neue Einträge benötigt wird. Dies ist die Standardeinstellung und dann zu empfehlen, wenn es nicht erforderlich ist, dass garantiert alle Meldungen erhalten bleiben müssen. Im Notfall kann es allerdings dazu kommen, dass eine Anwendung oder ein Prozess durch eine Fehlfunktion so viele Meldungen generieren, dass nach einer kurzen Zeit das gesamte Protokoll nur noch aus diesen besteht.

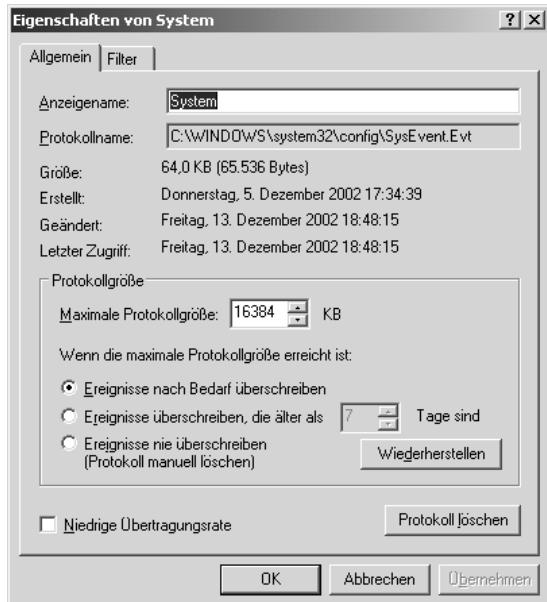


Abbildung 3.26:
Eigenschaften-Dialogfenster
eines Protokolls

- EREIGNISSE ÜBERSCHREIBEN, DIE ÄLTER ALS ... TAGE SIND: Hier können Sie genauer eingrenzen, wie alt die Ereignisse mindestens sein müssen, bevor sie überschrieben werden dürfen. Damit stellen Sie sicher, immer einen definierten Zeitraum im Überblick zu haben. Allerdings kann es dazu kommen, dass das Protokoll voll läuft.
- EREIGNISSE NIE ÜBERSCHREIBEN: Wollen Sie sicherstellen, dass garantiert alle Meldungen erhalten bleiben, müssen Sie diese Option wählen. Allerdings sollten Sie dann Maßnahmen treffen, die ein Volllaufen des Protokolls zuverlässig verhindern.



Sie sollten die Größe der einzelnen Protokolle und das Verhalten des Systems bei Erreichen des Maximalwertes so festlegen, dass eine Protokollierung immer zuverlässig gewährleistet ist. Wenn Sie das nicht beachten, legen Sie Ihr Server-System zuverlässig lahm, wenn beispielsweise das Systemprotokoll keine weiteren Einträge mehr aufnehmen kann.

Speicherorte der Protokolle ändern

Wenn Sie den Speicherort für ein Ereignisprotokoll verändern wollen, bleibt Ihnen ein Eingriff in die Windows-Registrierung nicht erspart. Es kann im Einzelfall sinnvoll sein, die Protokolldateien auf einer separaten Partition oder einem speziellen Netzwerk-Laufwerk abzulegen.



Zum Ändern starten Sie am Server den Registrierungseditor (siehe dazu Abschnitt *Windows-Registrierungseditor* ab Seite 726). In der Registrierung finden Sie die betreffenden Einträge unterhalb von diesem Schlüssel:

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog

Hier sind die Einstellungen zu den einzelnen Protokollen in eigenen Schlüsseln untergebracht.

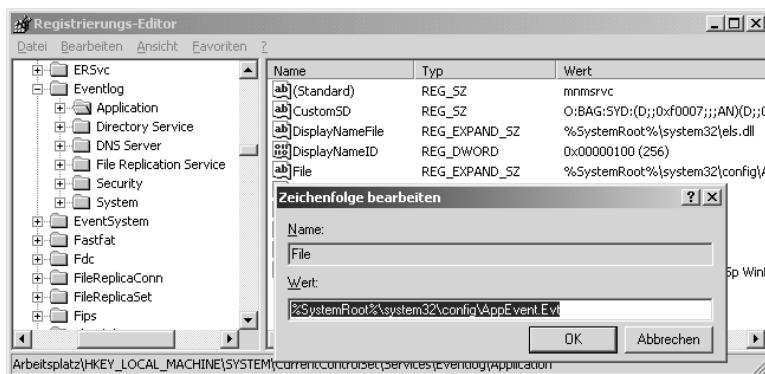


Abbildung 3.27:
Bearbeitung des
Speicherorts für
ein Protokoll

Im Wert FILE ist der Speicherort für das Protokoll hinterlegt. Nach dem Ändern ist ein Neustart erforderlich, damit die neuen Einstellungen wirksam werden.



Nehmen Sie Änderungen am Speicherort der Protokolldateien mit Bedacht und nur dann vor, wenn sie wirklich notwendig sind. Ohne Zugriff auf diese Dateien funktioniert Ihr Serversystem nicht oder nicht ordnungsgemäß.

Eigene Ereignismeldungen erzeugen

Zum Erzeugen von Ereignismeldungen steht unter Windows Server 2003 standardmäßig das Tool *Eventcreate.exe* zur Verfügung. Zugelassen werden damit nur Meldungen in den beiden Protokollen *Anwendung* und *System*.

Allerdings ist dies nicht nur auf den lokalen Computer beschränkt. Sie können Meldungen auch auf einem anderen, über das Netzwerk erreichbaren Computer erzeugen. Bedingung ist, dass dort als Betriebssystem mindestens Windows 2000 (Professional oder Server) läuft. Mit Windows XP funktioniert es ebenfalls. Ereignisse, die auf dem Server passieren, können Sie beispielsweise so auf Ihrem Administrator-PC anzeigen lassen.



Die Syntax für den Aufruf des Programms lautet:

```
Eventcreate [<optionen>] /t {ERROR | WARNING | INFORMATION}
  ↵ /id <ereignis-id> /d <beschreibung>
```

In der nachfolgenden Tabelle finden Sie einen Überblick über die wichtigsten Optionen. In der Online-Hilfe sind alle Optionen ausführlicher erklärt.

Option	Erklärung	Beispiel
/s <computer>	Zielcomputer, auf dem die Meldung erzeugt werden soll	/s 192.168.100.1 /s Server1.comzept.de
/u <benutzer>	Benutzerkonto, unter dem die Meldung generiert werden soll	/u Uwe /u COMZEPT\Joerg
/p <passwort>	Kennwort für den angegebenen Benutzer	/p Hall34oechen
/l <protokoll>	Zielprotokoll, gültig sind APPLICATION oder SYSTEM; Standardvorgabe ist APPLICATION	/l APPLICATION /l SYSTEM
/so <quelle>	Quelle für das Ereignis, kann beliebig gewählt werden	/so MeineAnwendung

Tabelle 3.1: Optionen von *Eventcreate.exe*

Wollen Sie eine Informations-Meldung auf dem lokalen Server im Systemprotokoll erzeugen, kann der Aufruf wie folgt aussehen:

```
Eventcreate /l SYSTEM /so Sicherscript /t INFORMATION /id 99 /d
  ↵ "Sicherung ist erfolgt"
```

Eine Fehler-Meldung auf einem entfernten PC könnte so erzeugt werden:

```
Eventcreate /s WKS402 /so MeinProg /t ERROR /id 1099 /d
  ↵ "Fehler beim Initialisieren von Modul 4711"
```

Ereignisse überwachen und darauf reagieren

Wie Sie bisher gesehen haben, ist das Ereignisprotokoll vielfältig für die Überwachung des Systems einsetz- und konfigurierbar. Mit Windows Server 2003 kommt ein weiteres Tool hinzu, welches Ihnen das explizite Überwachen bestimmter Ereignisse ermöglicht: *Eventtriggers.exe*. Über dieses Kommandozeilenprogramm können Sie Trigger (*Ereignisüberwacher*) anlegen, die auf bestimmte Ereignismeldungen reagieren.



Für den Aufruf des Programms gibt es drei verschiedene Betriebsmodi mit jeweils einer eigenen Syntax:

- **Eventtriggers /create:** Damit erstellen Sie einen neuen Trigger, indem Sie einer Ereignismeldung, die in einem bestimmten oder in allen Protokollen auftreten kann, eine Behandlungsroutine zuweisen. Diese kann ein Programm, eine Stapelverarbeitungsdatei oder ein Skript sein.
- **Eventtriggers /delete:** Trigger können über diese Option wieder gelöscht werden.
- **Eventtriggers /query:** Sie können sich die gesetzten Eigenschaften eines Triggers anzeigen lassen.

Der Aufruf von *Eventtriggers* ohne weitere Optionen gibt die Liste bisher angelegter Trigger aus.

Ereignismeldungen anzeigen und weiterverarbeiten

Zur Anzeige der Ereignismeldungen benutzen Sie in der Praxis primär das Snap-In *Ereignisanzeige*. Wollen Sie die Meldungen jedoch in anderen Anwendungen weiterverarbeiten oder einfach nur in Textdateien archivieren, gibt es zusätzliche Tools. Nachfolgend finden Sie eine kleine Übersicht über drei Tools, die im Lieferumfang von Windows Server 2003 oder frei erhältlich sind:

- **Eventquery.vbs:** Dieses Skript ist standardmäßig enthalten. Sie können damit Ereignismeldungen filtern, anzeigen und in eine Textdatei schreiben. Eine genaue Beschreibung finden Sie in der Online-Hilfe.
- **DumpEL.exe:** Dieses kleine Programm ist Teil des Windows Ressource Kits und wird von Microsoft zum freien Download angeboten. Sie finden es, wenn Sie die Suchseite zum Download-Center aufrufen und als Suchbegriff den Programmnamen eingeben:
www.microsoft.com/downloads/search.aspx/
- **DumpEVT.exe:** Dies ist ein leistungsfähiges Kommandozeilenprogramm, welches die Firma *Somarsoft* entwickelt hat. Es wird über die Website von *SystemTools.com* kostenlos angeboten:
www.systemtools.com/somarsoft/



3.5 Der Task-Manager

Mit dem Task-Manager erhalten Sie einen direkten Einblick in das System. Sie können damit alle laufenden Prozesse sowie die Belastung der wichtigsten Systemressourcen kontrollieren. Der Task-Manager ist eine »normale« Windows-Anwendung und kann nicht für die Remote Administration eingesetzt werden.

Starten des Task-Managers

Den Task-Manager können Sie über verschiedene Wege starten:

- Drücken Sie die Tastenkombination **Shift**+**Strg**+**Esc**. Der Task-Manager wird damit sofort gestartet.
- Klicken Sie mit der alternativen Maustaste auf eine freie Stelle in der Taskleiste und wählen Sie aus dem erscheinenden Kontextmenü den Eintrag **TASK-MANAGER**.
- Mit der Tastenkombination **Strg**+**Alt**+**Entf** rufen Sie das Dialogfenster **WINDOWS-SICHERHEIT** auf. Hier finden Sie ein Kontrollkästchen für den Aufruf des Task-Managers.
- An der Eingabeaufforderung lässt sich der Task-Manager ebenfalls starten. Der Aufruf lautet **Taskmgr.exe**.

Informationen zur Systemleistung auswerten

In der Standard-Ansicht des Task-Managers nach dem Aufruf ist die Registerkarte **SYSTEMLEISTUNG** aktiv.

Die wichtigsten Parameter, die Sie im Blick haben sollten, sind die folgenden:

- **VERLAUF DER CPU-AUSLASTUNG:** Hier sehen Sie pro CPU eine Grafik, die Ihnen Auskunft darüber gibt, wie stark diese momentan belastet ist.
- **VERLAUF DER AUSLAGERUNGSDATEIAUSLASTUNG:** In dieser Grafik sehen Sie, wie viel virtueller Speicher momentan benötigt wird. Insofern ist die Bezeichnung irreführend und wieder einmal eine »unglückliche« Übersetzung aus dem Englischen. Dort heißt dieser Parameter *Commit Charge* und drückt damit genauer aus, was gemeint ist: Der Verbrauch an virtuellem Speicher, dessen Gesamtumfang sich aus dem physikalischen Speicher und der momentan zugewiesenen Größe der Auslagerungsdatei zusammensetzt.
- **PHYSIKALISCHER SPEICHER:** Hier sind wichtige Informationen zum Verbrauch des im Server installierten RAM (*Random Access Memory*) untergebracht. **INSGESAMT** zeigt die Größe des installierten RAMs, **VERFÜGBAR** den momentan noch freien Anteil

davon. Sinkt dieser Wert dauerhaft auf wenige Tausend Kbyte, kann dies auf einen ernsten RAM-Engpass hindeuten oder auf Prozesse, die zuviel davon okkupieren.

- **ZUGESICHERTER SPEICHER:** Dies ist noch einmal die nichtgrafische Darstellung der Auslastung des virtuellen Speichers. Der **GRENZWERT** ist dabei dessen derzeitige maximale Größe, die sich aus dem belegten Wert für die Auslagerungsdatei und der Größe des installierten RAM (physikalischer Speicher: **INSGESAMT**) ergibt. Der **MAXIMALWERT** gibt an, wie viel vom virtuellen Speicher seit Systemstart maximal benötigt wurden ist. Wenn dieser Wert größer als der **GRENZWERT** ist, wurde zwischenzeitlich wegen eines Speicherengpasses die Auslagerungsdatei vergrößert. Dies ist dann nicht unbedingt ungewöhnlich, wenn die Größe der Auslagerungsdatei nicht fest, sondern wie standardmäßig vorgesehen dynamisch eingestellt worden ist.

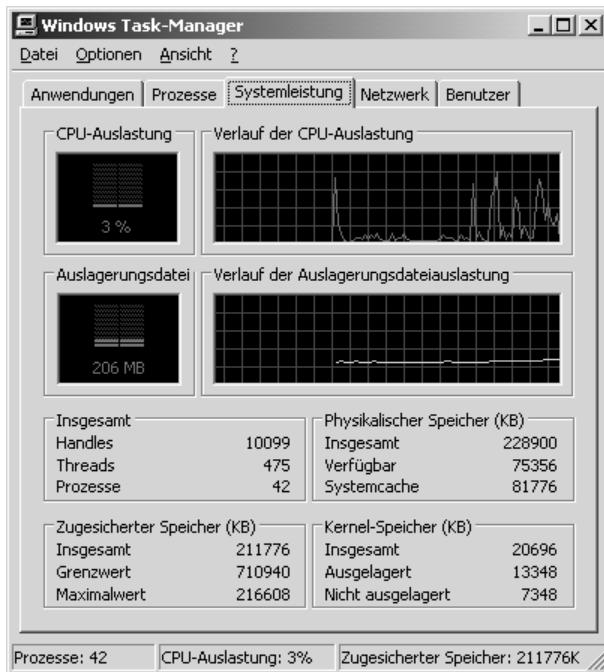


Abbildung 3.28:
Der Task-Manager mit Anzeige der Parameter zur Systemleistung

Kernel-Zeiten anzeigen lassen

Über den Punkt **KERNEL-ZEITEN ANZEIGEN** des Menüs **ANSICHT** wird eine zusätzliche rote Linie eingeblendet, welche die Belastung pro CPU mit Kerneloperationen zeigt. Je höher diese ist, desto mehr Prozesse laufen im privilegierten Modus.



Prozesse im Blick behalten

Bei einem Serversystem sind es weniger die momentan laufenden Anwendungen, die Sie als Benutzer am System gestartet haben, sondern vielmehr die Prozesse, auf die Sie ab und an einen kritischen Blick werfen sollten.

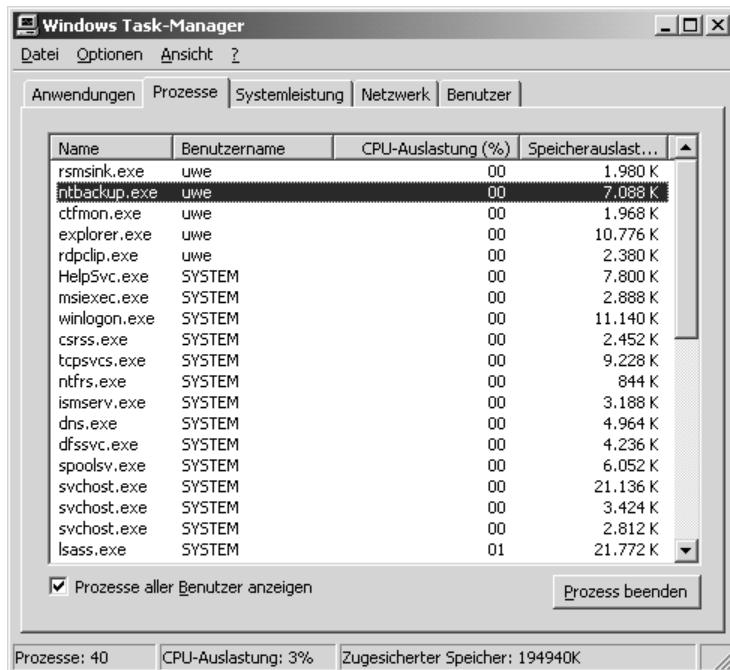


Abbildung 3.29:
Die Prozessliste im
Task-Manager

Hier lässt sich relativ schnell herausfinden, welche Prozesse das System besonders stark beschäftigen. Klicken Sie auf die Spaltenbezeichnung CPU-AUSLASTUNG und Sie erhalten die Prozesse nach ihrer Belastung der Prozessorleistung sortiert. Wenn dann an erster Stelle der *Leerlaufprozess* mit mehr als 90 % Dauerbelastung erscheint, hat der Server nicht viel zu tun. Ebenso können Sie leicht überprüfen, welche Prozesse derzeit den meisten Speicherbedarf aufweisen.

Prozesse anzeigen und beenden

Über Aktivieren des Kontrollkästchens PROZESSE ALLER BENUTZER ZEIGEN können Sie herausfinden, welche Prozesse von anderen Benutzeranmeldungen am Server gestartet worden sind. Dies sind beispielsweise Prozesse in einer laufenden Terminalsitzung. In Abbildung 3.29 zeigt der markierte Eintrag, dass in der Terminalsitzung des Benutzers Uwe



das Programm *Ntbackup* läuft. Dabei kann diese Terminalsitzung derzeit getrennt sein. Trotzdem können laufende Anwendungen und Prozesse in einer solchen Sitzung den Server stark beschäftigen. Im Notfall lassen sich diese in der Prozessliste des Task-Managers »gewaltsam« beenden. Am Tag 4 werden wir unter anderem die Terminaldienste von Windows Server 2003 eingehend behandeln.



Generell sollten Sie mit dem Beenden von Prozessen über den Task-Manager sehr vorsichtig umgehen. Das Beenden einzelner Prozesse kann zu Instabilitäten von Serveranwendungen oder des gesamten Systems führen. Prüfen Sie deshalb immer zuerst, ob Sie nicht besser einzelne Dienste neu starten können.

Zum Beenden von Prozessen steht Ihnen die Schaltfläche PROZESS BEENDEN zur Verfügung. Zusätzlich können Sie im Kontextmenü zum betreffenden Prozess (rechte Maustaste) den Punkt PROZESSSTRUKTUR BEENDEN verwenden. Damit beenden Sie alle mit dem Ausgangsprozess im Zusammenhang stehenden Prozesse. Ein Prozess beziehungsweise eine Anwendung startet meist nicht nur einen Prozess. Somit vermeiden Sie, dass »herrenlose« Prozesse weiter im System verbleiben.

Informationen zu Prozessen auswerten

Neben den bereits erwähnten Parametern CPU- und SPEICHERAUSLASTUNG können Sie der Prozessliste weitere wichtige Informationen entnehmen. Dazu müssen Sie die Liste um zusätzliche Spalten erweitern. Klicken Sie dazu im Menü ANSICHT auf den Punkt SPALTEN AUSWÄHLEN.

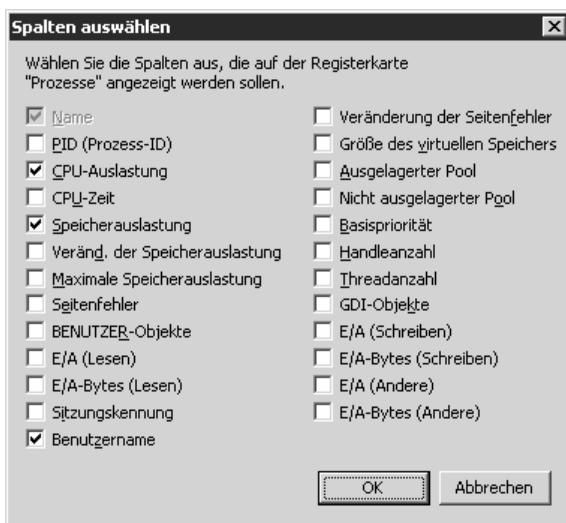


Abbildung 3.30:
Weitere Spalten für die Anzeige der Prozessliste auswählen



Die folgenden Werte können wertvolle zusätzliche Informationen bringen:

- **CPU-ZEIT:** Hier wird die Zeitspanne in Sekunden angezeigt, die dieser Prozess seit seinem Start die CPU beschäftigt hat.
- **VERÄNDERUNG DER SPEICHERAUSLASTUNG:** Dieser Wert gibt an, wie ein Programm dynamisch Speicherplatz anfordert und wieder freigibt. Wenn dieser Wert kontinuierlich steigt, anstatt immer wieder bei Null zu landen, zeigt dies an, dass der Prozess immer mehr Speicher anfordert. Dies kann auf eine Fehlfunktion des Prozesses hinweisen.
- **MAXIMALE SPEICHERAUSLASTUNG:** Der bisher maximal in Beschlag genommene Speicherplatz wird angezeigt.

Diese Werte sind die Leistungsindikatoren, die mit dem Systemmonitor angezeigt werden können.

Prozessprioritäten ändern

Sollte ein Prozess das gesamte System zu stark beschäftigen, sodass der Server für andere Aufgaben nicht mehr genügend Rechenkapazitäten zur Verfügung hat, können Sie dessen Priorität herabsetzen.



Das Ändern von Prozessprioritäten kann zu unerwünschten Nebeneffekten führen. Sie sollten dies daher nur im Notfall versuchen. Eine starke CPU-Belastung des Servers kann daher röhren, dass das System Hardware-seitig den Anforderungen nicht mehr genügt. Eine Aufrüstung mit einer leistungsstärkeren CPU, der Umstieg auf eine Mehrprozessormaschine oder die Verlagerung der Aufgaben auf mehrere Server sind dann vielleicht sinnvoller.

Um die Prozesspriorität zu ändern, markieren Sie eine Prozess und wählen Sie aus dem Kontextmenü den Punkt **PRIORITÄT FESTLEGEN**.

Auslastung der Netzwerkschnittstellen

Über die Registerkarte **NETZWERK** erhalten Sie Einblick in die momentane Belastung der Netzwerkschnittstellen. Für jede Netzwerkkarte wird in einer Grafik angezeigt, wie hoch die prozentuale Auslastung der maximal zur Verfügung stehenden Bandbreite ist. Ist die Netzwerkperformance aus Sicht der Client-PCs unbefriedigend, sollten Sie einen Blick auf diese Grafiken werfen.

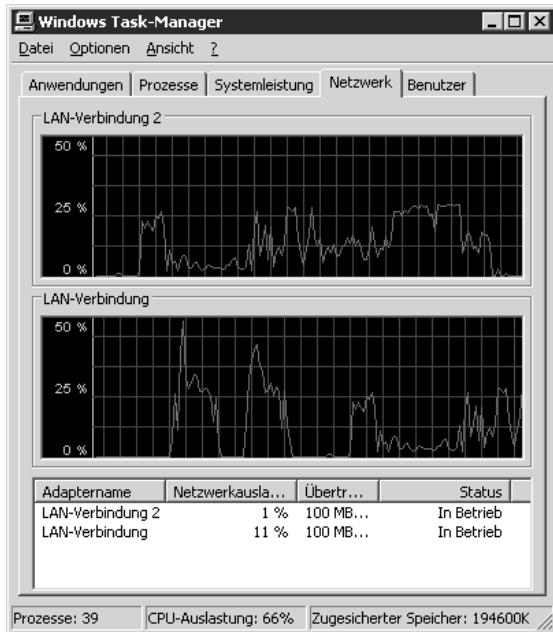


Abbildung 3.31:
Anzeige der Auslastung der
Netzwerkschnittstellen

Liegt die angezeigte Ausnutzung der Bandbreite am Server trotz voller Belastung durch Clientanfragen deutlich unter 25%, kann dies, wenn sonst die CPU-Belastung relativ gering ist, auf Probleme mit den Netzwerkkarten hinweisen (Treiber oder Hardware). Ist hingegen auch die CPU-Belastung des Servers hoch, könnte die Gesamtleistung des Servers unzureichend sein.

Angemeldete Benutzer

Hinter der Registerkarte BENUTZER verbirgt sich eine Liste, welche die Benutzersitzungen anzeigt, die auf dem betreffenden Server laufen. Dies können Sitzungen sein, die über eine Remote Desktop-Verbindung mittels der Terminaldienste von Windows Server 2003 initiiert worden sind.

In Abbildung 3.32 sehen Sie als Beispiel drei Benutzersitzungen, die auf dem Server ausgeführt werden und auf diesem natürlich Ressourcen binden. Unter STATUS erkennen Sie, ob die Verbindung derzeit besteht oder getrennt worden ist. Wird eine Terminalsitzung nur beendet, ohne dass eine Abmeldung erfolgt ist, laufen dort gestartete Programme beziehungsweise deren Prozesse noch weiter. Über den Task-Manager können Sie dies hier erkennen und im Notfall eine Sitzung über einen Klick auf ABMELDEN gewaltsam beenden. Laufende Programme werden dann allerdings ebenfalls beendet.



Abbildung 3.32:
Derzeit angemeldete Benutzer am Server

Unter **CLIENTNAME** sehen Sie den Namen des Computers, von dem aus der **BENUTZER** über eine Terminalsitzung mit dem System verbunden ist. Wird kein Clientname angegeben, obwohl der Status **AKTIV** ist, ist die Anmeldung direkt lokal am Serversystem erfolgt.

Anwendungen beenden

Die Registerkarte **ANWENDUNGEN** erlaubt einen Blick auf die Liste der gestarteten Programme. Bei einem Client-PC unter Windows NT/2000/XP werden Sie dies vielleicht schon häufiger eingesetzt haben, um hängende Anwendungen zu beenden. Bei einem Serversystem finden Sie hier in der Regel kaum Einträge, da die meisten serverbasierten Anwendungen als Dienste implementiert sind. Auf diese können Sie dann über das Managementkonsolen-Snap-In *Dienste* oder die Prozessliste im Task-Manager zugreifen.

3.6 Tasks für die automatische Ausführung planen

Damit ein Serversystem problemlos Tag und Nacht seine Arbeit verrichtet, sind von Zeit zu Zeit bestimmte Wartungsarbeiten, beispielsweise eine regelmäßige Defragmentierung der Festplatten, notwendig. Diese können Sie mit Hilfe des Windows Taskplaners und weiterer Kommandozeilen-Tools zeitgesteuert automatisiert ablaufen lassen.



Für die Einrichtung und Verwaltung von solchen Tasks stehen drei Werkzeuge zur Verfügung:

- *Windows Taskplaner*: Mit diesem grafischen Werkzeug können Sie sehr einfach und bei Bedarf mit Hilfe eines Assistenten Tasks neu erstellen oder bestehende bearbeiten.
- *Schtasks.exe*: Dies ist das Gegenstück zum grafischen Werkzeug und stellt auf der Kommandozeile ebenfalls alle Optionen zur Erzeugung und Bearbeitung von Tasks zur Verfügung.
- *At.exe*: Dieses Kommandozeilentool ist von Windows NT her bekannt und auch im neuen Serverbetriebssystem enthalten. Mit *At* erzeugte Tasks werden im Windows-Taskplaner angezeigt und können bei Bedarf dort gelöscht werden. Eine Bearbeitung von *At*-Task-Eigenschaften ist allerdings nur über *At.exe* selbst möglich. Das Programm gilt als Auslaufmodell und soll durch *Schtasks.exe* ersetzt werden.

Diese drei Werkzeuge werden in den nachfolgenden Abschnitten näher vorgestellt.

Der Windows-Taskplaner

Mit dem Taskplaner können Sie beliebige Programme oder Stapelverarbeitungsdateien zu bestimmten Zeitpunkten, beim Starten des Servers oder bei der Anmeldung ausführen lassen. Den Zugriff auf den Taskplaner erhalten Sie wie folgt:

- Sie starten das Programm GEPLANTE TASKS direkt am Server über das Startmenü ALLE PROGRAMME/ZUBEHÖR/SYSTEMPROGRAMME.
- Sie haben einen direkten Zugriff auf dieses Programm und schon geplante Tasks über das Startmenü, wenn Sie hier SYSTEMSTEUERUNG wählen.
- Sie greifen auf dieses Programm über das Netzwerk zu. Dazu suchen Sie den betreffenden Server in der NETZWERKUMGEBUNG am Client-System.

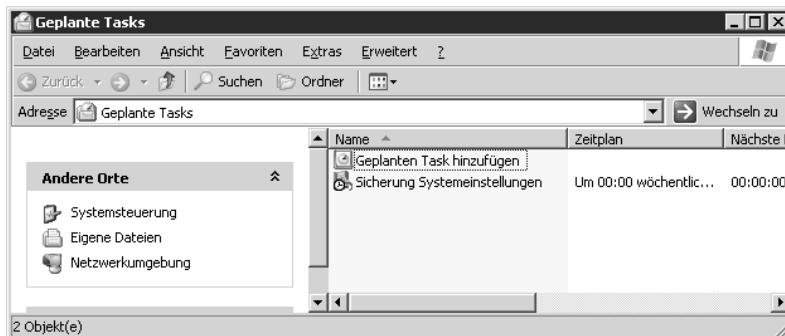


Abbildung 3.33:
Der Taskplaner
im direkten
Zugriff am
Server



Für das Planen von Tasks über das Netzwerk ist es natürlich notwendig, dass Sie sich mit Administratorrechten angemeldet haben.

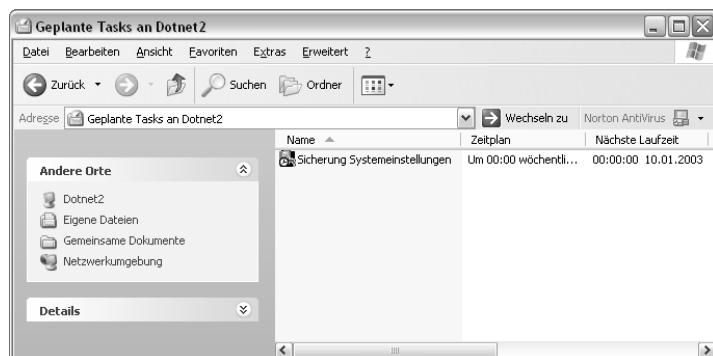


Abbildung 3.34:
Zugriff auf den Taskplaner über das Netzwerk

Auf den Taskplaner greifen auch reguläre Windows-Anwendungen zu. So finden Sie hier ebenfalls Einträge über geplante Datensicherungen, die Sie mit dem Standard-Datensicherungsprogramm *Ntbackup* einrichten können. Dieses Programm wird am Tag 21 eingehend behandelt.

Einen neuen Task erstellen

Nachfolgend wird gezeigt, wie Sie einen neuen Task einrichten können. Dabei soll als Beispiel das Planen einer regelmäßigen Defragmentierung eines Volumes dienen.

Starten Sie dazu zuerst den Taskplaner. Da für den Aufruf der Kommandozeilenversion des Defragmentierprogramms einige Optionen benötigt werden, ist es einfacher, den Task nicht über den Assistenten zu erstellen. Gehen Sie deshalb wie folgt vor:

1. Wählen Sie im Menü DATEI den Punkt NEU/GEPLANTER TASK. Daraufhin erscheint ein neues Symbol mit dem Namen NEUER TASK. Existiert bereits ein Task mit diesem Namen, wird der nächste mit einer eindeutigen, fortlaufenden Nummer versehen.
2. Sie sollten dem Task einen verständlichen Namen geben. Nennen Sie ihn beispielsweise »Festplatte C defragmentieren«. Klicken Sie auf das Task-Symbol und drücken Sie dann die Taste **F2**.
3. Doppelklicken Sie auf das Task-Symbol. Im EIGENSCHAFTEN-Dialogfenster zum Task können Sie nun alle weiteren Einstellungen vornehmen. Tragen Sie in der Registerkarte TASK unter AUSFÜHREN den kompletten Pfad zum Programm und alle notwendigen Optionen ein. Um das Defragmentierprogramm für die Bearbeitung der Festplatte C: zu starten, geben Sie ein:

`C:\WINDOWS\system32\defrag.exe c: -f`



Beachten Sie die folgenden Hinweise, wenn Sie ein Kommandozeilenprogramm mit Optionen im Task aufrufen:

- Geben Sie die gesamte Zeile ohne Anführungszeichen im Eingabefeld an.
- Benötigen Sie die Ausgabe des Programms zur Protokollierung, können Sie auf der Kommandozeile die Umleitungszeichen > und >> benutzen. Die Umleitungszeichen können Sie allerdings nicht im Aufruf des Programms direkt im Task-Eigenschaftenfenster verwenden. Erstellen Sie stattdessen eine Stapelverarbeitungsdatei, beispielsweise mit dem Namen *Defr.cmd*, in welcher der komplette Aufruf untergebracht wird:

```
C:\WINDOWS\system32\defrag.exe c: -f >>C:\Logs\Defr.txt
```

Unter AUSFÜHREN tragen Sie dann diese Stapelverarbeitungsdatei ein.

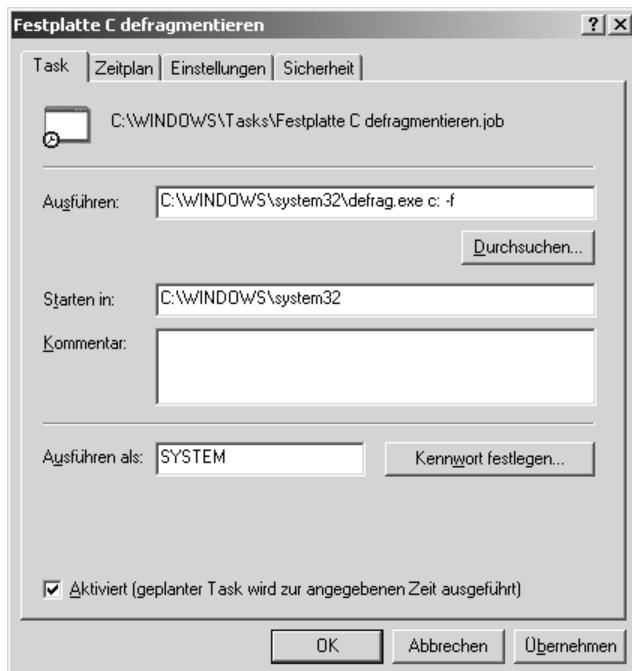


Abbildung 3.35:
Einstellungen zum Task vornehmen

4. Unter AUSFÜHREN ALS wird das Konto eingetragen, unter dem der Task ablaufen soll. Standardmäßig wird hier das Administrator-Konto eingetragen, wenn Sie als dieser am System angemeldet sind. Spätestens bei Abschluss der Einrichtung dieses Tasks müssen Sie das Kennwort für dieses Konto, also hier das des Administrators, eingeben. Wenn der Task startet, versucht er, sich mit dem angegebenen Konto und dem hier hinterlegten Kennwort am System anzumelden.



Wenn Sie das Kennwort für den Administrator ändern, was Sie in regelmäßigen Abständen auch tun sollten, werden die Tasks nicht mehr ausgeführt, in denen noch das alte Kennwort hinterlegt ist.

Um dieses Problem zu umgehen, sollten Sie, wenn möglich, die Tasks unter dem Konto SYSTEM laufen lassen. Tragen Sie dazu bei AUSFÜHREN ALS das Wort SYSTEM ein. Wenn Sie dann zur Eingabe des Kennworts für dieses Konto aufgefordert werden, lassen Sie es einfach leer. Das System-Konto hat kein Kennwort. Damit ist sichergestellt, dass dieser Task immer ausgeführt werden kann.

5. In der Registerkarte ZEITPLAN stellen Sie dann ein, wann und wie oft der Task ausgeführt werden soll.

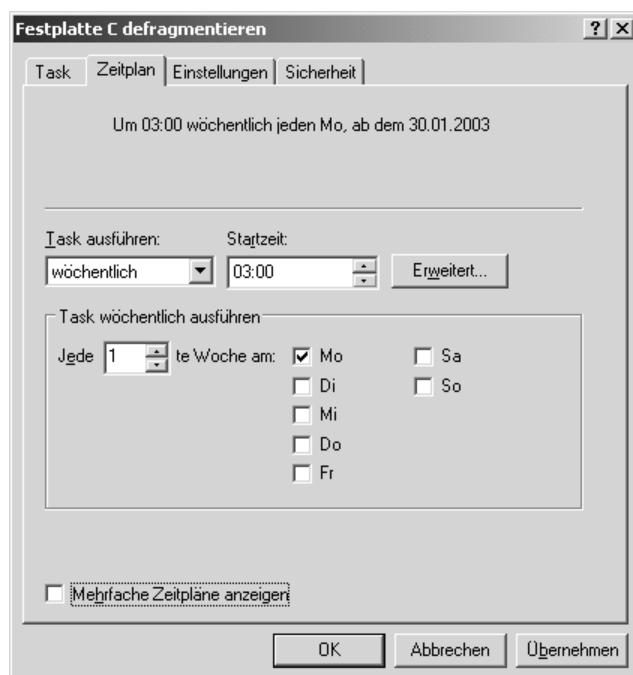


Abbildung 3.36:
Einstellungen zum Zeitplan
für den Task

Unter TASK AUSFÜHREN wählen Sie aus, ob der Task einmalig, regelmäßig, bei einem bestimmten Ereignis (Systemstart, Anmeldung) oder dann ausgeführt wird, wenn der Server gerade nichts zu tun hat (Leerlauf). Über die Schaltfläche ERWEITERT stehen noch weitere Optionen zur Verfügung. So lässt sich ein Task über die Angabe eines Start- und Enddatums zeitlich begrenzen.

Wenn Sie MEHRFACHE ZEITPLÄNE aktivieren, können Sie für einen Task verschiedene Zeitplanungen einrichten. Das erhöht allerdings nicht gerade die Übersichtlichkeit.



keit, da im Dialogfenster GEPLANTE TASKS dann unter ZEITPLAN nur noch MEHRFACHE PLANUNGSZEITEN erscheint anstelle der konkreten Angaben zum Zeitplan. Ein Ausweg: Das Kommandozeilentool *Schtasks.exe* zeigt Tasks mit mehrfachen Zeitplänen mit jedem Zeitplan separat an.

6. In der Registerkarte EINSTELLUNGEN haben Sie weitere Möglichkeiten, das Laufverhalten des Tasks zu beeinflussen. Wichtig ist die Option TASK BEENDEN NACH, da Sie damit einstellen, wie lange der Task maximal laufen soll. Ein Server sollte schließlich nicht auf Dauer mit einem hängenden Programm zu tun haben. Geben Sie einen Zeitraum ein, der maximal für die Abarbeitung des Tasks, zuzüglich einer Sicherheitsreserve, benötigt wird.

Sicherlich seltener benötigt wird es, einen Task nur bei *Leerlauf* des Servers ausführen zu lassen. Denkbar sind vielleicht spezielle Anwendungen wie das Indizieren einer großen Datenbank. Das kann damit immer dann gestartet werden, wenn der Server einmal nichts zu tun hat.

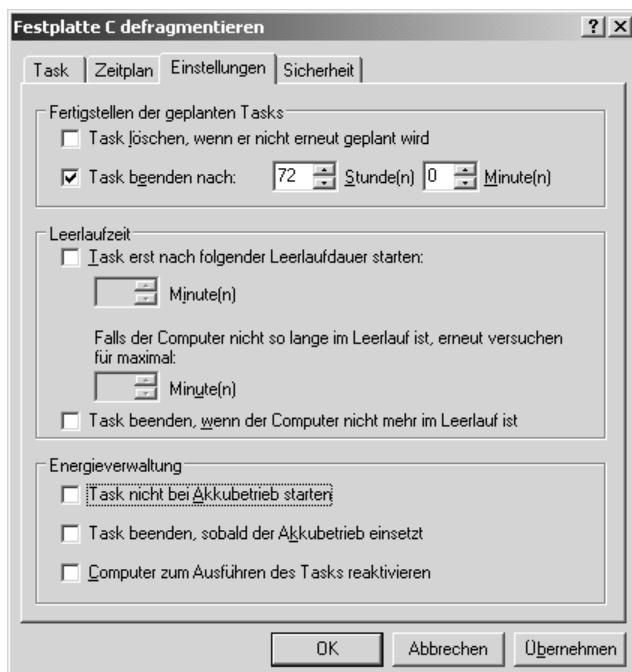


Abbildung 3.37:
Weitere Einstellungen zum Laufverhalten des Tasks

Bei einem Server nicht relevant sind die Einstellungen in der Rubrik ENERGIEVERWALTUNG. Im Interesse einer ständigen Verfügbarkeit sollten die Energieoptionen, einstellbar in der Systemsteuerung, stets auf *Dauerbetrieb* eingestellt sein.



7. Über die Registerkarte SICHERHEIT können Sie spezifizieren, welche Konten mit welchen Rechten den Task ausführen beziehungsweise ändern dürfen. In der Regel sollten nur der Administrator und das System-Konto Rechte haben.

Nach Abschluss der Einstellungen zu dem Task können Sie diesen testen, indem Sie im Menü DATEI des Dialogfensters GEPLANTE TASKS den Punkt AUSFÜHREN wählen.

Protokoll für Ausführung der Tasks einsehen

Ob ein Task erfolgreich gestartet werden konnte oder nicht, können Sie dem Protokoll des Taskplaners entnehmen. Wählen Sie im Menü ERWEITERT den Punkt PROTOKOLL ANZEIGEN.

```

SchedLgU.Txt - Editor
Datei Bearbeiten Format Ansicht ?
"Defragmentierung.job" (-f -v) 30.01.2003 22:46:33 ** FEHLER **
  Der Task konnte nicht gestartet werden..
  Der genaue Fehler ist:
  0x80070005: Zugriff verweigert
  suchen sie die Anwendung über die Schaltfläche "Durchsuchen" auf der Reihe
  "Festplatte C defragmentieren.job" (defrag.exe)
  Start: 30.01.2003 23:03:04
  "Festplatte C defragmentieren.job" (defrag.exe)
  Ende: 30.01.2003 23:03:06
  Ergebnis: Der Task wurde mit folgendem Ergebniswert abgeschlossen: (0).

```

Abbildung 3.38:
Protokoll des
Taskplaners

Wenn ein Task erfolgreich gestartet werden konnte, heißt das nur, dass das entsprechende Programm oder die Stapelverarbeitungsdatei gefunden und gestartet werden konnten. Ob diese selbst ihre Aufgaben erfolgreich abgeschlossen haben, können Sie in diesem Protokoll nur bedingt ermitteln. Ein ERGEBNISWERT von 0 deutet auf einen fehlerfreien Ablauf hin. Davon abweichende Werte sind meist die Fehlercodes, die von den aufgerufenen Programmen bei Misserfolg ausgegeben werden. Eine Garantie ist dies aber nicht, da es von der konkreten Programmierung der Anwendung abhängt, ob Fehlercodes generiert werden oder nicht.

Sicherer ist es deshalb, wenn Sie die Protokolliermöglichkeiten der Anwendungen selbst nutzen. Viele moderne Programme und Tools nutzen das Ereignisprotokoll zur Aufzeichnung ihrer Meldungen oder geben diese an der Kommandozeile aus. Um sie in eine Textdatei zu schreiben, können Sie die Umleitungszeichen > und >> einsetzen. Beachten Sie dazu aber den Hinweis auf Seite 112.

Kommandozeilen-Tools für das Planen von Tasks

Das Erstellen und Ändern von Tasks können Sie vollständig über die Kommandozeile durchführen.



Schtasks.exe

Da Sie mit diesem Programm alle Optionen zur Verfügung haben, die der grafische Taskplaner bietet, sind die Kommandozeilenoptionen entsprechend komplex. Um den Rahmen dieses Buches nicht zu sprengen, verzichten wir auf die umfassende Erläuterung der Syntax. Sie finden diese ausführlich in der Online-Hilfe.

An dieser Stelle wird zur Veranschaulichung das für den Taskplaner gewählte Beispiel der Planung einer regelmäßigen Defragmentierung mit *Schtasks* gezeigt:

```
Schtasks /create /sc wöchentlich /tn "Festplatte C defragmentieren" /tr  
c:\defr.cmd /ru SYSTEM /d M0 /st 03:00
```

Mit diesem Kommando können Sie den soeben erstellten Task zum ersten Test starten:

```
Schtasks /run /tn "Festplatte C defragmentieren"
```

Die Anzeige aller geplanten Tasks erhalten Sie, wenn Sie *Schtasks* ohne weitere Optionen oder mit */query* aufrufen. Mit */query* haben Sie dann noch weitere Möglichkeiten, die Ausgabe zu formatieren, beispielsweise Komma-separiert oder als Tabelle.

Einen Task können Sie mit diesem Kommando löschen:

```
Schtasks /delete /tn "Festplatte C defragmentieren" /f
```

Damit wird der oben angelegte Task zur regelmäßigen Defragmentierung wieder entfernt. Mit der Option */f* wird die Sicherheitsrückfrage unterdrückt, sodass der Aufruf innerhalb einer automatisch ablaufenden Stapelverarbeitungsdatei genutzt werden kann.

At.exe

Dieses Tool hat wesentlich weniger Optionen und ist damit zum schnellen Arbeiten an der Kommandozeile eigentlich besser geeignet. Vereinfacht lautet die Syntax wie folgt:

```
At <uhrzeit> /every:<wochentag> <programmaufruf>
```

Um eine Datensicherung jeden Freitag um 22:00 Uhr automatisch ausführen zu lassen, können Sie *At* so einsetzen:

```
At 22:00 /every:FR C:\Tools\Sicherung.cmd
```

Soll eine Defragmentierung jeden 1. des Monats um 2:00 Uhr gestartet werden, rufen Sie *At* mit diesen Optionen auf:

```
At 2:00 /every:1 C:\Tools\Defr.cmd
```

Um alle mit *At* erzeugten Tasks anzuzeigen, rufen Sie das Programm ohne weitere Optionen auf.



Beim Erzeugen eines Tasks mit *At* wird eine eindeutige *Statuskennung* zugeteilt. Wenn Sie einen bestimmten *At*-Task wieder löschen wollen, geben Sie dessen Kennung an:

At 1 /delete

Ohne Angabe einer Kennung entfernen Sie alle *At*-Tasks:

At /delete /YES

Die Option */YES* unterdrückt die Anzeige der Sicherheitsrückfrage und beantwortet diese für Sie mit »J«.



Beachten Sie, dass Sie mit dem Tool *At.exe* nur die Tasks bearbeiten und anzeigen können, die Sie mit *At.exe* selbst angelegt haben. Einen vollständigen Zugriff auf alle Tasks erhalten Sie nur über das Dialogfenster GEPLANTE TASKS und das Tool *Schtasks.exe*.

Für *At.exe* gibt es keine Option, mit der Sie das Konto angeben können, unter welchem der Task ausgeführt werden soll. Standardmäßig ist das Konto SYSTEM eingestellt, welches für die meisten Fälle die richtige Einstellung ist. Wenn Sie ein anderes Konto auswählen wollen, öffnen Sie im Dialogfenster GEPLANTE TASKS im Hauptmenü den Punkt ERWEITERT/AT-DIENSTKONTO. Hier können Sie dann ein anderes Konto, beispielsweise das des Administrators mit dessen Kennwort, angeben. Beachten Sie, dass von dieser Änderung alle bisher angelegten Tasks betroffen sind.

3.7 Wichtige Kommandozeilen-Tools und Skripte

Für praktisch alle Administrationsaufgaben gibt es unter Windows Server 2003 grafische Tools. Trotzdem werden Sie für die eine oder andere Aufgabe vielleicht auf die Kommandozeile oder vorgefertigte Skripte zurückgreifen wollen. Um beispielsweise die IP-Adresseinstellungen der Netzwerkkarten eines Servers zu ermitteln, geht es schneller, wenn Sie an der Eingabeaufforderung das Kommando *Ipconfig /all* eingeben, als wenn Sie sich durch alle Dialogfenster für die einzelnen Netzwerkadapter klicken.

Die Eingabeaufforderung starten

Das Dialogfenster EINGABEAUFLÖRUNG, meist mit dem Begriff *Kommandozeile* gleichgesetzt, stellt eine Instanz des Befehlsinterpreters *Cmd.exe* dar. Sie können diesen folgendermaßen starten:

1. Wählen Sie im Startmenü den Eintrag EINGABEAUFLÖRUNG, zu finden unter ALLE PROGRAMME/ZUBEHÖR.



2. Klicken Sie im Startmenü auf AUSFÜHREN und geben Sie dann den Befehl *Cmd* ein.

Für den Befehlsinterpretierer gibt es selbst eine Reihe von Optionen, die Sie sich mit *Cmd /?* anzeigen lassen können.



Wenn Ihnen die farbliche Darstellung im Dialogfenster EINGABEAUFGORDE-RUNG zu langweilig ist, können Sie diese so ändern:

- ▶ Rufen Sie an der Kommandozeile den Befehl *Color* auf. Mit *Color F1* erhalten Sie beispielsweise dunkelblaue Schrift auf weißen Untergrund. Mit *Color /?* werden alle Optionen angezeigt. Wenn Sie *Color* ohne Optionen aufrufen, werden die Farbwerte wieder auf die Standardeinstellung gesetzt.
- ▶ Rufen Sie *Cmd.exe* mit der Option */T* auf. Für das obige Beispiel wäre der Aufruf dann *Cmd /T:F1*.

In den nachfolgenden Abschnitten sind ausgewählte Kommandozeilen-Tools und bei Windows Server 2003 mitgelieferte Skripte nach den Haupt-Themengebieten tabellarisch aufgeführt. Die genaue Syntax finden Sie in der sehr ausführlichen Kommandozeilen-Referenz des Hilfe- und Supportcenters.

Datei- und Ordneroperationen

Kommando	Kurzbeschreibung
<i>Attrib.exe</i>	Anzeige und Ändern einfacher Dateiattribute
<i>Cacls.exe</i>	Anzeige und Ändern der Zugriffsberechtigungen von Dateien und Ordner
<i>Cipher.exe</i>	Einstellen der EFS-Verschlüsselung für Dateien
<i>Copy</i>	Kopieren von Dateien
<i>Cd; Chdir</i>	Wechseln des Verzeichnisses
<i>Comp</i>	Vergleich des Inhalts zweier Dateien
<i>Compact</i>	Anzeige und Einstellen der NTFS-Komprimierung für Dateien und Ordner
<i>Del; Erase</i>	Löschen von Dateien
<i>Dir</i>	Auflisten von Dateien und Ordner
<i>Diskcomp.com</i>	Vergleich des Inhalts zweier Disketten

Tabelle 3.2: Kommandozeilentools für Operationen mit Dateien und Ordner



Kommando	Kurzbeschreibung
<i>Diskcopy.com</i>	Kopieren von Disketten
<i>Expand.exe</i>	Entpackt komprimierte Dateien (nicht mit NTFS-Komprimierung zu verwechseln)
<i>Fc.exe</i>	Vergleich des Inhalts zweier Dateien mit umfangreicherer Möglichkeiten als bei Comp.exe
<i>Find.exe</i>	Suchen nach bestimmten Textinhalten in Dateien
<i>Findstr</i>	Suchen nach bestimmten Textinhalten in Dateien, wobei reguläre Ausdrücke verwendet werden können (ähnlich dem unter Unix bekannten Grep-Kommando)
<i>Md; Mkdir</i>	Anlegen eines neuen Verzeichnisses
<i>Move</i>	Verschieben von Dateien
<i>Rename; Ren</i>	Umbenennen von Dateien und Ordnern
<i>Replace</i>	Ersetzt von Dateien durch andere
<i>Rd; Rmdir</i>	Löschen eines Verzeichnisses
<i>Tree.com</i>	Grafische Anzeige von Verzeichnissen und Unterverzeichnissen
<i>Type</i>	Inhalt der angegebenen Datei anzeigen
<i>Xcopy.exe</i>	Kopieren von Dateien und Unterverzeichnissen

Tabelle 3.2: Kommandozeilentools für Operationen mit Dateien und Ordnern (Forts.)

Datenträgerverwaltung

Kommando	Kurzbeschreibung
<i>Bootcfg.exe</i>	Interaktive Einrichtung und Änderung der Datei Boot.ini
<i>Chkdsk.exe</i>	Fehlersuche und Reparatur von Volumes
<i>Chkntfs</i>	Beeinflussen der automatischen Überprüfung von NTFS-Volumes beim Systemstart
<i>Convert.exe</i>	Konvertieren eines FAT/FAT32-Volume nach NTFS

Tabelle 3.3: Kommandozeilentools für die Administration von Datenträgern



Kommando	Kurzbeschreibung
Defrag.exe	Defragmentieren von Laufwerken; ist die Kommandozeilen-Version des grafischen Defragmentierprogramms
Diskpart.exe	Einrichtung von Datenträgern (Festplatten) in Partitionen, logischen Laufwerken bis hin zu Funktionen der dynamischen Datenträgerverwaltung
Format.com	Formatieren von Volumes und Datenträgern
Freedisk.exe	Prüfung des verfügbaren Speicherplatzes auf einem Laufwerk
Fsutil.exe	Verwaltung von Dateisystem-Eigenschaften und -Funktionen
Ftonline	Schreibgeschützter Zugriff auf Windows NT 4-Datenträgersätze
Format.com	Formatieren von Volumes und Datenträgern
Label.exe	Ändern von Namen eines Volumes oder Datenträgers
Mountvol.exe	Verwaltung von Bereitstellungspunkten für Volumes
Recover.exe	Reparatur von beschädigten Volumes und Datenträgern
Vssadmin.exe	Einrichtung und Verwaltung von Volumenschattenkopien
Vol	Anzeige der Volumeinformationen

Tabelle 3.3: Kommandozeilentools für die Administration von Datenträgern (Forts.)

Dienste- und Gerätetreibersteuerung

Kommando	Kurzbeschreibung
Driverquery	Anzeige von Gerätetreibern und ihren Eigenschaften
Sc.exe	Anzeige und Steuerung von Diensten
Net.exe	Kann neben dem Management von Netzwerkfunktionen zur Dienststeuerung genutzt werden.
Mode.com	Anzeige und Steuerung von Anschlussports (LPT, COM, CON)

Tabelle 3.4: Kommandozeilentools für die Steuerung von Windows-Diensten



Druckdienste-Steuerung

Kommando	Kurzbeschreibung
Print.exe	Senden einer Textdatei zu einem Drucker
Prncnfg.vbs	Skript zur Diagnose und Konfiguration von Druckern
Prndrvr.vbs	Skript zum Installieren und Entfernen von Druckertreibern
Prnjobs.vbs	Skript zur Steuerung von Druckjobs
Prnmngr.vbs	Skript zum Installieren und Entfernen von Druckern
Prnport.vbs	Skript zum Installieren und Entfernen von TCP/IP-Druckerports

Tabelle 3.5: Kommandozeilentools für die Administration von Druckdiensten

Netzwerk

Kommando	Kurzbeschreibung
Arp.exe	Anzeige und Änderung der Übersetzungstabellen von IP-Adressen in physische MAC-Adressen
Ftp.exe	FTP-Client für den Zugriff auf einen FTP-Server
Getmac.exe	Liefern der MAC-Adresse des Netzwerkadapters
Hostname.exe	Ausgabe des Computernamens
Ipconfig.exe	Anzeige und Steuerung der IP-Adressierung
Lpq.exe	Informationen zum Status des LPD-Servers
Lpr.exe	Senden einer Datei zum Druck an einen LPD-Server
Net.exe	Umfassendes Tool für die Netzwerksteuerung
Netstat.exe	Statusanzeige zu Netzwerkverbindungen
Nslookup.exe	Abruf von Informationen von einem DNS-Server
Ping.exe	Einfache Verbindungskontrolle zwischen Hosts

Tabelle 3.6: Kommandozeilentools für Einstellungen und Diagnose am Netzwerk



Kommando	Kurzbeschreibung
Route.exe	Anzeige und Bearbeitung der lokalen IP-Routingtabelle
Tracert.exe	Diagnose des IP-Routings

Tabelle 3.6: Kommandozeilentools für Einstellungen und Diagnose am Netzwerk (Forts.)

Active Directory-Verwaltung

Kommando	Kurzbeschreibung
Adprep.exe	Vorbereitung einer Windows 2000 Domäne für ein Upgrade auf Windows Server 2003
Dsadd.exe	Hinzufügen von Objekten (Benutzer, Computer etc.) zum Verzeichnis
Dsget.exe	Ausgabe von Informationen zu einem Objekt
Dsmod.exe	Durchführen von Änderungen an einem Objekt
Dsmove.exe	Verschieben von Objekten innerhalb der Verzeichnisstruktur
Dsquery.exe	Suche nach Objekten im Verzeichnis
Dsrm.exe	Entfernen von Objekten aus dem Verzeichnis
Gpresult.exe	Ausgeben der Gruppenrichtlinien-Einstellungen und der resultierenden effektiven Rechte für Computer und Benutzer
Ntdsutil.exe	Administrationsarbeiten am Active Directory; vor allem für Wartung und Reparatur wichtig

Tabelle 3.7: Kommandozeilentools für die Administration des Active Directory

Systemmanagement und Sonstiges

Kommando	Kurzbeschreibung
At.exe; Schtasks.exe	Einrichten, Ändern und Entfernen von Tasks für die zeitgesteuerte Abarbeitung von Programmen
Cmd.exe	Starten einer neuen Instanz des Befehlsinterpreters

Tabelle 3.8: Kommandozeilen-Tools für das Systemmanagement und andere Aufgaben



Kommando	Kurzbeschreibung
Color	Einstellen der Farbe für das Fenster des Befehlsinterpreters
Date.exe	Einstellen des Systemdatums
Exit	Beenden der laufende Instanz des Befehlsinterpreters
Runas.exe	Starten eines Programm unter einem anderen Benutzerkonto
Shutdown.exe	Erlaubt ein Herunterfahren des Servers
Start.exe	Startet in einer neuen Instanz des Befehlsinterpreters das angegebene Programm
Systeminfo	Ausgabe von Informationen zu wesentlichen Hardware- und Betriebssystemparametern
Taskkill.exe	Beenden eines laufenden Prozesses
Tasklist.exe	Anzeige der laufenden Prozesse
Telnet.exe	Clientsoftware, um auf einen Telnet-Server zuzugreifen
Time.exe	Einstellen der Systemzeit
Title	Einstellen des Fenster-Titels des Befehlsinterpreters
Ver	Anzeige der Windows-Version
Whoami.exe	Ausgabe von Informationen zum angemeldeten Benutzer
Winnt.exe/ Winnt32.exe	Kann zur Installation oder zum Update sowie zur Nutzung der Wiederherstellungskonsole eingesetzt werden

Tabelle 3.8: Kommandozeilen-Tools für das Systemmanagement und andere Aufgaben (Forts.)

3.8 Fragen und Übungen

- F Wie nennt man die Erweiterungsmodule der MMC und wie werden sie eingebunden?
- F Wo erscheinen Meldungen des Betriebssystems?
- F Wie automatisieren Sie regelmäßig durchzuführende Arbeiten auf Windows Server 2003-Serversystem?
- F Mit welcher Tastenkombination wird der Task-Manager direkt gestartet?
- F Wie öffnet man die Kommandozeile, um Kommandozeilen-Tools benutzen zu können?