

Administratoren haben häufig die Anforderung, routinemäßige oder umfangreiche Aufgaben zu automatisieren. Windows NT stellt zu diesem Zweck einen Interpreter auf Kommandozeilenebene zur Verfügung, mit dem sich einfache Skripten erstellen lassen.

DIRK PELZER

Der erste Teil dieser Serie befaßte sich mit allgemeinen Skriptbefehlen, wie zum Beispiel der FOR-Schleife oder dem Abprüfen von Bedingungen über das IF-Kommando. Diesmal werden Kommandos und Methoden aufgezeigt, die sich mit der Benutzer- und Rechteverwaltung beschäftigen.

Das NET-Kommando

Im Zusammenhang mit dem Erstellen von Benutzerkonten und Gruppen spielt der Befehl *NET.EXE* eine zentrale Rolle. Dieser verfügt über zahlreiche Parameter, mit denen der Administrator zum Beispiel Benutzer anlegen oder aber auch Verzeichnisse freigeben kann. Um eine Liste aller verfügbaren NET-Kommandos zu erhalten, führt man von einer Kommandozeile den Befehl *NET /?* aus. Benötigt man eine Beschreibung über die Funktion und zu verwendende Parameter eines NET-Kommandos, gibt man einfach den Befehl *NET HELP <Kommandoname>* ein, so wie in Bild 1 dargestellt:

Benutzerkonten anlegen

Eine sehr häufig anzutreffende Aufgabe bei Aufbau und Wartung eines NT-Netzes ist das Anlegen von Benutzergruppen und Benutzerkonten, die dann wiederum Gruppen zugeordnet werden können. Um einen Benutzer anzulegen, setzt man den Befehl *NET USER* ein. Mit diesem hat der Administrator die Möglichkeit, Benutzerkonten auf dem Primären-Domänen-Controller (PDC) und auf NT-Workstations anzulegen, zu modifizieren oder zu löschen. Ruft man *NET USER* ohne zusätzliche Parameter auf, so erhält man eine Liste aller bereits vorhandenen Benutzerkonten.

Die allgemeine Syntax zum Anlegen eines Benutzerkontos auf einem Domänen-Controller lautet folgendermaßen:

```
NET USER <Benutzername> <Kennwort>
<Optionen> /ADD /DOMAIN
```

Bild 1: Verwendung des NET-Kommandos

```

C:\users\default>NET /?
Die Syntax dieses Befehls lautet:

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\users\default>NET HELP TIME
Die Syntax dieses Befehls lautet:

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

NET TIME synchronisiert die Systemzeit eines Computers mit der eines anderen
Computers oder einer Domäne. Zeigt die Systemzeit eines Computers oder einer
Domäne an. Ohne Optionen wird in einer Windows NT Server-Domäne das aktuelle
Datum und die Zeit des zum Zeitserver bestimmten Computers angezeigt.

\\Computername   Der Name des Computers, dessen Zeit angezeigt oder
                  übernommen werden soll.

/DOMAIN[:Name]   Gibt die Domäne an, mit der die Systemzeit synchronisiert
                  werden soll.

/SET             Synchronisiert die Systemzeit mit der Zeit des angegebenen
                  Computers oder der Domäne.

/YES            Führt den Befehl NET TIME aus, ohne eine Bestätigungsmeldung
                  anzuzeigen.
  
```

Das Resultat von NET USER hängt davon ab, ob es auf einem Domänen-Controller oder einer Workstation ausgeführt wurde, die Mitglied der NT-Domäne ist. Je nachdem, was der Administrator erreichen möchte, muß er den Parameter */DOMAIN* mit angeben oder nicht. Will er beispielsweise von seiner Workstation aus ein Benutzerkonto in der Domäne anlegen, so muß er den Parameter */DOMAIN* mit angeben. Nur dann wird NET USER auf dem Primären-Domänen-Controller ausgeführt. Läßt er */DOMAIN* weg, so wird NET USER auf seiner lokalen Workstation ausgeführt und der Benutzer in der lokalen Datenbank seiner NT-Workstation angelegt. Bei der Ausführung auf einem Domänen-Controller wird */DOMAIN* ignoriert.

Beispiel:

Es soll von einer NT-Workstation aus ein Benutzerkonto mit dem Namen *PeterM* auf dem Primären-Domänen-Controller angelegt werden. Bei der Erstellung des Kontos soll zudem folgende Informationen mit in die Benutzerdatenbank eingetragen werden:

<i>Vollständiger Name</i>	<i>Peter Maier</i>
<i>Kennwort</i>	<i>passwort</i>
<i>Beschreibung</i>	<i>Standard NTBenutzer</i>
<i>Anmeldeskript</i>	<i>STANDARD.CMD</i>
<i>Erlaubte Workstations</i>	<i>NT_PETERM</i>

Das Benutzerkonto soll zunächst nur Mitglied der Gruppe Domänen-Benutzer sein. Dazu ist folgendes Kommando notwendig:

```
NET USER PeterM passwort /ADD
/COMMENT:"Standard NT-Benutzer"
/FULLNAME:"Peter Maier"
/SCRIPTPATH:STANDARD.CMD
/WORKSTATIONS:"NT_PETERM" /DOMAIN
```

Der Benutzer wird automatisch Mitglied der Gruppe der Domänen-Benutzer. Um ihn anderen Gruppen zuzuordnen, verwendet der Administrator die weiter unten beschriebenen Kommandos NET GROUP beziehungsweise NET LOCALGROUP. Mit Hilfe der optionalen Parameter */COMMENT*, */FULLNAME*, */SCRIPTPATH* und */WORKSTATIONS* werden die zusätzlichen Informationen übergeben.

Darüber hinaus existieren noch weitere Optionen, mit denen der Netzwerkverwalter beispielsweise erlaubte Anmeldezeiten eintragen oder einen Pfad für das Benutzerprofil anlegen kann.

Für die Kennworteingabe ist es wichtig zu beachten, daß NT anders als beim Benutzernamen zwischen Groß- und Kleinschreibung unterscheidet. Wenn man sich nach der Ausführung des Kommandos die Eigenschaften des neuen Kontos im Benutzer-Manager für Domänen ansieht, fällt auf, daß das Kontrollkästchen vor dem Eintrag „Benutzer muß Kennwort bei der nächsten Anmeldung ändern“ nicht angekreuzt ist. Das bedeutet, der Benutzer kann zunächst weiter mit seinem vom Administrator vergebenen Standardkennwort arbeiten, was jedoch nicht unbedingt wünschenswert ist. Das NET USER-Kommando bietet bedauerlicherweise keine Möglichkeit, den Anwender bei der ersten Anmeldung zur Eingabe eines neuen Kennwortes aufzufordern. Ein Weg das Problem zu umgehen, besteht darin, im Benutzer-Manager alle neu erstellten Benutzerkonten mit gedrückter Strg-Taste zu markieren und dann nach dem Drücken der Eingabetaste unter „Benutzereigenschaften“ das entsprechende Kontrollkästchen anzukreuzen.

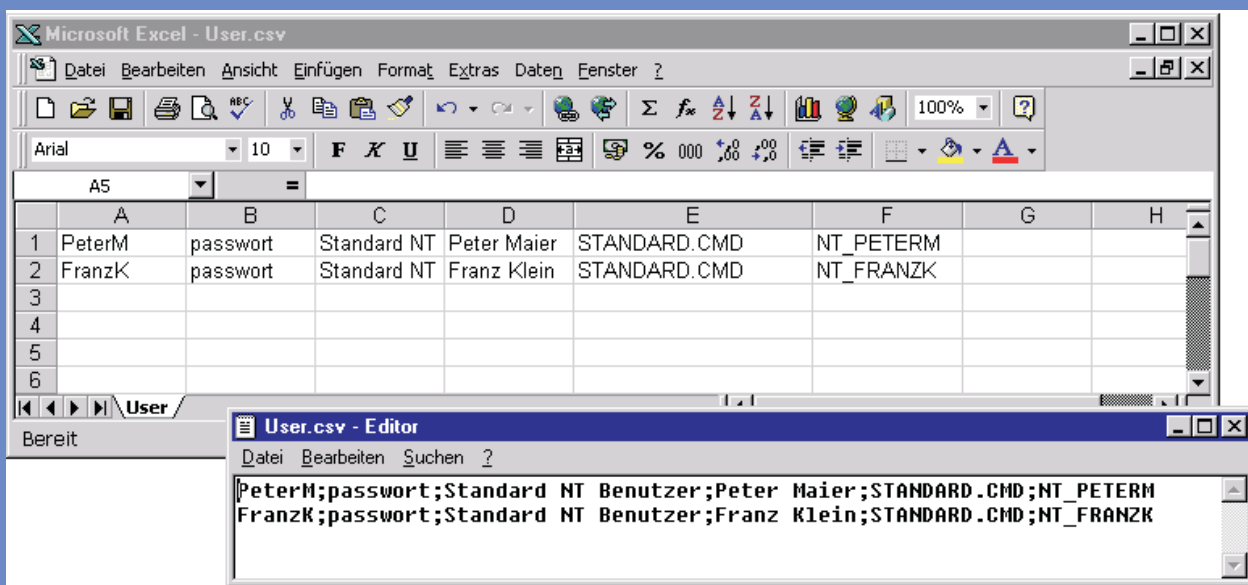
Um eine große Zahl von Benutzern anzulegen, empfiehlt sich die Verwendung einer Eingabedatei, in der sämtliche Parameter, wie Benutzerkennung, vollständiger Name, Kennwort, und so weiter eingetragen sind. Pro Benutzer ist eine Zeile mit allen notwendigen Parametern einzugeben. Zum Auslesen dieser Datei kann der Administrator dann das in Teil 1 dieser Serie vorgestellte FOR-Kommando benutzen. Am einfachsten läßt sich dies mit einer Excel-Tabelle realisieren. Diese muß dann lediglich analog Bild 2 im CSV-Format als ASCII-Text abgespeichert werden, damit sie vom FOR-Kommando ausgewertet werden kann.

Das Kommando zum Einlesen einer Eingabedatei USER.CSV würde dann folgendermaßen aussehen:

```
FOR /F "tokens=1,2,3,4,5,6 delims=;" %a IN
(USER.CSV) DO NET USER %a %b /ADD
/COMMENT:"%c" /FULLNAME:"%d"
/SCRIPTPATH:%e /WORKSTATIONS:"%f"
/DOMAIN
```

Es ist zu beachten, daß bei der Verwendung dieses Kommandos in einem Skript den Platzhaltern zwei Prozent-Zeichen vorangestellt werden müssen. Entsprechend ist zum Beispiel %%a an Stelle von %a zu verwenden.

Bild 2: Erstellen einer Eingabedatei zum Anlegen von Benutzern



Globale und lokale Gruppen

Zum Anlegen von Gruppen existieren zwei verschiedene Kommandos. Mit NET GROUP kann der Administrator globale Gruppen auf dem Primären Domänen-Controller anlegen. Lokale Gruppen auf NT-Workstations oder NT-Servern werden über NET LOCALGROUP erzeugt. Zudem können mit Hilfe der beiden Kommandos Benutzer in Gruppen hinzugefügt und auch wieder entfernt werden. Ohne weitere Parameter ausgeführt, zeigen NET GROUP und NET LOCALGROUP eine Liste der jeweiligen Globalen beziehungsweise Lokalen Gruppen an. Was die Syntax anbetrifft, so gibt es bei beiden Kommandos keine Unterschiede bezüglich der zu verwendenden Parameter. Es ist jedoch zu beachten, daß das Anlegen einer lokalen Gruppe über NET LOCALGROUP auf einer NT-Workstation von einem Domänen-Controller aus nicht möglich ist.

Die allgemeine Syntax zum Hinzufügen einer Gruppe lautet:

```
NET (LOCAL)GROUP <Gruppenname> /ADD
/COMMENT: "<Kommentar>"
```

Auch beim Anlegen von Gruppen gibt es wieder den Parameter /DOMAIN, über den festgelegt wird, ob eine Gruppe auf einer Workstation oder auf dem Primären-Domänen-Controller angelegt werden soll. Es gelten dieselben Regeln, wie bei NET USER.

Um also beispielsweise von einer Workstation aus die globale Gruppe Entwicklung auf dem Primären Domänen-Controller anzulegen, gibt man folgendes Kommando ein:

```
NET GROUP Entwicklung /ADD
/COMMENT:"Globale Gruppe der
Entwicklungsabteilung"/DOMAIN
```

Um einer Gruppe einen Benutzer hinzuzufügen, muß das NET Group-Kommando lediglich um die Benutzerkennung erweitert werden. Die Syntax lautet damit::

```
NET (LOCAL)GROUP <Gruppenname>
```

<Benutzer>/ADD

Möchte der Administrator also von einer Workstation aus der eben erstellten Gruppe Entwicklung den bereits vorhandenen Benutzer PeterM hinzufügen, so muß er folgendes auszuführen:

NET GROUP Entwicklung PeterM/ADD/DOMAIN

Benutzerdatenbanken synchronisieren

Hat der Administrator in der Benutzerdatenbank des Primären Domänen-Controller neue Konten und Gruppen angelegt, dauert es eine gewisse Zeit, bis diese durch Synchronisation der Benutzerdatenbank auch auf den Sicherungs-Domänen-Controllern (BDC) zur Verfügung stehen. Es gibt jedoch eine Möglichkeit, den Synchronisationsvorgang zu beschleunigen. Dazu benutzt der Administrator das Kommando *NET ACCOUNTS /SNYC*. Wird dieses auf dem PDC ausgeführt, sorgt es dafür, daß alle Sicherungs-Domänen-Controller mit der Synchronisation der Benutzerdatenbank beginnen. Wenn es dagegen auf einem BDC gestartet wird, synchronisiert sich nur dieser mit dem Primären-Domänen-Controller.

NET ACCOUNTS hat über die gezeigte Funktion hinaus auch noch andere Fähigkeiten. So kann der Administrator bestimmte Kennwort- und Anmeldebedingungen für sämtliche Benutzerkonten beeinflussen und beispielsweise die minimale Kennwortlänge oder die maximale Gültigkeitsdauer eines Kennwortes festlegen.

Beispiel:

Mit Hilfe von *NET ACCOUNTS* sollen folgende Richtlinien implementiert werden:

Minimale Kennwortlänge: 10 Zeichen

Maximale Gültigkeitsdauer eines Kennwortes: 30 Tage

Zeitraum, nach dem ein Kennwort frühestens geändert werden darf: 5 Tage

Anzahl der Kennwortänderungen, nach denen ein bereits benutztes Kennwort erneut verwendet werden darf: 9

Dazu ist folgendes Kommando notwendig:

NET ACCOUNTS /MINPWLEN:10 /MAXPWAGE:30 /MINPWAGE:5 /UNIQUEPW:9

Um sich die Auswirkungen des Kommandos zu überzeugen, kann der Administrator den Benutzer-Manager aufrufen und unter „Richtlinien“ den Eintrag „Konten“ auswählen.

Auch bei *NET ACCOUNTS* existiert wieder der */DOMAIN-Parameter* mit den mittlerweile bekannten Auswirkungen.

Verzeichnisse und Verzeichnisrechte

Sind alle Benutzer und Gruppen angelegt, steht der Administrator häufig vor der Anforderung, Verzeichnisse anzulegen und netzwerkseitig freizugeben, sowie entsprechende Zugriffsrechte zu erteilen. Auch zu diesem Zweck existieren geeignete Kommandozeilenbefehle. Über das MD beziehungsweise MKDIR werden Verzeichnisse angelegt. Beide Kommandos erzeugen wenn nötig jedes Zwischenverzeichnis. Wenn zum Beispiel das Verzeichnis \Benutzer nicht existiert, dann ist:

MD \Benutzer\Maier

dasselbe wie:

MD \Benutzer

CD \Benutzer

MD Maier

Datei- und Verzeichnisrechte werden über das Kommando *CACLS* (Change ACLs) gesetzt. *CACLS* verfügt über zahlreiche Parameter und ist in der Lage, Verzeichnisrechte zu ändern oder komplett zu überschreiben. Um die Rechte eines Verzeichnisses inklusive aller Unterverzeichnisse zu ändern, ist folgende Syntax zu verwenden:

CACLS <Verzeichnisname> /T /E /G <Benutzer>:<Zugriffsrecht>

Dabei bedeutet der Parameter */T*, daß von der Rechteänderung auch alle Unterverzeichnisse be-

Treffen sind und /E, daß die Dateizugriffsliste (ACL) modifiziert, aber nicht überschrieben werden soll. Mit dem Parameter /G übergibt der Administrator das Benutzerkonto, für das die Rechteänderung durchgeführt werden soll und das jeweilige Zugriffsrecht. Dieses kann sein „C“ für Ändern, „R“ für Lesen oder „F“ für Vollzugriff.

Wenn der Administrator also dem Benutzer PeterM nur Lesezugriff auf das Verzeichnis C:\Benutzer\Maier gewähren möchte, ohne bereits vorhandene Rechte zu entfernen, gibt er folgendes Kommando ein:

```
CACLS C:\Benutzer\Maier\T\E\G PeterM:R
```

Leider unterstützt CACLS nicht alle Differenzierungsmöglichkeiten zur Rechtevergabe, so wie sie der Administrator beispielsweise über den Explorer oder den Datei-Manager vergeben kann. So fehlt zum Beispiel die Möglichkeit, das Recht „Ausführen“ oder „Besitz übernehmen“ zu vergeben. Wer diese Differenzierungen benötigt, dem sei das Tool XCACLS empfohlen, welches auf der Begleit-CD zur Technischen Referenz für Windows-NT (NT Resource Kit) enthalten ist.

Verzeichnisse freigeben

Schließlich ist es in den meisten Fällen noch erforderlich, bestimmte Verzeichnisse für Netzwerk-anwender freizugeben. Dazu setzt der Administrator das Kommando NET SHARE ein, mit dem er Freigaben erstellen oder beenden kann. NET SHARE ohne Parameter aufgerufen, listet die momentan freigegebenen Netzverzeichnisse auf.

Die allgemeine Syntax zur Freigabe eines Verzeichnisses lautet:

```
NET SHARE <Freigabename>=<Pfad>
```

Um also das Verzeichnis C:\Benutzer\Mueller als Netzverzeichnis Mueller freizugeben, verwendet der Administrator folgenden Befehl:

```
NET SHARE Mueller=C:\Benutzer\Mueller
```

Bei Bedarf kann er auch einen Kommentar mit

angeben, aus dem beispielsweise etwas über den Inhalt eines Netzverzeichnisses hervorgeht. Ebenso läßt sich die maximale Anzahl von Benutzern festlegen, die auf das Verzeichnis zugreifen dürfen festlegen. Dazu existieren zwei weitere Parameter. Über /USERS:<Anzahl> wird die Zahl der Anwender pro freigegebenem Verzeichnis beschränkt. Mit Hilfe des Parameters /REMARK:<Beschreibung> kann der Administrator eine kurze Beschreibung über den Inhalt des Verzeichnisses bekannt machen.

Benutzerrechte zuweisen

Zuweilen kann es vorkommen, daß Anwendern bestimmte Benutzerrechte zugewiesen oder entzogen werden sollen. Beispiele für solche Benutzerrechte sind „Ändern der Systemzeit“ oder „Anmelden als Dienst“. Bislang existierte außer dem Benutzer-Manager keine Möglichkeit, diese Rechte über ein Kommandozeilenprogramm zu gewähren oder zu entziehen. Auf einer Ergänzungs-CD zum Windows-NT-Resource-Kit, der Supplement-2-CD befindet sich jedoch ein Tool namens NTRIGHTS, mit dem sich die gewünschte Funktion realisieren läßt.

Die allgemeine Syntax von NTRIGHTS zum Gewähren eines Rechtes ist:

```
NTRIGHTS -u <Benutzer|Gruppe> +r  
<Benutzerrecht>
```

Um beispielsweise dem Anwender PeterM das Recht „Sichern von Dateien und Verzeichnissen“ zu gewähren, muß der Administrator folgenden Befehl ausführen:

```
NTRIGHTS -u PeterM +r SeBackupPrivilege
```

Um einem Anwender ein Recht zu entziehen, ist anstelle von +r r zu verwenden. Das ganze funktioniert nicht nur lokal, sondern auch auf entfernten Rechnern. Über den Parameter m kann der Administrator einen beliebigen NT-Rechner spezifizieren. Damit die Ausführung auf einem entfernten Rechner jedoch auch funktioniert, muß der Netzwerkverwalter auch administrative Rechte auf der betreffenden Station besitzen.

Zu beachten ist die etwas eigenartige Schreibweise der Benutzerrechte. Für die korrekte Ausführung von NTRIGHTS ist es erforderlich, die Schreibweise zu verwenden, wie sie normalerweise in Win32-Programmen eingesetzt wird und die unabhängig von spezifischen Landessprachen ist. *SeBackup Privilege* zum Beispiel entspricht „Sichern von Dateien und Verzeichnissen“ oder *SeServiceLogon Right* ist gleichbedeutend mit „Anmelden als Dienst“. Eine Auflistung aller Benutzerrechte erhält man durch Eingabe von *NTRIGHTS /?* oder über die Hilfedatei des Resource-Kits (RKTOOLS.HLP).

Shortcut

Executive Summary

Über Kommandozeilen-Programme lassen sich zahlreiche administrative Aufgaben, wie zum Beispiel Backups oder die Einrichtung von Benutzern und Shares automatisieren. Windows NT liefert eine ganze Reihe entsprechender Werkzeuge, die für Automatisierungsaufgaben in Skripten verwendet werden können. Diese Serie vermittelt anhand zahlreicher Beispiele die Grundlagen erfolgreicher Skriptprogrammierung unter Windows NT.

Zur Person

DIPL. ING. DIRK PELZER arbeitet als freier Consultant und Journalist in München. Er betreibt ein Storage Labor für verschiedene namhafte Fachzeitschriften. Zudem beschäftigt er sich mit Speichernetzen und Hochverfügbarkeit.