Kapitel 11 Erstellen und Verwalten von Benutzerkonten ..... 1
11.1 Benutzerkonten ..... 1
11.1.1 Vordefinierte bzw. integrierte Benutzer ..... 2
11.1.2 Richtlinien für die Vergabe von Namen und Kennwörtern ..... 3
11.1.3 Erstellen von Benutzerkonten ..... 5
Anmeldeskripten ..... 8
Speicherort im Verzeichnis ..... 8
Der Befehl NET ..... 11
Basisverzeichnis ..... 13
Profil und Profilpfad ..... 14
Anmeldung und Kontooptionen ..... 14
Anmeldezeiten ..... 14
Remote-Zugriff ..... 15
Computer-Einschränkungen ..... 16
Kontooptionen ..... 17
11.2 Datenträgerkontingente ..... 19
11.3 Gruppen ..... 21
11.3.1 Gruppenbereich ..... 21
Gruppenbereich »Lokale Domäne« ..... 21
Gruppenbereich »Global« ..... 22
Gruppenbereich »Universal« ..... 23
Untergliederung der Gruppen ..... 23
11.3.2 Erstellen einer neuen Gruppe ..... 23
11.3.3 Vordefinierte Standardgruppen ..... 24

# Kapitel 11 Erstellen und Verwalten von Benutzerkonten

In diesem Kapitel geht es darum, wie Benutzerkonten erstellt, verwaltet und in Gruppen zusammengefasst werden. Die wesentliche Aufgabe bei der Benutzerverwaltung besteht darin, die Benutzerbasis zu erstellen und den Gruppen zuzuweisen, die in der Lage sein müssen, auf Ressourcen zugreifen zu können. Auch wenn dieses Kapitel mit dem Erstellen von Benutzerkonten beginnt, sollten Sie sich davon im Umgang mit der Sicherheit nicht beeinflussen lassen. Wie bereits im vorhergehenden Kapitel erwähnt, sollten Sie zuerst die Gruppe für die Ressource erstellen und dann die Benutzer zuweisen. Es ist jedoch kein Fehler, wenn Sie wissen, wer zu der Gruppe gehören soll, die Sie erstellen.
Benutzerkonten bei Windows 2000 sind deutlich leistungsfähiger als sie das bisher waren. Dieses Kapitel soll Ihnen dabei helfen, die Verwaltung von Benutzerkonten zu verstehen. Wenn Sie bereits wissen, wie Benutzerkonten erstellt werden und jetzt wissen möchten, wie Richtlinien erstellt und verwendet werden, dann sollten Sie im folgenden Kapitel weiterlesen.

## 11.1 Benutzerkonten

Das Benutzerkonto ist die Stelle, an der das Gummi die Straße in der Welt des Netzwerkbetriebssystems berührt. Das Benutzerkonto ist die Schlüsselkomponente, die verwendet wird, um auf Netzwerkressourcen zuzugreifen, und es stellt den Kontrollpunkt für jede Berechtigung und jede Richtlinie dar. Bei Windows 2000 haben diese Konten enorm an Bedeutung gewonnen.

Bevor Sie damit beginnen, diese Konten zu erstellen, sollten Sie einige Grundregeln kennen lernen und einige wichtige Informationen erhalten. Das Erstellen von Gruppen und das Hinzufügen von Benutzern zu diesen Gruppen wird hier erwähnt, aber erst später ausführlicher behandelt. Wenn Sie als Administrator noch keine Erfahrung haben, sollten Sie diesen ausführlicheren Abschnitt zuerst lesen, bevor Sie sich daran machen, Konten zu erstellen. So können Sie verhindern, dass Sie Konten erstellen, die Sie später wieder löschen müssen.

### 11.1.1 Vordefinierte bzw. integrierte Benutzer

Wenn Windows 2000 installiert wird, werden einige Benutzerkonten sofort erstellt. Diese Konten werden vom System und von den ersten Benutzern des Systems verwendet, um überhaupt auf das System zugreifen zu können. Ebenso wie bei einem neuen Haus, bei dem es einen ersten Satz Schlüssel gibt, können diese Konten entweder geändert oder so wie sie sind verwendet werden. Es ist jedoch sinnvoll, diese Schlüssel so schnell wie möglich zu ändern.
Welche Konten automatisch erstellt werden, hängt davon ab, welche Dienste installiert sind. In jedem Fall werden auf jedem Server die Konten **Gast** und **Administrator** erstellt. Diese Konten werden erstellt, damit grundlegende Dienste zur Verfügung stehen. Wenn Sie die Konsole **Active Directory-Benutzer und -Computer** öffnen und anschließend auf **Users** klicken (siehe Abbildung 11.1), können Sie die vordefinierten Konten sehen.

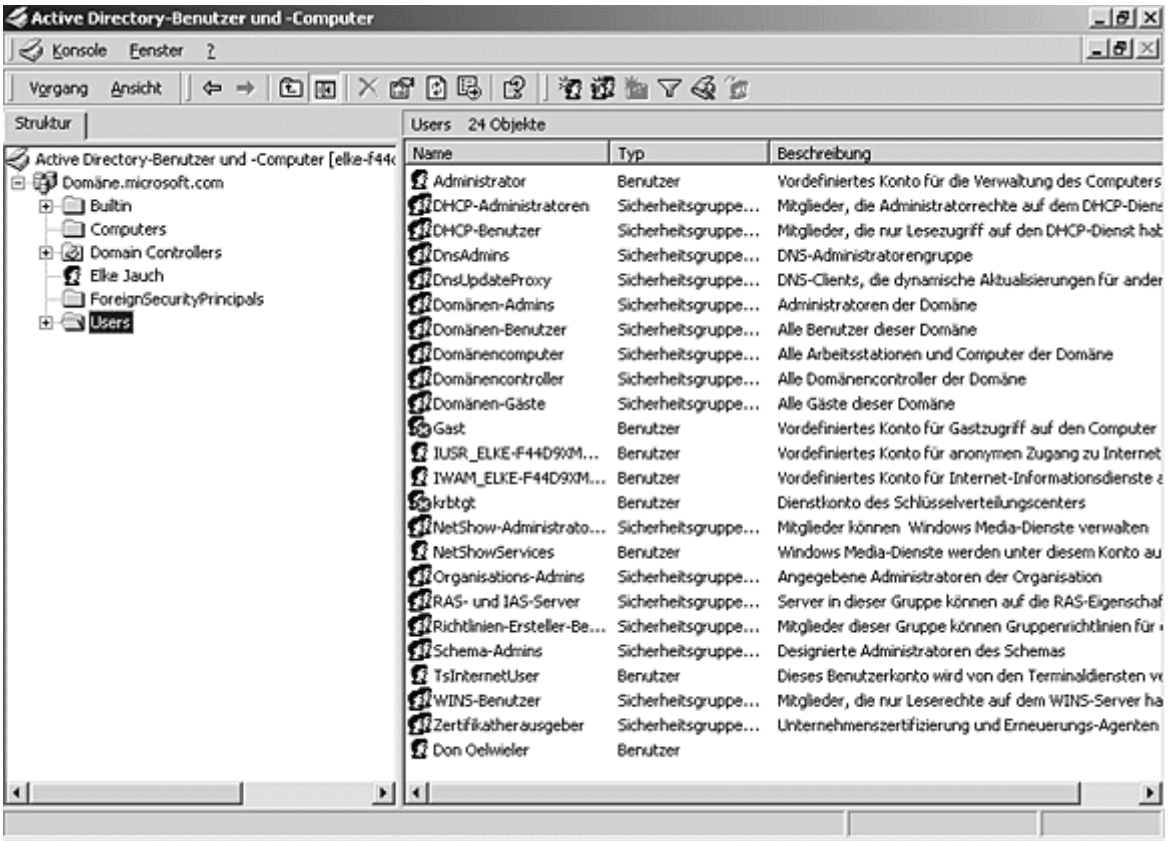


**Abbildung 11.1: Standardkonten für Benutzer und Gruppen**

Mit dem Gastkonto kann nichts installiert werden und das sollte auch so beibehalten werden. Dieses Konto sollte nur dazu dienen, Besuchern Ihres Systems Zugriff auf öffentliche Bereiche wie Drucker oder auch auf Freigaben zu gewähren. Das Beste an diesem Konto ist, dass es zur Gruppe **Domänen-Benutzer** gehört. Das bedeutet, dass dem Gastkonto der für die Gruppen **Domänen-Benutzer** bzw. **Jeder** freigegebene Dienst zur Verfügung steht.

Sie sollten wissen, dass Sie das Gast- und das Administratorkonto nicht löschen, aber umbenennen können.
Eine Ihrer ersten Aufgaben sollte es sein, die vordefinierten Konten umzubenennen. Eindringlinge, die sich auskennen, werden versuchen, sich im System mit Hilfe der vordefinierten Konten anzumelden. Wenn sie einen Kontonamen in Erfahrung bringen können, haben sie die Schlacht schon halb gewonnen. Wenn es sich bei dem Konto dann noch um das Administratorkonto handelt, ist der Krieg vorbei.
Das Administratorkonto wird für die Erstanmeldung und die Erstellung sowie für das Starten von Diensten erstellt. Das Administratorkonto wird auch dann erstellt, wenn der Server nicht in einer Domäne installiert ist. Das Konto wird in der Domäne nicht jedes Mal erstellt, wenn ein neuer Server oder Domänencontroller installiert wird. Wenn Sie einen neuen Server in einer bereits vorhandenen Domäne installieren, fragt das System nach einem Administratornamen und -kennwort, um das Computerkonto in der Domäne zu erstellen.
Benennen Sie das Administratorkonto so schnell wie möglich um. Wenn Sie sich in einer großen Unternehmensumgebung befinden, können Sie nie wissen, wer sich wie lange schon im System aufhält, bis Sie die Konten umbenennen.
Als Nächstes sollten Sie ein zweites Konto erstellen, das Mitglied der Gruppen **Domänen-Admins** und **Administrator** ist. Dadurch, dass Sie dieses Konto erstellen, lassen Sie sich eine Hintertür offen, falls das Administratorkonto einmal unbrauchbar werden sollte. Es kommt gar nicht so selten vor, dass das Kennwort des Administratorkontos geändert wird und sich keiner mehr an den Namen erinnern kann. Damit ist die Burg verschlossen und der Schlüssel auf Nimmerwiedersehen verschwunden.
Eine gute Übung für Systemadministratoren ist es, sich bei ihrer täglichen Arbeit mit der Domäne nicht als Administrator anzumelden. Oder anders ausgedrückt: Verwenden Sie kein Konto, das allmächtig ist, wenn Sie mit einem Textverarbeitungs- oder Tabellenkalkulationsprogramm arbeiten. Sie sollten immer daran denken, dass Sie Dateien ohne Kontrolle ändern können, wenn Sie sich als Administrator anmelden. Dabei kann es Ihnen wie Gulliver bei den Liliputanern ergehen. Sie könnten auf etwas treten. Oder noch schlimmer: Wenn Sie Ihren Arbeitsplatz verlassen, ohne sich abzumelden, ist das Sicherheitssystem geöffnet.
Allzu häufig kennen die Besitzer oder leitende Angestellte eines Unternehmens das Administratorkennwort für die Domäne, in der ihre Daten enthalten sind, nicht. Es ist jedoch durchaus sinnvoll, den Besitzern oder leitenden Angestellten eines Unternehmens eine Liste dieser Kennwörter zur Verfügung zu stellen, für den Fall, dass ein Mitarbeiter das Unternehmen verlässt oder aus anderen Gründen nicht erreichbar ist. So ist es möglich, dass die Angestellten wieder an ihr System kommen.

### 11.1.2 Richtlinien für die Vergabe von Namen und Kennwörtern

Sie sollten die Aufgabe des Erstellens von Benutzerkonten ernst nehmen. Wenn Sie Robert Schmidt den Benutzernamen »Bert« und das Kennwort »Angela« (den Namen seiner Frau) zuweisen, ist das in einer kleinen Büroumgebung kein Problem. Wenn Sie jedoch 30 oder mehr Konten einrichten, wird es etwas schwieriger, sich solche netten Kombinationen auszudenken. Das ist allerdings die kleinste Sorge, die Sie in einem Szenario wie dem eben geschilderten haben werden. Die Sicherheit ist praktisch mit ihrer Einrichtung schon nicht mehr existent.
Bei Windows 2000 kann praktisch jede beliebige Methode für die Vergabe von Namen für Benutzer und Gruppen eingerichtet und verwendet werden. Das

Programm ermöglicht dabei auch die Kontrolle darüber, ob ein Benutzer berechtigt ist, ein bestimmtes Kennwort zu verwenden. Bei Kennwörtern wird übrigens nach Groß- bzw. Kleinschreibung unterschieden.
Im Folgenden sind einige grundlegende Regeln aufgeführt, die dazu beitragen, dass Ihr System sicherer wird - vorausgesetzt, Sie befolgen diese Regeln:

- Verwenden Sie Kennwörter, die aus mindestens acht Zeichen bestehen. Dabei sollte es sich um alphanummerische Zeichen handeln, die Sie nach Möglichkeit groß schreiben sollten. Damit wird verhindert, dass Utilities verwendet werden, die einfach das Wörterbuch nach dem Server werfen, wenn ein Benutzername entdeckt wird. Wenn Sie diese Regel befolgen, können Sie die Zeit, die erforderlich ist, um das Kennwort eines Benutzers zu knacken, von einer Stunde auf vier Tage erhöhen. Beispiele dafür sind »492je429« und »7382jnne«.
- Weisen Sie Benutzern wann immer möglich Kennwörter zu. So können Sie genau nachvollziehen, was als Kennwort verwendet wird.
- Definieren Sie eine Richtlinie für Kennwörter, die Benutzer auffordert, ihre Kennwörter alle 30 bis 90 Tage zu ändern (siehe Abbildung 11.2).

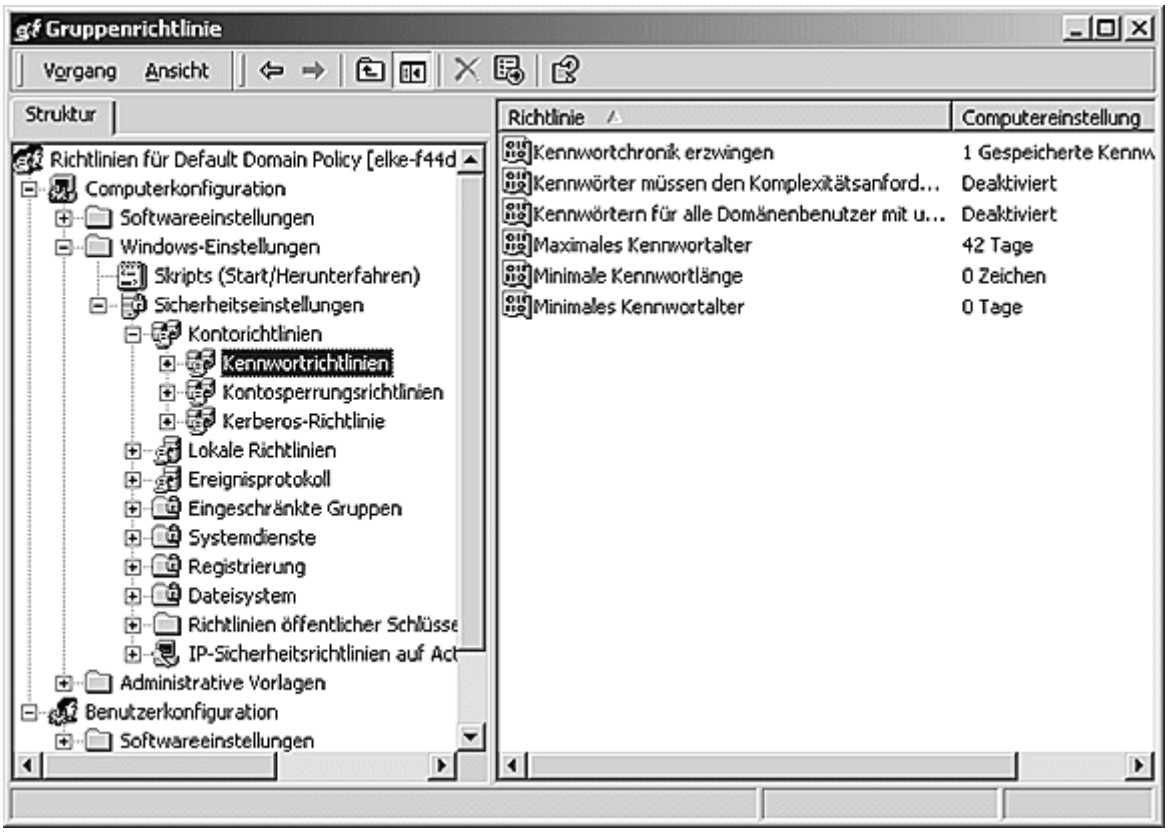


**Abbildung 11.2: Richtlinie für Kennwörter**

- Sorgen Sie für Eindeutigkeit in Bezug auf Kennwörter. Oder anders ausgedrückt: Achten Sie darauf, dass kein Benutzer den Namen seiner Katze als Kennwort verwendet. Lassen Sie darüber hinaus ebenso wenig zu, dass Benutzer zuerst den Namen ihrer Katze, dann den ihres Hundes und anschließend wieder den ihrer Katze verwenden. Das Kennwort sollte über mehrere Iterationen hinweg beibehalten werden.

Um diese Kennwortrichtlinien durchzusetzen, müssen Sie Änderungen in den Gruppenrichtlinien (insbesondere bei den Richtlinien für Kennwörter) für die Benutzer vornehmen, die Sie überwachen möchten. Mit **Default Domain Policy** können Sie die Richtlinie für sämtliche Konten standardmäßig durchsetzen.


Denken Sie immer daran, dass jeder Stein, den Sie den Benutzern in den Weg legen, mehr Arbeit für die Hotline bedeutet. Es ist daher ein schmaler Grad, den Sie gehen müssen, wenn Sie festlegen, ob die Richtlinien eher streng oder in der Anwendung eher einfach sein sollen. Sie werden wohl am meisten zu tun haben, wenn die Kennwörter von allen ablaufen.

Benutzernamen sind nicht annähernd so kompliziert wie Kennwörter. Die schwierigste Entscheidung, die Sie im Zusammenhang mit Benutzernamen treffen müssen, ist die, welche Regel angewendet werden soll, und ob es für das Unternehmen sinnvoll ist, wenn Benutzernamen verwendet werden, die mit den tatsächlichen Namen der Benutzer zu tun haben. Was das betrifft, gibt es grundsätzlich zwei verschiedene Ansichten.
Die eher konventionelle Ansicht in der heutigen, vom Internet geprägten Welt ist die, dass Benutzernamen vergeben werden sollten, die eine Abwandlung des tatsächlichen Namens der Benutzer darstellen. Ein Grund, der für diese Ansicht spricht, ist der, dass Benutzer einfacher erkannt und die Benutzernamen in andere Dienste integriert werden können - die Benutzernamen können den E-Mail-Adressen oder SQL Server-Konten entsprechen.
Das Problem dabei wurde bereits erwähnt. Wenn ein Hacker weiß, dass die Benutzerkonten in Ihrem Unternehmen aus dem ersten Buchstaben des Vornamens und dem Nachnamen (Robert Newton = rnewton) bestehen, weiß er schon die Hälfte dessen, was er wissen muss, um in Ihr System einzudringen.
Die diesem Ansatz entgegenstehende Ansicht ist die, dass für Benutzerkonten ähnlich wie bei den bereits erwähnten Kennwörtern Zahlen oder alphanummerische Namen verwendet werden sollten. Die Idee, die dahinter steckt, ist dieselbe wie die, die sich hinter der Idee von Kennwörtern verbirgt: Je komplexer und unnatürlicher der Benutzername und das Kennwort, um so weniger wahrscheinlich ist es, dass ein Hacker die Kombination knackt.
Das Problem bei diesem System ist allerdings, dass Benutzer sich ihre Kombinationen häufig nicht merken können. Das führt zu einem oder zwei weiteren Problemen:

- Benutzer rufen häufiger bei der Hotline an, da sie sich die Kombination nicht merken können oder weil sie sich bei der Eingabe der Kombination vertippen.
- Benutzer notieren sich ihre Benutzernamen und/oder Kennwörter und geben diese auch an andere weiter. Diese Erfahrung machen und hassen viele Administratoren.


Denken Sie immer daran, dass die häufigste Sicherheitsverletzung im gemeinsamen Netzwerk ein Benutzer ist, der sich am System anmeldet und dann seinen Arbeitsplatz verlässt. Achten Sie daher darauf, dass Bildschirmschoner mit aktiviertem Kennwortschutz spätestens nach 15 Minuten Wartezeit aktiv werden. Dies können Sie übrigens ebenfalls mit Hilfe der Gruppenrichtlinien durchsetzen.

### 11.1.3 Erstellen von Benutzerkonten

Wenn Sie 100 Benutzerkonten erstellen müssen, ist schon allein der Gedanke daran schmerzlich, dies mit Hilfe der Konsole tun zu wollen. Glücklicherweise gibt es eine Lösung zu diesem Problem: net user. Der Befehl net ist ein Allzweckbefehl, der in der Eingabeaufforderung eingegeben wird und mit dem Netzwerkressourcen schnell und effizient genutzt werden können. Mit Hilfe der unterschiedlichen Kombinationen des Befehls net user können Informationen über Benutzerkonten angezeigt und Benutzerkonten erstellt bzw. gelöscht werden.
Die Syntax für den Befehl lautet folgendermaßen:
NET USER [Benutzername [Kennwort | *] [Optionen]] [/DOMAIN]
NET USER Benutzername {Kennwort | *} /ADD [Optionen] [/DOMAIN]
NET USER Benutzername [/DELETE] [/DOMAIN]

Mit jedem Teil dieser Befehle können Sie bestimmte Informationen aufrufen oder einen gewünschten Effekt erzielen. Dieser Befehl ähnelt den Befehlen CD, RD und MD, mit denen Verzeichnisse in der Dateistruktur geändert werden. Im Folgenden ist eine Liste von Parametern mit ihren unterschiedlichen Auswirkungen aufgeführt:

- *Keine Parameter.* Wird der Befehl ohne Parameter verwendet, wird mit Hilfe von net user eine Liste der Benutzerkonten auf dem Computer angezeigt.
- Benutzername. Der Name des Benutzerkontos, das hinzugefügt, gelöscht, geändert oder angezeigt werden soll. Der Name des Benutzerkontos darf maximal 20 Zeichen umfassen.
- Kennwort. Weist dem Benutzerkonto ein Kennwort zu oder ändert es. Das Kennwort muss die mit der Option /MINPWLEN des Befehls NET ACCOUNTS festgelegte Mindestlänge aufweisen. Die maximale Länge beträgt 14 Zeichen.
- *. Es erscheint die Eingabeaufforderung für das Kennwort. Das Kennwort wird bei der Eingabe nicht angezeigt.
- /DOMAIN. Führt den Vorgang auf einem Domänencontroller der aktuellen Domäne aus. Dieser Parameter ist nur auf Windows 2000 Professional-Computern gültig, die Mitglieder einer Windows 2000 Server-Domäne sind. Windows 2000 Server führen standardmäßig Vorgänge auf dem primären Domänencontroller aus.
- /ADD. Fügt ein Benutzerkonto der Benutzerkontendatenbank hinzu.
- /DELETE. Löscht ein Benutzerkonto aus der Datenbank.

Wenn der Befehl mit Optionen angegeben werden kann, wird die Art, wie die Daten geändert werden können, näher definiert. So kann beispielsweise die Option gewählt werden, dass zum neu erstellten Benutzerkonto eine Beschreibung hinzugefügt werden kann. Um eine dieser Optionen hinzuzufügen, ersetzen Sie einfach die Zeile Option in der Syntaxzeile durch die entsprechende Option. Und das sind nun die möglichen Optionen:

- /ACTIVE:{YES | NO}. Deaktiviert oder aktiviert das Konto. Wenn das Konto nicht aktiv ist, kann der Benutzer nicht auf den Server zugreifen. Standardeinstellung ist YES.
- /COMMENT:"Beschreibung". Es kann eine Beschreibung zum Benutzerkonto eingegeben werden. Diese Beschreibung kann bis zu 48 Zeichen umfassen. Der Text muss in Anführungszeichen stehen.
- /COUNTRYCODE:nnn. Verwendet die Landeskennzahl des Betriebssystems, anhand derer die Dateien der Online-Hilfe und der Fehlermeldungen in der

jeweiligen Landessprache angezeigt werden. Bei der Eingabe des Wertes 0 wird die Standardländereinstellung gewählt.

- /EXPIRES:{Datum | NEVER}. Lässt ein Benutzerkonto zum angegebenen Datum ablaufen. Bei Eingabe von NEVER wird keine zeitliche Beschränkung für das Benutzerkonto festgelegt. Ablaufdaten können je nach angegebener Ländereinstellung in der Reihenfolge Monat/Tag/Jahr oder Tag/Monat/Jahr eingegeben werden. Monatsnamen können ausgeschrieben, mit drei Buchstaben abgekürzt oder als Zahlen geschrieben werden. Jahreszahlen können aus zwei oder vier Ziffern bestehen. Als Trennzeichen zwischen Tages-, Monats- und Jahreseingabe müssen Kommata oder Schrägstriche verwendet werden (keine Leerzeichen).
- /FULLNAME:"Name". Definiert den vollständigen Namen des Benutzers (nicht den Benutzernamen). Der Name muss in Anführungszeichen stehen.
- /HOMEDIR:PFAD. Bezeichnet den Pfad für das Basisverzeichnis eines Benutzers. Der Pfad muss bereits existieren.
- /PASSWORDCHG:{YES | NO}. Legt fest, ob Benutzer ihr eigenes Kennwort ändern können. Standardeinstellung ist YES.
- /PASSWORDREQ:{YES | NO}. Legt fest, ob ein Benutzerkonto ein Kennwort haben muss. Standardeinstellung ist YES.
- /PROFILEPATH[:Pfad]. Bezeichnet den Pfad für das Anmeldeprofil des Benutzers. Dieser Pfad verweist auf ein Registrierungsprofil.
- /SCRIPTPATH:Pfad. Bezeichnet den Pfad für das Anmeldeskript des Benutzers. Der Wert Pfad darf kein absoluter Pfad sein. Pfad wird relativ zu %systemroot%\System32\Repl\Import\Scripts angegeben.
- /TIMES:{Zeiten | ALL}. Legt die Anmeldezeiten fest. Die Werte für Zeiten werden in der Form Tag[-Tag][,Tag[-Tag]] ,Uhrzeit[-Uhrzeit][,Uhrzeit[-Uhrzeit]] angegeben, wobei die Angabe der Uhrzeit zu vollen Stunden erfolgen muss. Tage können ausgeschrieben oder abgekürzt werden. Beim 12-Stunden-Format muss nach der Uhrzeit AM, PM oder A.M., P.M. stehen. Bei ALL kann sich der Benutzer jederzeit anmelden. Ein Leerzeichen bewirkt, dass sich der Benutzer überhaupt nicht anmelden kann. Tag und Uhrzeit werden mit einem Komma getrennt, mehrere aufeinander folgende Zeitangaben mit einem Semikolon.
- /USERCOMMENT:"Beschreibung". Hier kann der Administrator eine Beschreibung zum jeweiligen Benutzerkonto eingeben oder ändern. Der Text muss in Anführungszeichen stehen.
- /WORKSTATIONS:{Computername[,...] | *}. Es können bis zu acht Computer angegeben werden, von denen aus sich der Benutzer am Netzwerk anmelden kann. Die unterschiedlichen Einträge werden durch Kommata voneinander getrennt. Wenn nach /WORKSTATIONS nichts oder * angegeben wird, kann sich der Benutzer von jedem Computer aus anmelden.

Diese Befehlszeile verwenden Sie für die Erstellung mehrerer Benutzerkonten am besten, indem Sie ein Beispiel Ihres gewünschten Kontos erstellen und dann in eine Stapelverarbeitungsdatei replizieren. Es kann nicht genügend betont werden, wie wichtig es ist, dass Sie dieses Verfahren ein-, zweimal ausprobieren sollten, bevor Sie die Stapelverarbeitungsdatei mit einer umfangreichen Gruppe von Benutzern füllen. Nach hundert falschen Benutzernamen zu suchen und diese zu berichtigen, kann sehr lästig sein.
So sieht beispielsweise eine Stapelverarbeitungsdatei aus, die Sie verwenden könnten:

```
NET USER bnewton 23nre32 /ADD /COMMENT:"Reisekoordinator"
NET USER jschmo 12nrw53 /ADD /COMMENT:"Reiseplaner"
```

```
NET USER snewton 2v2bt3 /ADD /COMMENT:"Reiseplaner"
NET USER jmeyer hrn598 /ADD /COMMENT:"Reisesekretärin"
```

#### Anmeldeskripten

Anmeldeskripten sind bei einigen Betriebssystemen schwierig zu lernen und anzuwenden. In der Welt von Windows wurden schon immer die guten alten Stapelverarbeitungsdateien verwendet. Die Befehlszeilen-Stapelverarbeitungsdatei gibt es schon seit rund zwei Jahrzehnten. Diese Schnittstelle wird schon seit den frühen Anfängen von DOS und in vielen anderen Betriebssystemen noch heute verwendet.
Eine *Stapelverarbeitungsdatei* ist eine Textdatei, die Befehle enthält, die zeilenweise ausgeführt werden. Wenn ich beispielsweise mit einem Befehl eine Anwendung ausführen, eine Anweisung über die Anwendung zurückübertragen und dann das Ergebnis der Anwendung löschen möchte, sollte ich eine Stapelverarbeitungsdatei erstellen.
Anmeldeskripten sind Stapelverarbeitungsdateien, die verwendet werden, um einen Benutzer in einer Umgebung zu definieren, die das Netzwerk besser nutzbar macht. Benutzern kann mittels Stapelverarbeitungsdatei ein Laufwerk, ein Druckeranschluss oder eine Anwendung zugewiesen werden.
Bei Windows 2000 wurden einige dieser Optionen erweitert. Der wichtigste Unterschied ist der, dass nun Containerobjekten Skripten zugewiesen werden können. Bei Windows NT gibt es so etwas wie *Gruppenanmeldeskripten* nicht. In der Familie der Skripten gibt es außerdem ein neues Mitglied, das so genannte *Abmeldeskript*.
Skripten werden zusammen mit sämtlichen anderen Windows 2000-Richtlinien für Benutzer und Profildaten in der folgenden Reihenfolge ausgeführt:

- Standort
- Domäne
- Organisationseinheit
- untergeordnete Organisationseinheit usw.
- Benutzer

#### Speicherort im Verzeichnis

Skripten können von jeder beliebigen im Netzwerk freigegebenen Datei ausgeführt werden. Der Standardspeicherort von Skripten ist jedoch das Verzeichnis `\WINNT\System32\Repl\Import\Scripts`. Dies liegt in der möglichen Replikation dieser Skripten begründet.
Wenn kein bestimmter Pfad angegeben wird, erhalten die Clients eines Windows 2000- bzw. NT-Servers ihre Anmeldeskripten von dem DC, der sie im Netzwerk authentifiziert. Daher ist es in einem Netzwerk mit mehreren DCs sinnvoll, auf sämtlichen Servern eine aktuelle Liste von Anmeldeskripten zu verwalten. Wenn Sie die Skripten nicht nach jeder Bearbeitung für sämtliche Server kopieren möchten, müssen Sie eine Dateireplikation konfigurieren.
Die einzige Voraussetzung für ein Skript ist, dass darauf über eine Freigabe zugegriffen werden kann. Daher kann die Datei in der Freigabe `\\mcp\scripts` gespeichert und ebenso aufgerufen werden.

Wie bereits erwähnt, handelt es sich bei einem Skript in der Regel um eine Stapelverarbeitungsdatei (**.bat**). Damit Sie sich vorstellen können, wie ein Skript üblicherweise aussieht, sehen Sie sich folgendes Beispiel an:

```
***Beginn des Skripts
echo off
cls
echo Willkommen beim Macmillan Server-Cluster.
echo Die folgenden Ressourcenzuweisungen
echo wurden vorgenommen.
net use f: /home
net use g: \\mcp\data
net use m: \\mcp\apps
net use lpt2 \\mcp\laser_stock3
echo Einen schönen Tag!
pause
```

Mit diesem Skript wird zunächst die Befehlsanzeige ausgeschaltet. Anschließend wird der Bildschirm gelöscht und der Benutzer begrüßt. Darüber hinaus werden dem Benutzer die erstellten Umgebungsvariablen genannt. Abschließend wird dem Benutzer ein schöner Tag gewünscht. Aufgrund der Pause kann der Benutzer lesen, was auf dem Bildschirm steht, bevor er seine Arbeit fortsetzt und sich wundert, warum alles, was an LPT2 gesendet wird, über den Hewlett Packard 4MV ausgedruckt wird.
Ein Skript wird an einem von zwei möglichen Orten gespeichert: im Gruppenrichtlinienobjekt für einen Container bzw. für eine Gruppe oder im Benutzerobjekt. Das hängt natürlich davon ab, welche der Möglichkeiten jeweils am besten geeignet ist.
Bevor Sie nun Skripten erstellen, zunächst einmal ein paar zur Vorsicht mahnende Worte. Das Erstellen von Skripten ist so ähnlich wie das Erteilen von Berechtigungen. Es ist sinnvoller, wann immer möglich, Gruppenrichtlinienskripten zu erstellen. Darüber hinaus ist es immer einfacher, bestimmte Vorgänge für eine Gruppe, statt für jedes Benutzerkonto einzeln zu definieren. Auch Vorgänge für einen einzelnen Benutzer sollten möglichst in einem Gruppenrichtlinienskript definiert werden. Häufig wird das, was zunächst für einen Benutzer erforderlich ist, schon nach kurzer Zeit auch für andere Benutzer relevant.
Wenn Sie ein Gruppenrichtlinienskript zuweisen möchten, beginnen Sie in der Konsole **Active Directory-Benutzer und -Computer**. Gehen Sie dabei wie folgt vor:
1. Klicken Sie mit der rechten Maustaste auf den Container bzw. das Gruppenobjekt, in dem die Gruppenrichtlinie enthalten ist, und wählen Sie dann die Option **Eigenschaften**.
2. Doppelklicken Sie auf der Registerkarte **Gruppenrichtlinie** auf die Gruppenrichtlinie, die Sie ändern möchten. (Wenn keine Gruppenrichtlinie vorhanden ist, müssen Sie eine erstellen, bevor Sie ein Skript zuweisen können.)
3. Klicken Sie auf das Pluszeichen (**+**) neben **Benutzerkonfiguration** und dann auf **Windows-Einstellungen**.
4. Wählen Sie die Option **Skripts (Anmelden/Abmelden)** und doppelklicken Sie anschließend auf das Symbol **Anmelden** bzw. **Abmelden**. Klicken Sie danach auf **Hinzufügen**.
5. Definieren Sie im Dialogfeld **Hinzufügen eines Skripts** die von Ihnen gewünschten Optionen und klicken Sie dann auf **OK**.

- **Skriptname**. Geben Sie den Pfad für das Skript ein oder klicken Sie auf **Durchsuchen**, um die Skriptdatei in der Netlogon-Freigabe auf dem Domänencontroller zu suchen.
- **Skriptparamater**. Geben Sie die gewünschten Parameter ein (wie in der Befehlszeile). Wenn das Skript beispielsweise die Parameter //logo (Vorspann anzeigen) und //I (interaktiver Modus) enthält, geben Sie folgende Zeile ein:
- //logo//I
-

6. Definieren Sie im Dialogfeld **Eigenschaften von Anmelden** bzw. **Eigenschaften von Abmelden** sämtliche von Ihnen gewünschten Optionen:

- **Skripts zum Anmelden für**. Zeigt eine Liste aller Skripten an, die dem ausgewählten Gruppenrichtlinienobjekt derzeit zugewiesen sind. Wenn Sie mehrere Skripten hinzufügen, werden die Skripten in der angegebenen Reihenfolge abgearbeitet. Um ein Skript in der Liste nach oben zu verschieben, klicken Sie zunächst auf das Skript und dann auf **Nach oben**; mit **Nach unten** wird das Skript entsprechend nach unten verschoben.
- **Hinzufügen**. Öffnet das Dialogfeld **Hinzufügen eines Skripts**, in dem Sie weitere Skripten auswählen können.
- **Bearbeiten**. Öffnet das Dialogfeld **Skript bearbeiten**, in dem Sie Skriptdaten wie Name und Parameter ändern können.
- **Entfernen**. Entfernt das ausgewählte Skript aus der Liste der Skripten.
- **Dateien anzeigen**. Hiermit lassen Sie die Skriptdateien anzeigen, die im ausgewählten Gruppenrichtlinienobjekt gespeichert sind.

7. Klicken Sie auf **OK**.

Wenn Sie ein einzelnes Benutzerskript zuweisen möchten, beginnen Sie in der Konsole **Active Directory-Benutzer und -Computer**. Gehen Sie dabei wie folgt vor:
1. Klicken Sie mit der rechten Maustaste auf das Benutzerobjekt und wählen Sie die Option **Eigenschaften**.
2. Wählen Sie die Registerkarte **Profil**.
3. Geben Sie den Namen und den Pfad der Anmeldeskriptdatei ein, wenn sich diese vom Standardspeicherort auf den DCs unterscheidet.
4. Klicken Sie auf **OK**.

**Der Befehl NET**

Ein Administrator, der mit Befehlszeilenanweisungen und Stapelverarbeitungsdateien umgehen kann, tut sich leichter, wenn es darum geht, Skripten zu verstehen. Es kann dennoch vorkommen, dass er die NET-Befehle nicht versteht. Der Befehl NET wird hier zum zweiten Mal in diesem Kapitel erwähnt, da mit diesem Befehl weitaus mehr gemacht werden kann, als nur Benutzerkonten zu erstellen und zu löschen. Der Befehl NET wird für Netzwerkressourcen ohne grafische Benutzeroberfläche verwendet und eignet sich daher hervorragend für Skripten oder jede andere Stapelverarbeitung.
Wenn Sie den Befehl NET verwenden möchten, müssen Sie lediglich NET mit der entsprechenden Variablen eingeben. Wie Benutzerkonten erstellt werden, wurde bereits beschrieben. Daher sollen hier nun einige Variablen genannt werden, die für ein Skript recht hilfreich sein können.
Die unten aufgeführte Liste ist eine unvollständige Liste der Variablen, die zusammen mit dem Befehl NET verwendet werden können, um eine Umgebung zu ändern oder Informationen abzurufen. Sie verwenden die Variablen einfach, indem Sie NET und dann den entsprechenden Befehl eingeben. Zu jeder Variablen ist ein Beispiel angegeben, damit Sie sehen, wie diese verwendet wird. Die Syntax entspricht folgendem Muster:
NET (Variable) (Parameter)

- USE. Verbindet einen Computer mit einer freigegebenen Ressource oder beendet diese Verbindung. Dieser Befehl steuert darüber hinaus auch die Wiederaufnahme von gespeicherten Netzwerkverbindungen. Beispiele:
- NET USE [Gerätename | *] [\\Computername\Freigabename[\Datenträger]] [Kennwort |
- *]] [/USER:[Domänenname\]Benutzername] [[/DELETE] | [/PERSISTENT:{YES | NO}]]
- NET USE Gerätename [/HOME[Kennwort | *]] [/DELETE:{YES | NO}]
- NET USE [/PERSISTENT:{YES | NO}]
-

  Hier nun eine Liste einiger USE-Parameter:

  - Kein. Ohne Parameter zeigt NET USE eine Liste der Netzwerkverbindungen an.
  - Gerätename. Der Name der Ressource, zu der die Verbindung hergestellt oder das Gerät, das getrennt werden soll. Es gibt Gerätenamen für Laufwerke (D: bis Z:) und für Drucker (LPT1: bis LPT3:). Geben Sie einen Stern (*) anstatt eines bestimmten Gerätenamens an, wenn der nächste verfügbare Gerätename verwendet werden soll.
  - \\Servername. Der Name des Servers und der freigegebenen Ressource. Wenn der Computername Leerzeichen enthält, müssen die beiden umgekehrten Schrägstriche (\\) und der Computername in Anführungszeichen eingegeben werden. Die Länge des Computernamens kann 1 bis 15 Zeichen betragen.
  - \Datenträger. Gibt einen NetWare-Datenträger auf dem Server an. Sie müssen den Client Service für NetWare (Windows 2000 Professional) oder den Gateway Service für NetWare (Windows 2000 Server) installiert und aktiviert haben, um eine Verbindung zu NetWare-Servern herstellen zu können.

    - Kennwort. Das Kennwort, mit dem Sie auf eine freigegebene Ressource zugreifen können.
    - *. Erzeugt eine Eingabeaufforderung für das Kennwort. Das Kennwort wird bei der Eingabe nicht angezeigt.
    - /USER. Gibt einen anderen Benutzernamen an, mit dem die Verbindung hergestellt wird.
    - Domänenname. Der Name einer anderen Domäne. NET USE D:\\Server/USER:admin\mariel verbindet beispielsweise die Benutzer-ID »Mariel«, als würde die Verbindung von der Admin-Domäne hergestellt. Ohne Eingabe eines Domänennamens gilt die aktuelle Domäne, an der der Benutzer angemeldet ist.
    - Benutzername. Legt den Benutzernamen fest, mit dem Sie sich anmelden.
    - /DELETE. Beendet eine Netzwerkverbindung. Wenn der Benutzer die Verbindung mit einem Stern angibt, werden sämtliche Verbindungen beendet.
    - /HOME. Verbindet den Benutzer mit seinem Basisverzeichnis.
    - /PERSISTENT. Steuert die automatische Wiederaufnahme von gespeicherten Netzwerkverbindungen. Standardmäßig wird die zuletzt eingestellte Verbindung verwendet.
    - YES. Speichert alle hergestellten Verbindungen und stellt sie bei der nächsten Anmeldung wieder bereit.
    - NO. Aktuelle und nachfolgende Verbindungen werden nicht gespeichert. Nur bestehende Verbindungen werden bei der nächsten Anmeldung wiederhergestellt. Verwenden Sie den Parameter /DELETE, um gespeicherte Verbindungen zu entfernen.
- GROUP. Fügt globale Gruppen auf Windows 2000 Server-Domänen hinzu, zeigt sie an oder ändert sie. Dieser Befehl steht nur auf Windows 2000 Server-Domänencontrollern zur Verfügung. Im Folgenden einige Beispiele:
- NET GROUP [Gruppenname [/COMMENT:"Beschreibung"]] [/DOMAIN]
- NET GROUP Gruppenname {/ADD [/COMMENT:"Beschreibung"] | /DELETE} [/DOMAIN]
- NET GROUP Gruppenname Benutzername [ ...] {/ADD | /DELETE} [/DOMAIN]
-

- HELP. Zeigt eine Liste mit Netzwerkbefehlen und Hilfethemen an. Darüber hinaus bietet dieser Befehl Hilfestellung bei bestimmten Befehlen und Themen. Die zur Verfügung stehenden NET-Befehle sind auch in der Befehlsreferenz im Dialogfeld **Befehle** unter **N** aufgeführt. Klicken Sie in der Windows 2000-Befehlsreferenz auf die Liste **Siehe auch**. Hier einige Beispiele:
- NET HELP [Befehl]
- NET Befehl {/HELP | /?}
-

- SEND. Sendet Nachrichten an andere Benutzer, Computer oder Nachrichtennamen im Netzwerk. Um Nachrichten zu erhalten, muss der Nachrichtendienst aktiv sein. Hier ein Beispiel:
- NET SEND {Name | * | /DOMAIN[:Name] | /USERS} Nachricht
-

- TIME. Synchronisiert die Systemzeit eines Computers mit der eines anderen Computers oder einer Domäne. Ohne die Option /SET wird die Uhrzeit für einen anderen Computer oder eine Domäne angezeigt. Hier ein Beispiel:

- NET TIME [\\Computername | /DOMAIN[:Name]] [/SET]
-

- USER. Wurde bereits beschrieben.
- VIEW. Zeigt Domänen, Computer oder die von einem bestimmten Computer freigegebenen Ressourcen an. Hier einige Beispiele:
- NET VIEW [\\Computername | /DOMAIN[:Domänenname]]
- NET VIEW /NETWORK:NW [\\Computername]
-

**Basisverzeichnis**

Das Basisverzeichnis eines Benutzers ist so etwas wie die Operationsbasis für jeden Benutzer in der Domäne. Es ist keine absolute Notwendigkeit, trägt jedoch dazu bei, dass der Benutzer das Gefühl hat, für seine eigenen Daten einen Speicherort in der Domäne zu haben.
Das Basisverzeichnis eines Benutzers wird auf der Registerkarte **Profil** im Dialogfeld **Eigenschaften** des Benutzerobjekts (siehe Abbildung 11.5) definiert. Bevor ein Basisverzeichnis erstellt werden kann, muss das freigegebene Verzeichnis, in dem das Basisverzeichnis erstellt werden soll, bereits bestehen. Der Administrator muss über Zugriffsberechtigungen verfügen, um in dieses Verzeichnis schreiben zu können und die Freigabe muss verfügbar sein. Außerdem sollte kein Verzeichnis mit dem Anmeldenamen des Benutzers existieren.

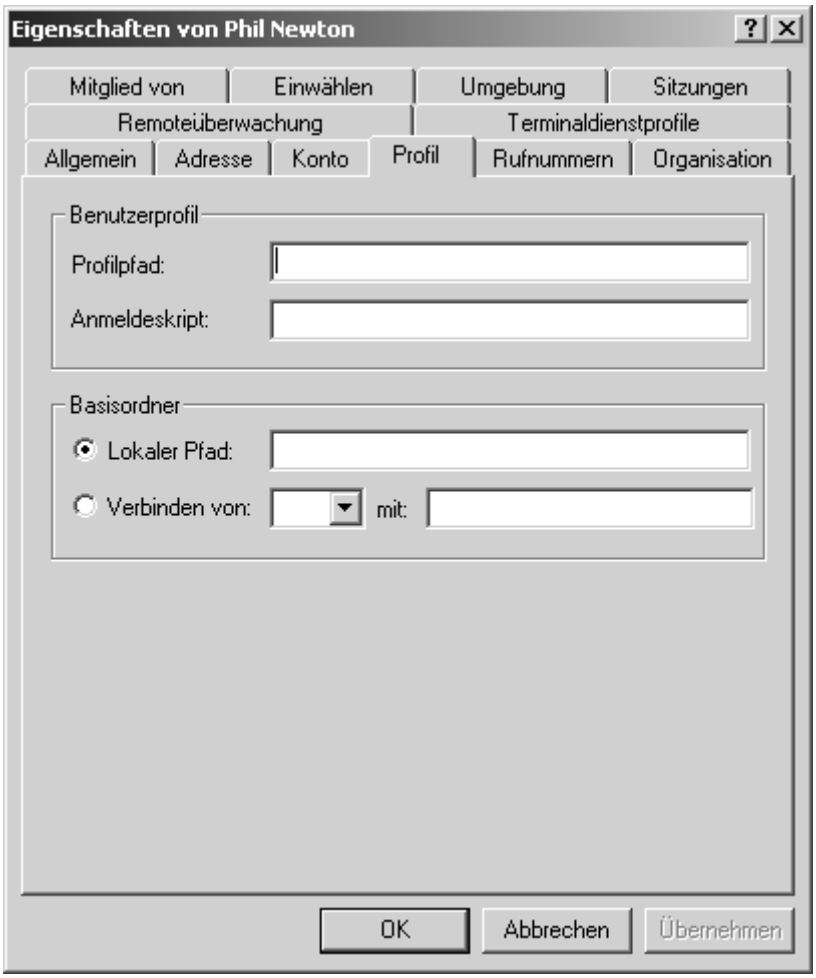


**Abbildung 11.5: Die Registerkarte Profil im Dialogfeld Eigenschaften von [Benutzer]**

Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer**, um ein Basisverzeichnis auf einem Domänen-Server zuzuweisen und gehen Sie dann wie folgt vor:
1. Doppelklicken Sie auf das Benutzerobjekt und aktivieren Sie die Registerkarte **Profil**.
2. Klicken Sie auf das Optionsfeld **Verbinden von**.
3. Wählen Sie in der Dropdown-Liste einen Laufwerkbuchstaben, der verfügbar ist, wenn der Benutzer angemeldet ist. Drücken Sie auf die (Tab)-Taste.
4. Geben Sie die UNC-Adresse des Verzeichnisses ein, das das Basisverzeichnis für diesen Benutzer sein soll, und klicken Sie anschließend auf **OK**.


Die Variable %USERNAME% kann in der UNC-Adresse für die Erstellung des Basisverzeichnisses (\\SERVERNAME\%USERNAME%) verwendet werden. Damit ist es möglich, dass Sie Vorlagen erstellen, die keinen Benutzernamen definieren, sondern Basisverzeichnisse erstellen, wenn ein neuer Benutzer kopiert wird.

#### Profil und Profilpfad

Mit dem Profil eines bestimmten Benutzers wird das Verhalten des Betriebssystems auf dem Arbeitsplatzrechner für diesen Benutzer definiert. Hier werden Software-Einstellungen, Hintergrundbild, Bildschirmschoner, manuelle Laufwerkzuordnungen und viele andere Dinge festgelegt. Wann immer sich ein Benutzer von Windows 2000, NT oder auch 95/98 (falls konfiguriert) an einem neuen System anmeldet, zeichnet dieses System den Benutzernamen auf und beginnt ein Profil für die Einstellungen dieses Benutzers.


Profileinstellungen können durch Richtlinien deaktiviert werden, die bestimmte Verhalten (wenn Sie beispielsweise Benutzern ein eigenes Startmenü zuweisen möchten) nicht zulassen oder diese provozieren. Diese Einstellungen sind kompliziert und werden in Kapitel 12 näher beschrieben.

Der Administrator einer Domäne kann Profile als Werkzeug für die Steuerung sowohl der Domäne als auch des Arbeitsplatzes des lokalen Arbeitsplatzrechners verwenden. Die Idee ist die, dass ein Profil erstellt werden soll, das zu der allen Benutzern präsentierten Umgebung passt und dass dieses Profil dann mit den Benutzern dahin mit wandert, wo diese sich anmelden. Daher wird dieses Profil auch als Roaming-Profil (engl. roaming = wandern) bezeichnet. Roaming-Profile bzw. servergespeicherte Profile können auch zu verbindlichen Profilen gemacht werden. Damit wird das Profil unveränderlich und stellt ein konsistentes und erzwingbares Profil dar.

#### Anmeldung und Kontooptionen

Außer der Umgebung, in der sich der Benutzer befindet, soll auch der Zugriff auf die Domäne gesteuert werden können. Über das Dialogfeld **Eigenschaften** des Benutzerobjekts (siehe Abbildung 11.4) können Sie den Zugriff und das Verhalten, angefangen bei den zulässigen Anmeldezeiten bis hin zu den Computern steuern, an denen man sich anmelden kann.

#### Anmeldezeiten

Die Anmeldezeiten können Sie definieren, indem Sie auf der Registerkarte **Konto** die Schaltfläche **Anmeldezeiten** anklicken (siehe Abbildung 11.6). Wenn Sie auf diese Schaltfläche klicken, können Sie Stunden auswählen, indem Sie auf die Stunden klicken und dann die Option **Anmeldung zulassen** bzw. die Option **Anmeldung verweigern** wählen. Danach wird der Zugriff auf dieser Basis zugelassen bzw. verweigert.

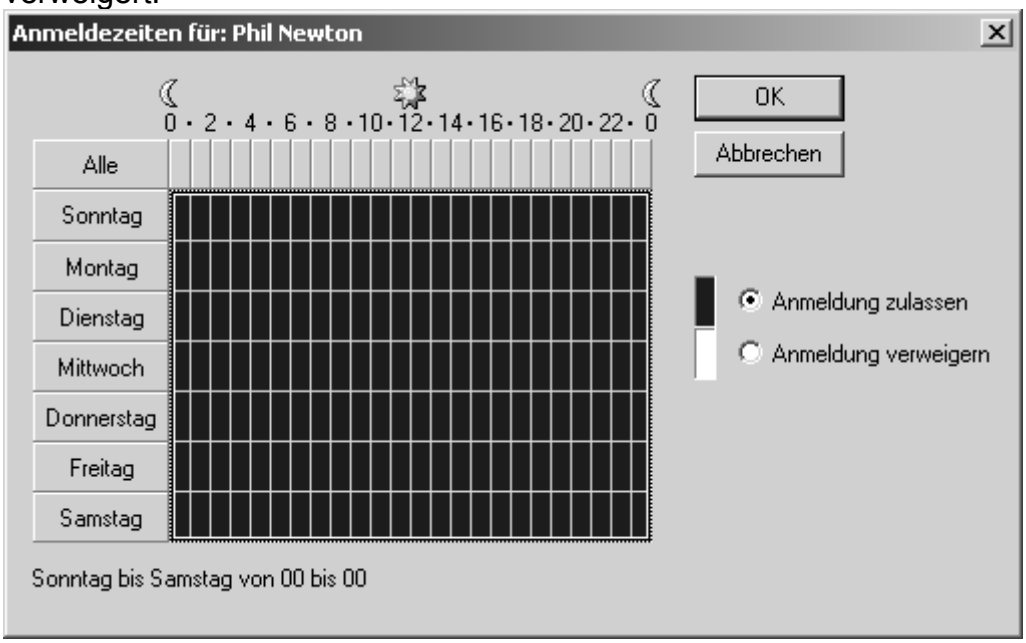


**Abbildung 11.6: Das Dialogfeld Anmeldezeiten für: [Benutzer]**

#### Remote-Zugriff

Den Remote-Zugriff der Benutzer können Sie mit Hilfe der Registerkarte **Einwählen** (siehe Abbildung 11.7) einzeln überwachen. Hier können Sie den Zugriff gestatten oder verweigern, indem Sie entweder die Option **Zugriff gestatten** oder die Option **Zugriff verweigern** wählen.

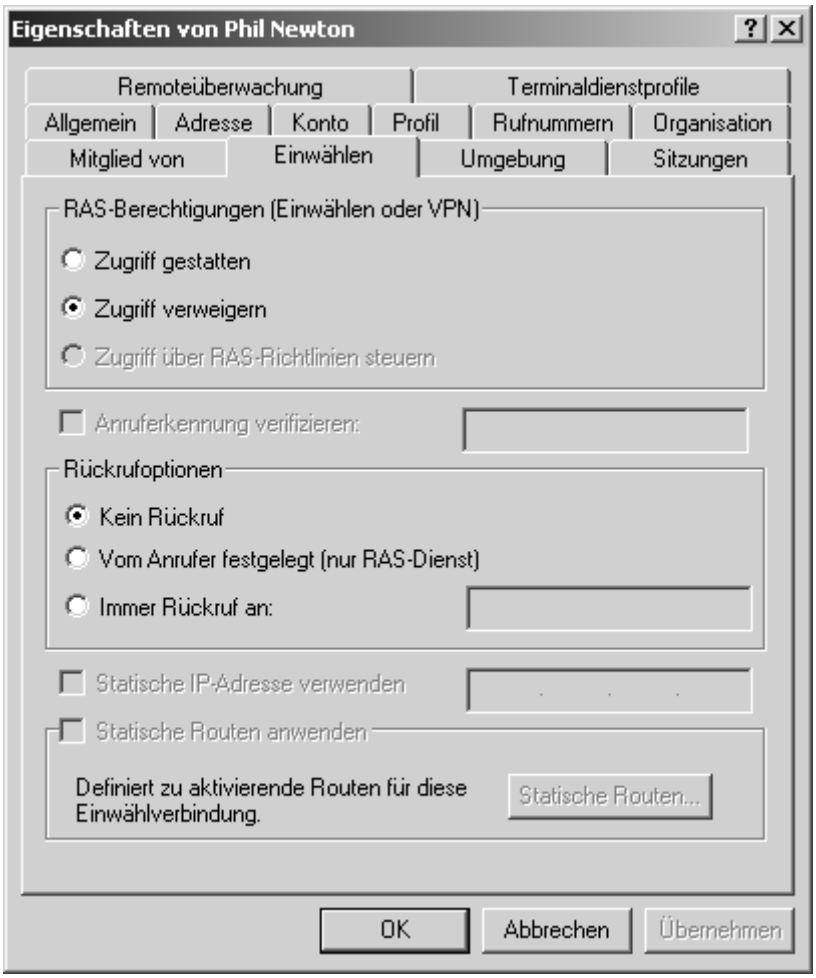


**Abbildung 11.7: Die Registerkarte Einwählen im Dialogfeld Eigenschaften von [Benutzer]**

Die andere hier zur Verfügung stehende Option dient der Sicherheit. Dabei handelt es sich um *Rückrufoptionen*. Die Idee dabei ist die, dass der Server Benutzer, die sich im Netzwerk einwählen, zurückruft, um sicher zu stellen, dass diese auch tatsächlich die Benutzer sind, die sie vorgeben zu sein bzw. dass diese sich an einem bereits geprüften Standort befinden.
Am sichersten ist es, wenn das System den Anrufer immer über eine bestimmte Rückrufnummer zurückruft. Es ist jedoch auch möglich, dass der Anrufer eine Rückrufnummer festlegt. Dabei geht es darum, dass der Benutzer wissen muss, dass die Rückrufoption erforderlich ist. Diese Option bietet allerdings auch die Flexibilität, dass einer Ihrer Benutzer zu einem Konkurrenten Ihres Unternehmens wechselt und von dort aus Ihre Kundenliste herunterlädt. Das ist natürlich unsinnig.

#### Computer-Einschränkungen

Es ist darüber hinaus auch möglich, den Computer zu schützen, auf den ein Benutzer über die Domäne zugreifen kann. Wenn beispielsweise ein Praktikant angestellt wird, der nur an seinem PC arbeiten soll, können Sie der Domäne mitteilen, dass sich der Praktikant nur über seinen PC anmelden darf. Wenn Sie sich vor Augen führen, dass die größte Bedrohung für die Sicherheit ein unbeaufsichtigter, angemeldeter Arbeitsplatzrechner ist, dann dürfte klar sein, wie wichtig diese Sicherheitsvorkehrung ist.

Die entsprechende Änderung können Sie im Dialogfeld **Eigenschaften** des Benutzers auf der Registerkarte **Konto** vornehmen, indem Sie auf die Schaltfläche **Anmelden** klicken (siehe Abbildung 11.8).


**Abbildung 11.8: Das Dialogfeld Anmeldearbeitsstationen**

Wenn Sie sich in diesem Dialogfeld befinden, geben Sie einfach den Namen des Computers ein, an dem sich der Benutzer anmelden darf, und klicken dann auf die Schaltfläche **Hinzufügen**.

#### Kontooptionen

Mit vielen der Optionen auf der Registerkarte **Konto** können unterschiedliche Arten von Konten gesteuert werden.
Mit den Kontooptionen auf dieser Registerkarte können viele Dinge gestattet bzw. verweigert werden. Die folgende Ausführung soll dazu beitragen, dass Sie diese Optionen verstehen und wissen, warum diese verwendet werden:

- **Benutzer muss Kennwort bei nächster Anmeldung ändern**. Der Benutzer wird aufgefordert, ein neues Kennwort zu verwenden, wenn er sich das erste Mal anmeldet. Damit soll ermöglicht werden, dass Sie zwar bei einer Einführung Kennwörter vergeben, die Benutzer die Kennwörter von da an jedoch selbst definieren. Damit wird die Sicherheit verstärkt, indem jeder Einzelne die Verantwortung für diese Aufgabe innerhalb seiner eigenen Konten selbst übernimmt.
- **Benutzer kann das Kennwort nicht ändern**. Wenn Sie sämtliche Kennwörter verwalten, muss diese Option gewählt werden, um zu verhindern, dass Benutzer ihre Kennwörter selbst ändern.
- **Kennwort läuft nie ab**. Das ist das Kennzeichen eines Unternehmens mit geringem Sicherheitsbedürfnis oder eines faulen Administrators. Damit gibt es aber natürlich weniger Nachfragen nach Kennwörtern.

- **Kennwort mit reversibler Verschlüsselung speichern**. Diese Option wird für Macintosh-Clients verwendet, die sich mit einem Apple-Client anmelden. Wenn sich Macintosh-Clients mit der Auswahl anmelden, muss diese Option aktiviert sein.
- **Das Konto ist deaktiviert**. Diese Option wird verwendet, um das Konto vorübergehend zu deaktivieren. Wenn ein Konto gelöscht werden soll, ist es besser, das Konto zunächst nur zu deaktivieren. Nehmen wir beispielsweise einmal an, Ihr Vorgesetzter sagt Ihnen, Sie sollen Pauls Konto löschen, weil Paul entlassen wird. Wenn Sie jedoch sehen, wie Paul aus dem Büro des Vorgesetzten mit einem Lächeln herauskommt und der Vorgesetzte und Paul einander die Hände schütteln, haben Sie bestimmt Zeit gespart, da Sie Pauls Konto nicht neu zu erstellen brauchen. Wenn Paul jedoch tatsächlich entlassen wird, dann können Sie sein Konto immer noch löschen.
- **Benutzer muss sich mit einer Smartcard anmelden**. Mit Hilfe von Smartcards ist es möglich, dass das System jedes Mal, wenn sich ein Benutzer anmeldet, ein anderes Kennwort verwendet. Diese Option ermöglicht es dem Administrator, ausschließlich diese Art der Anmeldung zu verwenden.
- **Konto wird für Delegierungszwecke vertraut**. Mit diesem Konto können anderen Konten Berechtigungen innerhalb des Verzeichnisses zugewiesen werden.
- **Konto kann nicht delegiert werden**. Damit wird festgelegt, dass dem Konto kein delegierter Teil des Verzeichnisses zugewiesen werden kann. Sie mögen sich fragen, warum nicht einfach die Berechtigung delegiert wird. Mit dieser Option kann ein Administrator in einer großen Umgebung einen anderen warnen und damit verhindern, dass ein Konto delegiert wird.
- **DES-Verschlüsselungstypen für dieses Konto verwenden**. Aktivieren Sie diese Option, wenn Sie die DES-Unterstützung (Data Encryption Standard) aktivieren möchten. DES unterstützt mehrere Verschlüsselungsebenen.
- **Keine Kerberos-Präauthentifizierung erforderlich**. Aktivieren Sie diese Option, wenn das Konto eine andere Implementierung des Kerberos-Protokolls verwendet. Nicht alle Implementierungen oder Varianten des Kerberos-Protokolls unterstützen diese Funktion. Das Kerberos Key Distribution Center (Schlüsselverteilungscenter) verwendet für die Zuweisung der Netzwerkauthentifizierung innerhalb einer Domäne ticketgenehmigende Tickets. Der Zeitpunkt, zu dem ein ticketgenehmigendes Ticket vom Schlüsselverteilungscenter ausgegeben wird, ist für das Kerberos-Protokoll von Bedeutung. Windows 2000 verwendet andere Mechanismen zur Zeitsynchronisierung, sodass auch die Kerberos-Präauthenitifizierung eingesetzt werden kann.

Die letzte Option auf der Registerkarte **Konto** dient lediglich dazu, für ein Konto ein Ablaufdatum festzulegen. Damit können temporäre Konten erstellt werden. Das ist dann recht nützlich, wenn für Zeitarbeiter oder Praktikanten Konten eingerichtet werden, die bei all den anderen verwaltungstechnischen Aufgaben leicht in Vergessenheit geraten können.
Die Anwendung dieser Option ist so einfach wie sie aussieht. Sie legen das Ablaufdatum fest, indem Sie einfach das Optionsfeld **Am** aktivieren und dann ein Datum angeben. Nach Ablauf dieses Tages kann sich der Benutzer nicht mehr am System anmelden.

## 11.2 Datenträgerkontingente

Das Netzwerkbetriebssystem Windows benötigt schon seit längerem eine Steuerungsfunktion der durch ständig anwachsende Benutzerzahlen kontinuierlich zunehmenden Nutzung der Festplatte. In Windows 2000 gibt es nun diese Funktion. Sie wird von einem Datenträger aus implementiert und stellt keine völlige Benutzerbeschränkung dar, wie das bei NetWare der Fall ist. Sie bietet jedoch weitaus bessere Steuerungsmöglichkeiten.
Um eine Beschränkung des Datenträgerkontingents zu definieren, müssen Sie zunächst einmal die Kontingentverwaltung auf dem Datenträger aktivieren. Dazu gehen Sie wie folgt vor:
1. Klicken Sie auf dem Server mit der rechten Maustaste auf das Symbol des Datenträgers und wählen Sie dann die Option **Eigenschaften**.
2. Aktivieren Sie die Registerkarte **Kontingent** (siehe Abbildung 11.9).

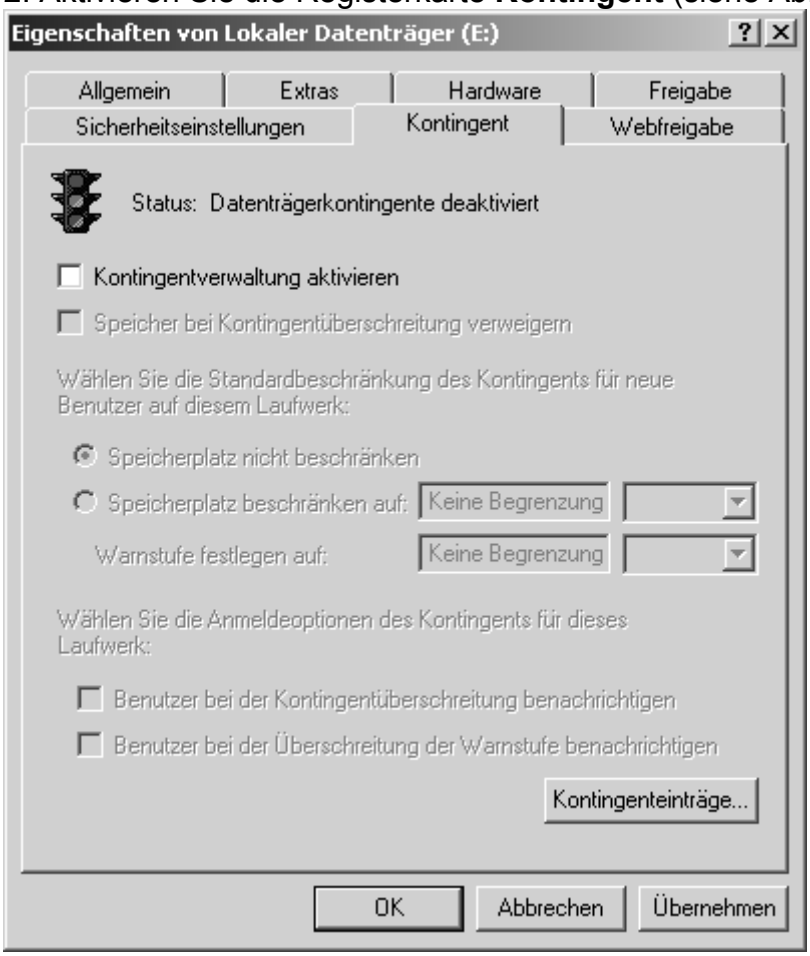


**Abbildung 11.9: Die Registerkarte Kontingent im Dialogfeld Eigenschaften von [Datenträger]**

3. Aktivieren Sie das Kontrollkästchen **Kontingentverwaltung aktivieren**.
4. Klicken Sie auf **OK**.

Wenn Sie das erledigt haben, können Sie damit beginnen, Kontingente zu definieren. Im ersten Dialogfeld sind viele Einstellungen vorzunehmen, noch bevor Sie die eigentlichen Kontingente festlegen. Dabei handelt es sich um Anweisungen an das System in Bezug darauf, wie mit möglichen Überschreitungen der Kontingente umgegangen werden soll:

- **Speicher bei Kontingentüberschreitung verweigern**. Mit dieser Option wird verhindert, dass Benutzer weiter Daten auf dem Datenträger speichern, wenn sie das ihnen zugewiesene Kontingent überschreiten. Daraus könnte geschlossen werden, dass der Benutzer allein dadurch gestoppt wird, dass Sie eine Beschränkung definieren. Das ist jedoch nicht der Fall. Indem Sie Grenzen setzen, errichten Sie lediglich eine Schwelle für das Auslösen einer Reihe von Reaktionen, von denen eine verhindert, dass ein Benutzer Daten auf einem Datenträger speichert, wenn das Kontingent überschritten ist.
- **Wählen Sie die Standardbeschränkung des Kontingents für neue Benutzer auf diesem Laufwerk**. Mit den hier zur Verfügung stehenden Optionen stellen Sie sicher, dass für Benutzer eine Beschränkung definiert ist, falls für diesen keine Beschränkung manuell konfiguriert wurde.
- **Wählen Sie die Anmeldeoptionen des Kontingents für dieses Laufwerk**. Mit den hier gewählten Optionen können Sie festlegen, was geschehen soll, wenn ein Benutzer das Kontingent überschritten hat. Sie können damit Benutzer warnen, falls sie die Grenze ihres Kontingents erreichen.

Um ein neues Kontingent zu definieren, öffnen Sie zunächst das Dialogfeld **Eigenschaften** des Laufwerks und aktivieren die Registerkarte **Kontingent**. Gehen Sie dann wie folgt vor:
1. Klicken Sie auf die Schaltfläche **Kontingenteinträge**.
2. Klicken Sie anschließend auf **Kontingent** und wählen Sie dann die Option **Neuer Kontingenteintrag**.
3. Wählen Sie aus dem Dropdown-Menü **Suchen in** die Domäne aus, die den Benutzer oder die Gruppe enthält, deren Kontingent beschränkt werden soll.
4. Klicken Sie auf den Benutzer- oder Gruppeneintrag und dann auf die Schaltfläche **Hinzufügen**. Wiederholen Sie diesen Schritt, bis sich alle gewünschten Benutzer- bzw. Gruppenobjekte im unteren Feld befinden. Klicken Sie auf **OK**.
5. Wählen Sie in dem nun erscheinenden Dialogfeld **Kontingenteinträge** die Option **Speicherplatz beschränken auf** und geben Sie dann die Werte für den Speicherplatz und die Warnstufe ein (siehe Abbildung 11.10).
6. Klicken Sie auf **OK** und schließen Sie die Konsole **Kontingenteinträge**.

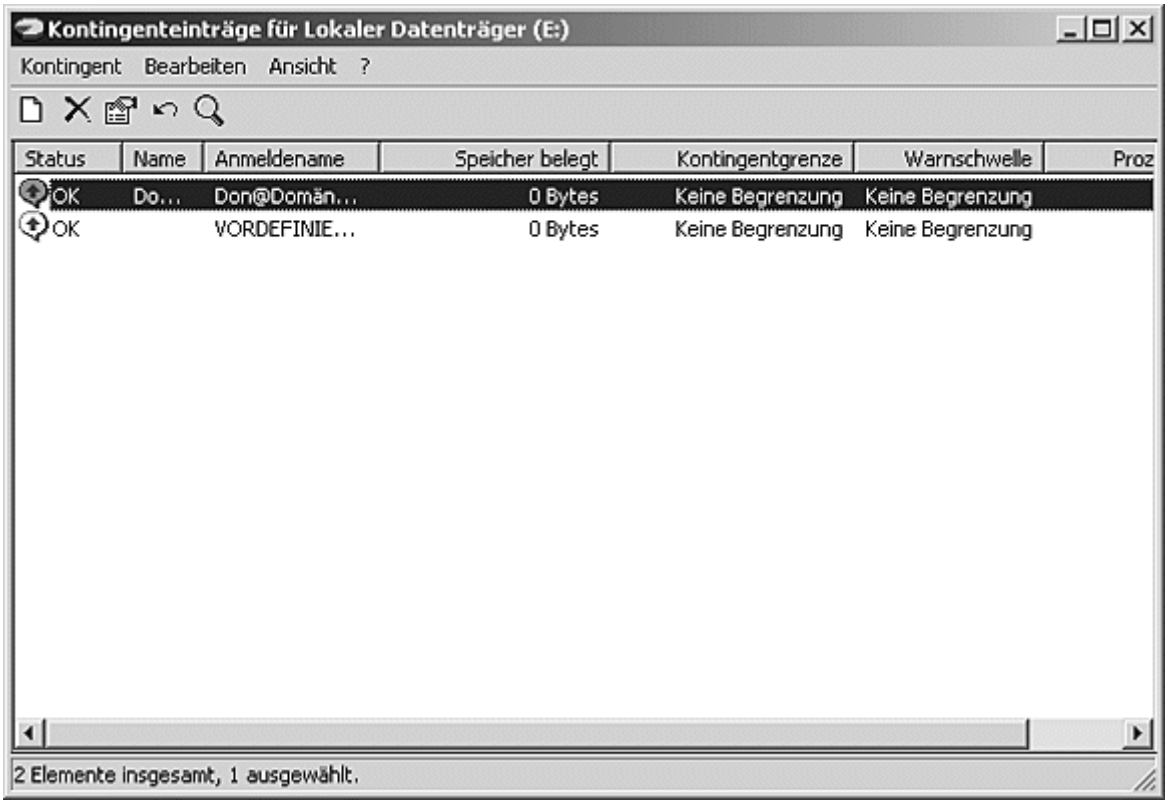


**Abbildung 11.10: Die Konsole Kontingenteinträge**

## 11.3 Gruppen

Gruppen von Benutzerkonten bei Windows 2000 bedeuten die Zusammenfassung von Benutzerkonten, um gleichzeitig mehrere Benutzerkonten überwachen zu können. Das ist wie bei Viehherden: Es dürfte ziemlich aufwändig sein, jede Kuh einzeln auf die Weide zu treiben. Daher sollten Sie sich, wenn Sie mit der Verwaltung von Benutzern beginnen, als Erstes darum kümmern, Benutzer zu Gruppen zusammenzufassen.

### 11.3.1 Gruppenbereich

Unter *Gruppenbereich* versteht man die Stelle im Verzeichnis, die der Gruppe zugewiesen wird, sowie mögliche Mitgliedschaften der Benutzer. Es gibt drei Gruppenbereiche: »Lokale Domäne«, »Global« und »Universal«.
Die Auswahl des Gruppenbereichs hängt vom Betriebsmodus ab, in dem sich das Sicherheitssystem derzeit befindet. Wenn sich die Domänencontroller im gemischten Modus befinden, stehen nur die Gruppenbereiche »Lokale Domäne« und »Global« zur Verfügung. Das kommt daher, weil Windows NT die Verschachtelung von Gruppen nicht zulässt. Im einheitlichen Modus sind alle drei Optionen verfügbar und Gruppen können Mitglieder von Gruppen sein, d.h., die Verschachtelung von Gruppen ist möglich.

**Gruppenbereich »Lokale Domäne«**

Der Gruppenbereich »Lokale Domäne« in Active Directory (Windows 2000) ist die Reinkarnation der guten alten lokalen Gruppen von Windows NT. Wenn lokale

Gruppen von Windows NT übernommen werden, werden diese zu Gruppen der lokalen Domäne.
Gruppen der lokalen Domäne werden verwendet, um Ressourcen in der lokalen Domäne zu verwalten. Darin unterscheiden sich diese Gruppen von den alten lokalen Gruppen ein wenig. Dennoch ähneln sich diese beiden Gruppen in ihrer Grundkonzeption. Eine Gruppe der lokalen Domäne kann folgende Mitglieder enthalten:

- Gruppen mit dem Bereich »Global«
- Gruppen mit dem Bereich »Universal« (nur im einheitlichen Modus)
- Benutzerkonten
- andere Gruppen mit dem Bereich »Lokale Domäne« (nur im einheitlichen Modus)
- eine beliebige Kombination der oben genannten Objekte (abhängig vom Modus)

Die Idee, die dahinter steckt, ist die, dass Gruppen der lokalen Domäne verwendet werden, um darin Konten und Gruppen unterzubringen, die eine bestimmte Ressource gemeinsam nutzen. Wenn die Gruppe für die Ressource erstellt ist und die Konten zur Gruppe hinzugefügt sind, ist es einfach, Benutzer hinzuzufügen und in Erfahrung zu bringen, welche Benutzer bzw. Gruppen Zugriff auf die Ressource haben, indem man einfach in der Gruppe der Ressource nachsieht.
Wenn Sie die gesamte Gruppe der Buchhaltung zu den Gruppen hinzufügen müssen, die auf die Laufwerkfreigabe *Servername**Buchhaltung* zugreifen dürfen, ist es am einfachsten, die Gruppe Rechnungswesen zu erstellen und die globale Gruppe Buchhaltung zur Gruppe der Ressource zuzuweisen. Wenn mit der Freigabe eigenartige Dinge geschehen, ist es nun einfacher festzustellen, wer Zugriff auf die Freigabe hatte und Änderungen lassen sich leichter vornehmen.

**Gruppenbereich »Global«**

Eine globale Gruppe ist bei Windows 2000 nicht dasselbe wie bei Windows NT. Sie wird jedoch sehr ähnlich verwendet. Eine Gruppe mit dem Bereich »Global« ist eine Gruppe, die für das tägliche Hinzufügen von Benutzern oder anderen Gruppen zu Gruppen, denen später Ressourcen zugewiesen werden, verwendet wird.
Die Schlüsselwörter hier sind *Benutzer* und *täglich*. Eine globale Gruppe unterscheidet sich von einer universellen Gruppe dadurch, dass die globale Gruppe nicht über die Grenzen der Domäne hinaus repliziert werden kann. Außerdem kann eine globale Gruppe keine Mitglieder von außerhalb der Domäne haben. Eine globale Gruppe kann folgende Mitglieder enthalten:

- Globale Gruppen aus ihrer eigenen Domäne (nur im einheitlichen Modus)
- Benutzerkonten
- Eine beliebige Kombination der oben genannten Objekte (abhängig vom Modus)

Wenn die Mitgliedschaft von globalen Gruppen geändert wird oder wenn die einer globalen Gruppe zugewiesenen Berechtigungen geändert werden, werden diese Änderungen nur innerhalb der Domäne repliziert.
Aus diesem Grund ist es sinnvoll, Benutzer globalen Gruppen und dann die globalen Gruppen den Gruppen der lokalen Domäne zuzuweisen, die den Zugriff auf die

Ressourcen steuern. Das Problem dabei ist jedoch, dass im gemischten Modus globale Gruppen von anderen Domänen nicht zu globalen Gruppen zugewiesen werden können, die erstellt worden sind, um sämtliche Benutzer zusammenzufassen.

**Gruppenbereich »Universal«**

Gruppen mit dem Bereich »Universal« stehen nur im Domänenmodus zur Verfügung. Universelle Gruppen in ihrer reinsten Form kann man sich als domänenübergreifende Lösung für Gruppen vorstellen, die Domänengrenzen überschreiten müssen. Es ist verlockend, sich universelle Gruppen als »magische« lokale Gruppen vorzustellen, die die Grenzen von Domänen überschreiten können. Universelle Gruppen können folgende Mitglieder enthalten:

- globale Gruppen aus einer beliebigen Domäne
- Gruppen mit dem Bereich »Universal«
- Benutzerkonten

Am besten ist es, wenn diese universellen Gruppen erstellt, diesen die globalen Gruppen zugewiesen und dann die universellen Gruppen der Gruppe der lokalen Domäne zugewiesen werden, die für die Ressource verantwortlich ist.

**Untergliederung der Gruppen**

Administratoren von lokalen Domänen können Benutzer zu den globalen Gruppen hinzufügen. Da diese globalen Gruppen Mitglieder der universellen Gruppen sind, die über Berechtigungen für den Zugriff auf die Ressource verfügen, haben die Mitglieder die Berechtigungen, die sie benötigen.
Für die domänenübergreifende Replikation sind lediglich die Namen der globalen Gruppen erforderlich, die den universellen Gruppen angehören. Da diese Mitgliedschaft sehr selten geändert werden muss, kommt es praktisch nicht zur Replikation. Domäneninterne Replikationen kommen vor, sind jedoch auf die Mitglieder der Domäne beschränkt.
Die Gruppen der lokalen Domäne tragen dazu bei, dass der lokale Administrator einen genauen Überblick über die Gruppen und Benutzerkonten hat, die Zugriff auf die Ressourcen haben. Darüber hinaus erleichtern diese Gruppen das Entfernen und Hinzufügen von Gruppen, da nicht jede einzelne Gruppe, der Berechtigungen zugewiesen worden sind, gesucht werden muss.

### 11.3.2 Erstellen einer neuen Gruppe

Um eine Gruppe zu erstellen, gehen Sie wie folgt vor:
1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** und wählen Sie das Containerobjekt, zu dem Sie das Gruppenobjekt hinzufügen möchten. Dies kann der Benutzercontainer für die Domäne oder eine beliebige Organisationseinheit sein, die bereits erstellt ist.
2. Klicken Sie mit der rechten Maustaste auf das Containerobjekt und wählen Sie dann die Optionen **Neu** und **Gruppe**.
3. Geben Sie den Namen der neuen Gruppe ein und drücken Sie dann auf die (Tab)-Taste.
4. Geben Sie, falls erforderlich, den Gruppennamen für Clients mit älteren Windows-Versionen ein und drücken Sie dann auf die (Tab)-Taste.

5. Geben Sie den Gruppenbereich ein.
6. Klicken Sie auf **OK**.

### 11.3.3 Vordefinierte Standardgruppen

Wie Benutzerkonten, so verfügt auch das Betriebssystem Windows 2000 über vordefinierte Gruppen, die verfügbar werden, wenn ein Computer und/oder eine Domäne eingerichtet wird. Diese Gruppen werden als eine Art öffentliche Gruppenfunktion erstellt. Die grundlegenden Funktionen der Domäne gehören zu diesen Gruppen.
Einige der Gruppen sind Teil von Windows 2000 in jeder Form (Arbeitsgruppe oder Domäne), während andere erst erstellt werden, wenn eine Domäne eingerichtet wird. Darüber hinaus gibt es so genannte *implizite Gruppen*, die nur für die zugewiesenen Berechtigungen verfügbar sind. Zu diesen Gruppen können keine Mitglieder hinzugefügt werden. Sie sind außerdem in der Konsole **Active Directory-Benutzer und -Computer** nicht zu sehen. Das kommt daher, weil sie vom Betriebssystem ausschließlich für das Betriebssystem erstellt werden. Wenn Sie sich die Beschreibungen der Gruppen einmal durchlesen, wird deutlich, wozu diese Gruppen benötigt werden.
Im Folgenden sind nun die vordefinierten Gruppen aufgeführt:

- *Konten-Operatoren (nur Domäne)*. Mitglieder dieser Gruppe können die Benutzer- und Gruppenkonten auf dem lokalen Computer ändern. Domänenbenutzer und Gruppen gehören nicht dazu.
- *Administratoren (Domäne und lokal)*. Mitglieder dieser Gruppe können sämtliche Aufgaben auf dem lokalen Computer ausführen. Mitglieder dieser Gruppe auf dem Domänencontroller sollten Mitglieder der Gruppe für alle Computer in der Domäne sein.
- *Sicherungs-Operatoren (Domäne und lokal)*. Mitglieder dieser Gruppe dürfen Dateien und Ordner des Systems sichern und wiederherstellen. Sie dürfen außerdem das System herunterfahren.
- *Ersteller-Besitzer (implizit)*. Der Ersteller eines Objekts (Datei, Druckauftrag, Ordner usw.) wird automatisch Mitglied der Gruppe Ersteller-Besitzer für dieses Objekt. Damit verfügt der Benutzer über sämtliche Berechtigungen für das Objekt.
- *Jeder (implizit)*. Eine integrierte und transparente Gruppe, die sämtliche im System authentifizierten Benutzer enthält. Der Unterschied zwischen den Gruppen Benutzer und Jeder ist der, dass die Gruppe Benutzer Mitglieder der Domäne sind, während die Gruppe Jeder lokale Benutzer und/oder Domänenbenutzer enthält. Denken Sie daran, dass anonyme Benutzer über den IIS-Server ebenfalls dazu gehören.
- *Gäste (Domäne und lokal)*. Mitglieder dieser Gruppe dürfen auf alle Ressourcen zugreifen, auf die die Gruppen Jeder und Benutzer zugreifen dürfen.
- *Interaktiv (implizit)*. Jeder Benutzer, der an einem System lokal angemeldet ist.
- *Netzwerk (implizit)*. Jeder über das Netzwerk angemeldete Benutzer. Beachten Sie, dass anonyme Benutzer über den IIS-Server ebenfalls dazu gehören.
- *Druck-Operatoren (nur Domäne)*. Mitglieder dieser Gruppe dürfen sämtliche Druckerfunktionen steuern, d.h., sie dürfen Drucker freigeben, Drucker löschen und Druckaufträge starten, beenden und löschen.

- *Replikations-Operator (Domäne und lokal)*. Mitglieder dieser Gruppe dürfen Verzeichnisreplikationsaufträge erstellen, löschen und verwalten.
- *Server-Operatoren (nur Domäne)*. Mitglieder dieser Gruppe sind eigentlich Administratoren ohne die Kompetenzen von Konten-Operatoren. Server-Operatoren können sowohl Datei- als auch Druckerfreigaben steuern, erstellen und löschen. Sie sichern Dateien und stellen diese vom Server wieder her, aber sie können keine Berechtigungen für diese Aufgaben erteilen.
- *Benutzer (Domäne und lokal)*. Diese Gruppe ist eine lokale Gruppe auf dem Computer, auf dem diese Gruppe eingerichtet ist. Mitglieder sind sämtliche Benutzerkonten, die auf dem Computer erstellt wurden, und die Domänengruppe Domänenbenutzer, wenn der Computer Mitglied einer Domäne ist.
- *Domänen-Admins (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Administratoren der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind, und können darüber hinaus alles in der Domäne, in der Struktur und in der vertrauenden Gesamtstruktur steuern.
- *Domänencomputer (nur Domäne)*. Sämtliche in der Domäne erstellten Computerkonten werden automatisch Mitglied dieser Gruppe. Diese Gruppe kann an sämtliche Konten von Domänencomputern Änderungen vornehmen und für sämtliche Konten von Domänencomputern Eigenschaften festlegen.
- *Domänencontroller (nur Domäne)*. Sämtliche in der Domäne installierten Domänencontroller werden automatisch Mitglied dieser Gruppe. Diese Gruppe kann an sämtlichen Konten von Domänencontrollern Änderungen vornehmen und für sämtliche Konten von Domänencontrollern Eigenschaften festlegen.
- *Domänen-Gäste (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Gäste der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind.
- *Domänen-Benutzer (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Benutzer der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind.
- *Organisations-Admins (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Administratoren der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind, und können darüber hinaus alles in der Domäne, in der Struktur und in der vertrauenden Gesamtstruktur steuern.
- *Gruppenrichtlinien-Admins (nur Domäne)*. Mitglieder dieser Gruppe haben die Berechtigung, Gruppenrichtlinien innerhalb der Domäne zu bearbeiten und zu prüfen.
- *Schema-Admins (nur Domäne)*. Mitglieder dieser Gruppe können die Informationen im Schema bearbeiten. Dieses Active Directory-Schema kann verwendet werden, um Informationen zu speichern. Darüber hinaus kann es auch bearbeitet werden, um weitere Ressourcen innerhalb des Schemas zu definieren.
- *System (implizit)*. Vom Betriebssystem durchgeführte Operationen.