

Windows Server 2003

Konfiguration als Domänencontroller & weitere Möglichkeiten



Inhaltsverzeichnis

- [Teil 1](#) - Grundwissen und ein bisschen Theorie
- [Teil 2](#) - Einrichten des Active Directory
- [Teil 3](#) - Konfiguration von DNS-/WINS- und DHCP-Serverdienst
Einstellungen auf den Clients + Hineinheben der Clients
in die Domäne
- [Teil 4](#) - Erstellen der benötigten Freigaben, Anlegen von Usern
Zuweisen Basis- und Profilordner Einführung
Gruppenrichtlinien
- [Teil 5](#) - Erstellen und Verknüpfen eines Login-Skripts, setzen
von lokalen Berechtigungen, DHCP-Reservierungen für
die Clients
- [Teil 6](#) - Installation und Konfiguration der Software Update
Services (SUS)
- [Teil 7](#) - SUS-Server Dateien bei Neuinstallation sichern
- [Teil 8](#) - Clients nur kurzfristig an SUS-Server anbinden

Windows Server 2003

Konfiguration als Domänencontroller & weitere Möglichkeiten

Teil 1 - Grundwissen und ein bisschen Theorie

Vorwort

Dieser Artikel richtet sich an alle Hobby-Administratoren, die für ihr privates Netzwerk über einen Windows Server 2003 verfügen und dessen Möglichkeiten auch ausreizen wollen. Der Artikel wird sich aufgrund der Fülle an Möglichkeiten in mehrere Teile aufgliedern, wobei ein Teil auf dem anderen aufbauen wird.

Wünschenswert sind Grundkenntnisse über die Funktionsweise eines Netzwerks sowie die Kenntnis über Fachterminologie. Wem einige Fachbegriffe nicht geläufig sind, der kann diese im [Glossar von AT-Mix](#) nachschlagen.

Entsprechend dieser Vorgabe werde ich in diesem Artikel nicht alle technischen Details ausführlich behandeln (können) und einen Großteil der Theorie aussparen - erfahrene Administratoren werden also das ein oder andere vermissen. Nichtsdestotrotz wird der komplette Weg zur eigenen Domäne mit den für ein privates [LAN](#) nützlichen Features so ausführlich wie möglich geschildert.

Zur Person

Mein Name ist Jörg Alexander Ott, ich bin Baujahr 1976 und beschäftigte mich seit annähernd 20 Jahren mit Computern. Seit einigen Jahren arbeite ich als System- und Netzwerk-Administrator und bin für Planung, Installation, Wartung und Troubleshooting der Systeme in einem heterogenen Umfeld zuständig - so betreue ich neben Windows- auch Linux-Server und eben alle Client-Systeme (W9x bis XP). Passend dazu nehme ich momentan die Möglichkeit zur Weiterbildung zum MCSE2003 wahr, was wohl bis zum Herbst 2004 abgeschlossen sein sollte.

Teil 1 - Grundwissen und ein bisschen Theorie

Vor die Installation hat Gott die Theorie gestellt - an diesem Leitsatz kommt auch dieser Artikel (leider) nicht vorbei, wobei ich versuchen werde, die Theorie auf ein Mindestmaß zu beschränken. Ganz weglassen kann ich sie allerdings nicht...

Was ist eigentlich eine "Domäne" ?!?

Der Begriff Domäne dürfte vor allem in Verbindung mit Internet-Domänen bekannt sein. Ähnlich verhält es sich auch mit lokalen Domänen, auch hier besteht eine Domäne aus mindestens zwei "Teilen". In der Praxis sieht das dann meist so aus: domaene.local oder standort.domaene.local. Und genau wie bei Internet-Domänen müssen auch hier die Richtlinien für korrekte DNS-Auflösung beachtet werden (zwar bietet auch der 2003-er Server noch NetBios-Auflösung, aber primär wichtig ist die DNS-Auflösung). Sinn und Zweck einer lokalen Domäne - seit [Windows 2000](#) als Active Directory bekannt - ist es im Grunde, [Rechner](#) eines Netzwerks in einer zentral verwaltbaren Umgebung einzufassen und somit von zentraler Stelle aus alle Rechner

verwalten zu können. Gleichzeitig lassen sich mit einer Domäne alle Nicht-Domänenmitglieder von der Benutzung von Ressourcen ausgrenzen, was z.B. in einem Peer-to-Peer-Netz ohne Domäne fast aussichtslos ist.

Der Begriff "Domäne" stammt noch aus NT4-Zeiten, mittlerweile spricht man vom "[Active Directory](#)" (nachfolgend AD genannt), und das hat auch seinen Grund:

Das AD stellt einen Verzeichniskatalog dar, in dem Objekte unterschiedlichster Art gespeichert werden können. Objekte können Benutzerkonten sein, Computerkonten oder auch Drucker. Mittels der AD-Funktionalitäten können jedem Objekt bestimmte Sicherheitseinstellungen zugewiesen werden, sodass z.B. User1 auf Drucker1 Dokumente drucken kann, User2 aber nicht usw. Gleiches gilt natürlich insbesondere für die Datei-Freigaben innerhalb des AD - hier kommen die Möglichkeiten der Sicherheitseinstellungen erst richtig zur Geltung.

Jedes Objekt im AD erhält eine eigene SID und ist somit einzigartig, entsprechend auch relativ leicht wieder zu finden (wobei der Punkt mit dem "Wieder finden" eher in großen Netzen zur Geltung kommt; in einem privaten Netz sollte das Wieder finden von Objekten kein Problem sein).

Wichtig dabei ist, dass jedem AD-Mitglied der Zugriff auf ein beliebiges Objekt im AD gestattet oder verweigert werden kann - dazu später mehr.

Wichtigster Rechner im AD ist der Domänen-Controller (nachfolgend DC genannt) - er enthält alle Infos des AD, den sog. "Globalen Katalog". Gleichzeitig dient er als Anmeldeserver, der die Authentifizierung vornimmt und somit Zugriff gestattet oder verweigert. In einer "Ein-Server-Umgebung" wird der DC auch als Anwendungs- und File-Server genutzt.

Was ist vor der Heraufstufung eines Windows 2003 Servers zum Domänencontroller zu beachten?

Wichtig für das erfolgreiche Nachbauen anhand dieses Artikels ist vor allem, dass der Server frisch installiert wurde und noch keinerlei Einstellungen verändert wurden eine ganz normale Standard-Installation mit den beim Setup vorgeschlagenen Default-Werten also. Sicherlich ist es auch möglich, einen bereits im Produktivbetrieb befindlichen und entsprechend konfigurierten Server zum DC heraufzustufen - das aber muss vorher gut geplant werden und bedarf vor allem der Rücksetzung einiger Einstellungen auf die Default-Werte, worauf ich hier verständlicherweise nicht eingehen kann.

Die einzige Einstellung, die vor dem Heraufstufen geändert werden muss, ist die Vergabe einer statischen IP-Adresse, dazu später mehr.

Vorraussetzungen für den Betrieb eines Domänen-Controllers

Um ein AD im LAN zu betreiben, bedarf es ein wenig Vorplanung. Man muss sich vorher darüber im Klaren sein, welches IP-Segment man wählt - ist der DC erst mal mit einer statischen IP-Adresse versehen und heraufgestuft, lässt sich dies nachher nur noch schwer ändern. Insbesondere wenn vom LAN aus später Zugriffe auf externe Netze stattfinden sollen, ist die Wahl des IP-Segments ausschlaggebend:

Verwendet z.B. das Firmennetz das gleiche IP-Segment, dann sind VPN-Verbindungen später ein Problem etc. Auch dazu später mehr Details, wählt das IP-Segment eures DCs (und somit eures LANs) also am besten außerhalb aller bereits vorhandenen Netze, in diesem Artikel wird das IP-Segment 192.168.10.0/24, also ein privates Klasse-C-Netz verwendet.

Weiterhin ist das Betriebssystem der Clients im Netz wichtig: Windows 2000 Professional oder Windows XP Professional sind die Betriebssysteme, die in ein AD hineingehören, mit älteren Systemen wie 9x, ME oder NT lässt sich im AD nicht viel anstellen. In diesem Artikel gehe ich von Windows XP Professional als Client-Betriebssystem aus, wobei die meisten Einstellungen 1:1 auch für Windows 2000 Professional übernommen werden können.

Last but not least muss natürlich das Netzwerk selbst vernünftig laufen, es sollte also zumindest ein Switch oder ein Router mit integriertem Switch samt der passenden Kabel zum Anschluss der Clients vorhanden sein. Von Direktverbindungen via Crossover-Kabel rate ich an dieser Stelle ab, das führt unweigerlich zu Problemen, wenn nicht permanent beide Rechner laufen - jeder DC muss permanent an eine aktive Netzwerkverbindung angeschlossen sein, sonst hagelt es Fehlermeldungen. Bei einer Crossover-Verbindung wird die Netzwerkverbindung aber beim Abschalten des Clients deaktiviert, somit sind die Probleme vorprogrammiert. Davon abgesehen stellt sich die Frage, ob für einen Rechner unbedingt ein DC her muss...

So, das sollte an Theorie erst mal genügen - der zweite Teil, der dann - wie alle anderen nachfolgenden Teile auch - mit Screenshots versehen sein wird, beschäftigt sich mit der Heraufstufung eines Windows 2003 Servers zum Domänen-Controller und beschreibt Vorgehensweise und Auswirkungen.

Teil 2 - Einrichten des Active Directory

Nach der erfolgreichen Installation des W2k3-Servers mit den Standardvorgaben können wir nun loslegen und richten zuerst das [Active Directory](#) ein, d.h. wir stufen den Server zum Domänencontroller hoch.

Damit die Angaben übertragbar sind, hier die von mir bei der Installation vergebenen Daten:

Servename:	TESTSERVER
IP-Adresse:	192.168.10.254/24
DNS-Domain:	mydomain.local
NETBIOS-Domain:	MYDOMAIN

Um die nachfolgenden Schritte durchzuführen, MUSS der Server über eine aktives Netzwerk-Interface verfügen!!! Verbindet also bitte die Netzwerkkarte des Servers mit einem Hub/Switch/Router, andernfalls kann die Promotion zum DC nicht erfolgen.

Zu allererst müssen wir dem Server eine statische [IP-Adresse](#) zuordnen, diese muss natürlich zu dem IP-Segment passen, das ihr in eurem LAN verwendet; die von mir gewählten Angaben sind also entsprechend anzupassen.

Zum Vergabe einer IP-Adresse geht man wie folgt vor:
Start => Systemsteuerung => Netzwerkverbindungen => LAN-Verbindung =>
Rechtsklick => Eigenschaften auswählen. Es erscheint folgender Dialog:



Vergeben der IP-Adresse

Den Eintrag "Internetprotokoll (TCP/IP)" auswählen und auf Eigenschaften klicken, dann die Werte - entsprechend angepasst an eure Umgebung - eintragen:

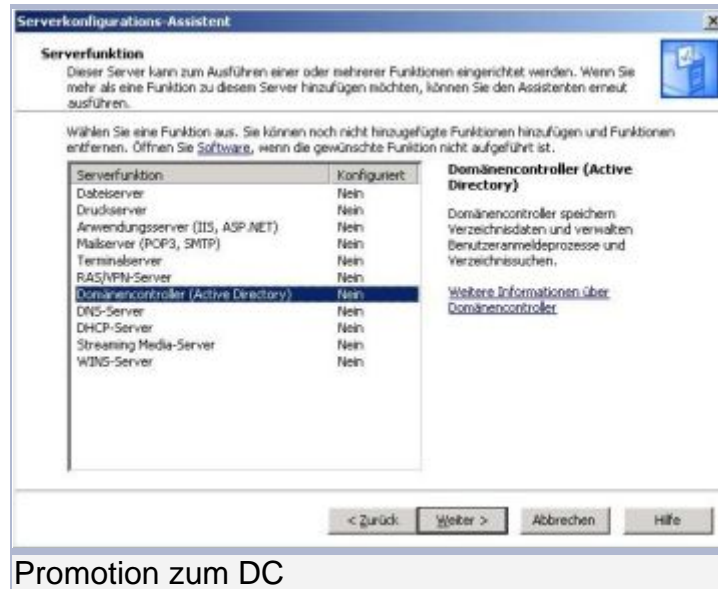


Vergeben der IP-Adresse

Der Eintrag „Standardgateway“ zeigt immer auf den Router, also euer Internetgateway. Sollte ein solches bei euch nicht vorhanden sein, lasst dieses Feld leer.

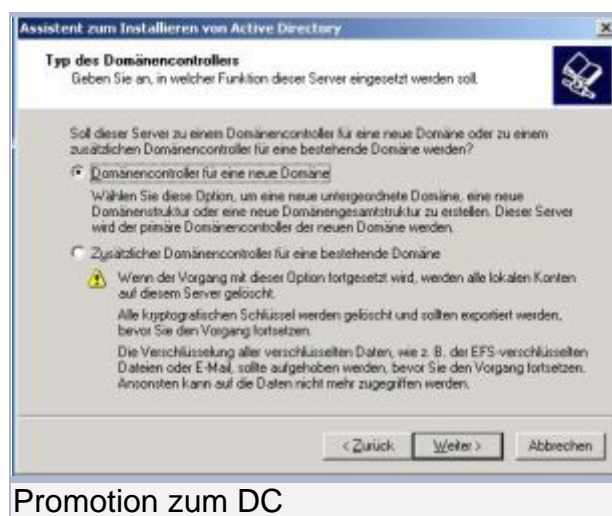
Die Dialoge bestätigt ihr alle mit OK, somit ist die Vergabe einer statischen IP-Adresse abgeschlossen.

Nun kann der Vorgang des Heraufstufens - auch Promotion genannt - angestoßen werden, dazu gibt es zwei Möglichkeiten: Die erste wäre Start => Ausführen => dcpromo => Enter, die zweite führt über den Serverkonfigurations-Assistenten, den ihr über Start => Verwaltung => Serverkonfigurations-Assistent aufrufen könnt. Im Assistenten wählt ihr dann "Funktionen hinzufügen" und landet in diesem Dialog:



"Domänencontroller (Active Directory)" markieren und auf "Weiter" klicken startet - genau wie dcpromo - den "Assistenten zum Installieren von Active Directory", dessen Willkommensbildschirm ihr mit "Weiter" wegklickt, ebenso wie den nächsten Dialog "Betriebssystemkompatibilität".

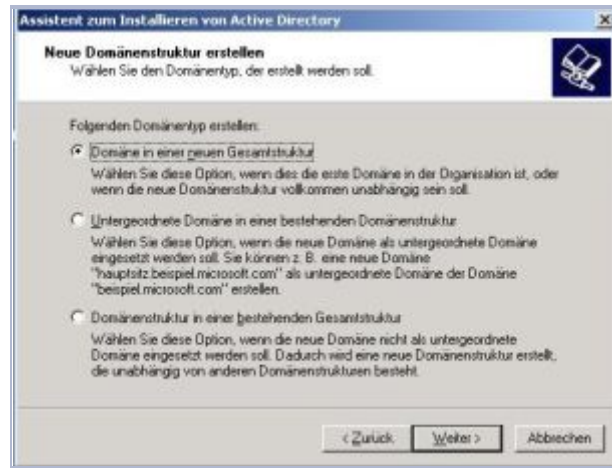
Im nächsten Dialog "Typ des Domänencontrollers" wählt ihr "Domänencontroller für eine neue Domäne" und bestätigt mit "Weiter". Der zweite Punkt ist zu wählen, wenn ihr bereits eine Domäne habt und einen weiteren DC installieren wollt.



Der nächste Dialog "Neue Domänenstruktur erstellen" erwartet nur eine Auswahl, ob dieser DC einer bereits bestehenden Domäne hinzugefügt werden oder aber der erste DC einer neuen Domäne werden soll. Die Auswahlmöglichkeit "Domänenstruktur in einer bestehenden Gesamtstruktur" dient zur Erstellung

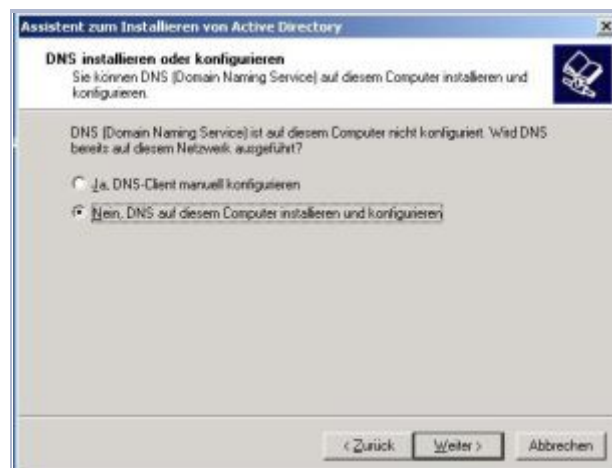
mehrerer Domänen innerhalb großer Organisationen - da wir uns hier mit einem Heimnetzwerk beschäftigen, kommt dies also nicht in Frage.

Der zu installierende DC ist der erste DC für eine neue Domänenstruktur, somit ist also die erste Auswahl die richtige.



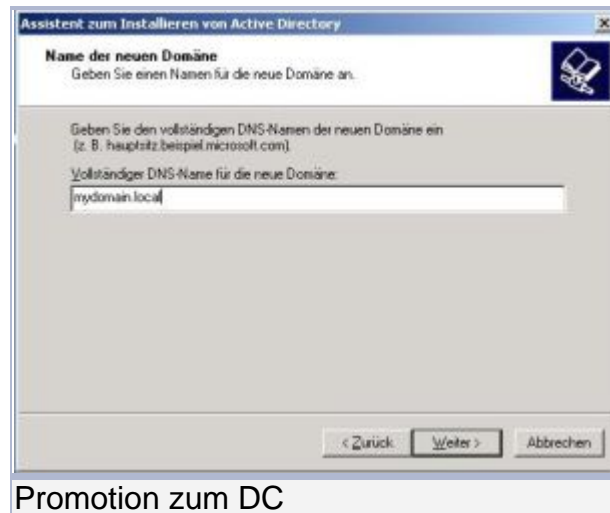
Promotion zum DC

Ein Klick auf "Weiter" bringt euch zum nächsten Dialog "DNS installieren oder konfigurieren". Da wir den Server mit den Standardvorgaben installiert haben, ist noch kein DNS-Server-Dienst installiert. Um die Promotion des Servers zum DC erfolgreich abzuschließen, muss die [Windows Server](#) 2003-CD im Laufwerk eingelegt sein, da der DNS-Server nun nachinstalliert wird. Entsprechend trifft ihr folgende Auswahl: "Nein, DNS auf diesem Computer installieren und konfigurieren" und klickt dann auf "Weiter".

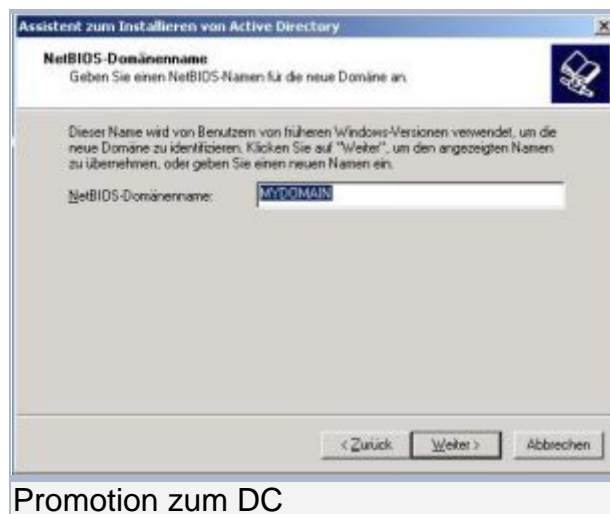


Promotion zum DC

Nun geht es um den DNS-Namen, den eure Domain erhalten soll. Solltet ihr bereits eine eigene Domain im Internet haben: Nehmt bitte NICHT den Namen eurer Domain, sondern einen anderen bzw. ändert den bestehenden Namen! Statt "maxmustermann.de" nehmt besser "maxmustermann.local"; das verhindert, dass es später zu DNS-Problemen kommt.



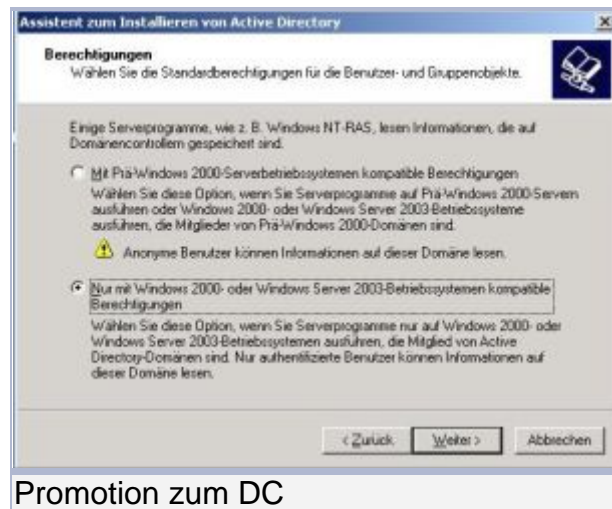
Gestaltet den Namen auch nicht zu kompliziert, für unser Szenario reicht ein ähnlicher Name wie angegeben völlig aus. Bestätigt auch diese Eingabe mit „Weiter“, ihr kommt dann zum Dialog „NetBIOS-Domänenname“. Dies ist der Domänen-Name, den ihr später in der Netzwerkumgebung sehen werdet, per default schlägt Windows den ersten Teil des DNS-Domainnamens vor. Ihr könnt den Namen ruhig ändern, NetBIOS- und DNS-Namen der Domain müssen nicht zwangsläufig gleich lauten, allerdings empfiehlt es sich in diesem Fall. Entsprechend habe ich für die Domain den Namen MYDOMAIN vergeben.



Ein Klick auf "Weiter" bringt euch zum Dialog "Datenbank- und Protokollordner". Hier könnt ihr ruhigen Gewissens die Standardeinstellungen lassen und auf "Weiter" klicken, da für eine kleine Domäne keine getrennten Speicherorte für Datenbanken und Protokollordner erforderlich sind. Diese Einstellungen ändert man eigentlich nur, wenn man Domänen mit mehreren hundert oder tausend Usern/Objekten erstellt.

Der nächste Dialog "Freigegebenes Systemvolume" schlägt per default den Pfad C:\Windows\SYSVOL vor, auch hier können die Standardeinstellungen einfach übernommen werden. In diesem Ordner werden die zu replizierenden Daten abgelegt, was wiederum nur bei mehreren DCs bzw. mehreren Domänen eine Rolle spielt. Klickt also auf "Weiter" und trifft im Dialog "Berechtigungen" die Auswahl "Nur

mit Windows 2000- oder Windows Server 2003-Betriebssystemen kompatible Berechtigungen".



Hiermit legt ihr fest, dass weitere DCs bzw. Domänen mindestens auf Windows 2000 bzw. Server 2003 ausgeführt werden müssen, NT4-DCs bzw. Domänen sind nicht kompatibel. Prinzipiell für uns uninteressant, da wir ja nun mal nur einen DC haben - und der läuft ja unter Windows Server 2003. Nach dem Klick auf "Weiter" erscheint der nächste Dialog "Administratorkennwort für, Verzeichnisdienste wiederherstellen". Für den Fall, dass euer DC mal defekt sein sollte und ihr ihn vom Backup wiederherstellen müsst, gibt es einen speziellen Wiederherstellungsmodus (zu erreichen mit F8 beim Bootvorgang) - nur dafür ist dieses Kennwort, es hat nichts mit dem eigentlichen Administrator-Kennwort zu tun, das ihr bei der Installation vergeben habt. Geschickterweise würde ich allerdings hier dasselbe Kennwort wählen wie für den Administrator-Account - lässt sich einfach besser behalten.

Ein erneuter Klick auf "Weiter" bringt euch zum Zusammenfassungs-Dialog, alle benötigten Angaben sind gemacht und sollten nun noch kurz kontrolliert werden. Stimmt alles, wird mit Klick auf "Weiter" der Server zum DC hochgestuft und das Active Directory installiert.

Nach Abschluss der Promotion ist zwingend ein Neustart erforderlich. Wenn euer Server dann neu gestartet ist, werdet ihr bei der Anmeldung feststellen, dass ein weiteres Feld hinzugekommen ist: Neben Benutzernamen und Kennwort steht (nach Klick auf "Optionen") das Feld "Anmelden an" zur Verfügung. Hier taucht nun der NetBIOS-Name eurer Domain auf, den ihr im Assistenten eingegeben habt.

Wenn später die Clients in die Domäne eingebunden werden, wird dieses Feld auch auf den Clients zur Verfügung stehen. Während die Clients dann aber dennoch eine lokale Anmeldung erlauben, ist diese am DC nicht mehr möglich - da er ja die Domäne bereitstellt, ist nur eine Anmeldung an der Domäne möglich.

Was ist nun während der Promotion passiert: Es wurden der DNS-Server und die entsprechende DNS-Zone für die Domain installiert, die Verzeichnisdatenbank wurde erstellt und in die vorher angegebenen Ordner gespeichert und der Server wurde zur primären Verwaltungsinstanz für die Domain gemacht, d.h. er hält ALLE Betriebsmasterfunktionen (auch FSMO genannt).

Unter Verwaltung findet ihr nun neue Einträge, z.B. "Active Directory Benutzer- und Computer" und einige mehr, in der Netzwerkumgebung sollte nun bereits der NetBIOS-Domainname auftauchen und darunter der Server mit seinem bei der Installation vergebenen Namen.

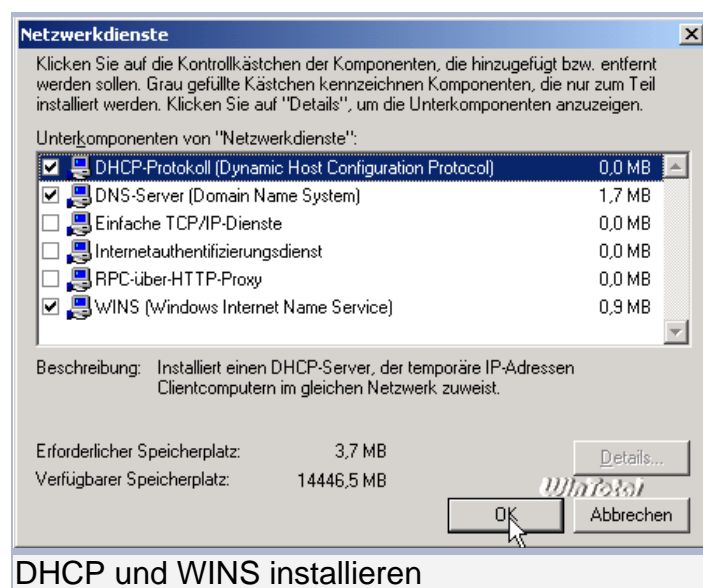
Bestenfalls sollte der Server zum Abschluss noch auf <http://windowsupdate.microsoft.com> mit den neuesten Patches/Updates versorgt werden.

Bevor nun die Clients im Netz in die Domäne aufgenommen werden können, beschreibt Teil 3 die Konfiguration von DNS, DHCP und WINS und erläutert, welche Einstellungen an den Clients noch getroffen werden müssen, um ein reibungsloses Zusammenspiel zwischen Server und Clients zu ermöglichen, allen Rechnern Internetzugang zu gewähren etc.

Teil 3

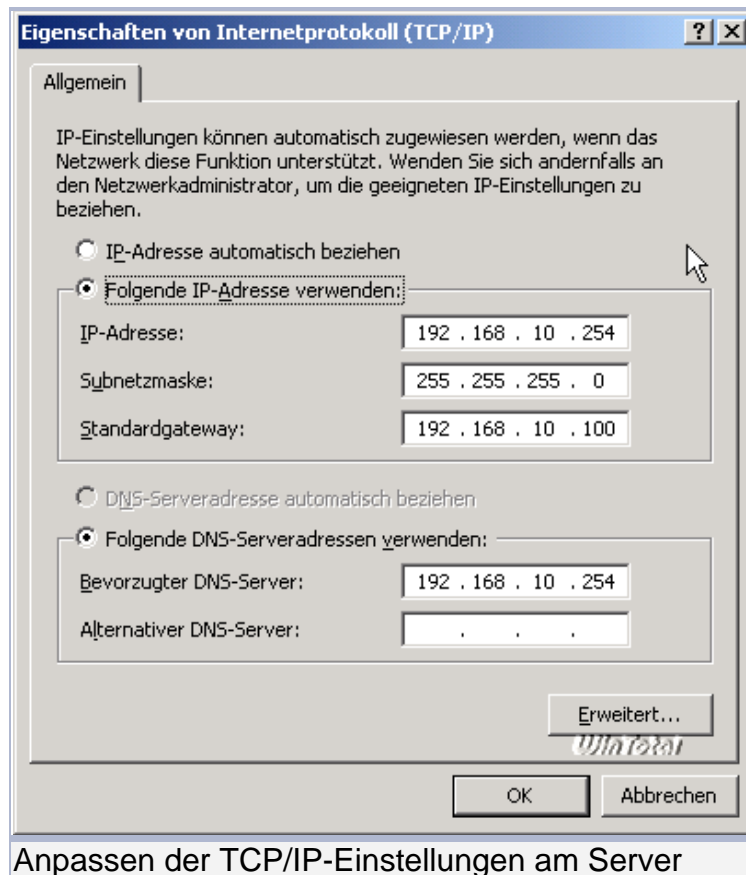
Konfiguration von DNS-/WINS- und DHCP-Serverdienst Einstellungen auf den Clients + Hineinheben der Clients in die Domäne

Nach der erfolgreichen Installation des W2k3-Servers und der Hochstufung zum Domänencontroller, richten wir nun den DNS/WINS und DHCP-Dienst ein. Danach heben wir die Clients in die Domäne. Nachdem die Promotion zum DC erfolgreich war, gilt es nun, den Server so zu konfigurieren, dass die Clients problemlos Zugriff haben - die wichtigsten drei Dienste sind DNS (Domain Name Services), WINS (Windows Internet Name Services) und DHCP (Dynamic Host Protocol Configuration). Doch zuallererst ergänzen wir unsere Installation, also bitte die Server-CD ins Laufwerk legen und über Start => Systemsteuerung => Software => Komponenten hinzufügen oder entfernen => Netzwerkdienste die Dienste DHCP und WINS nachinstallieren.

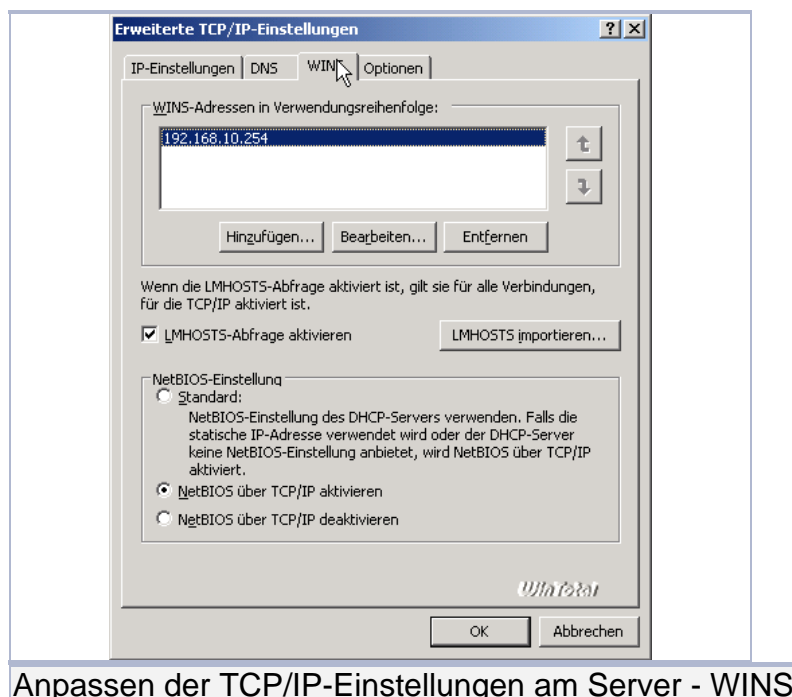


Einfach die Haken vor den Dienstnamen setzen und dann mit OK die Installation durchführen. Danach müssen wir bei den TCP/IP-Einstellungen des Servers noch

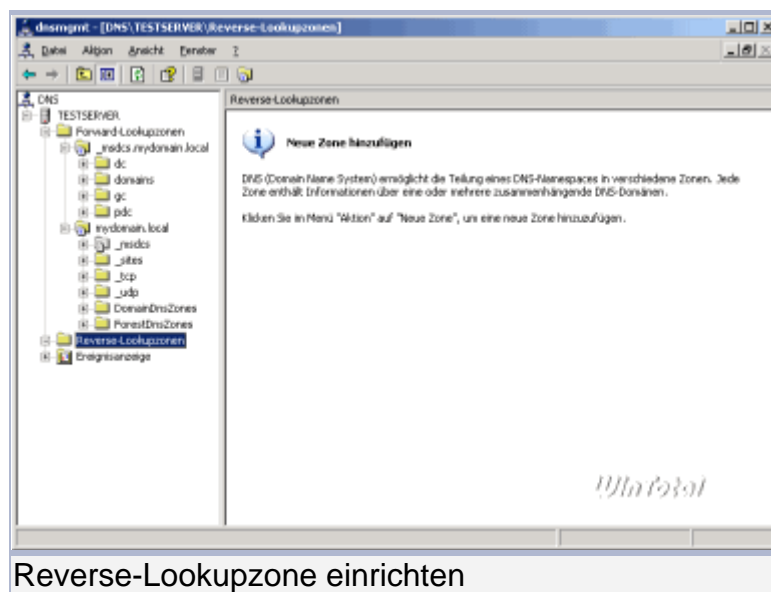
etwas nacharbeiten, d.h. wir ergänzen zuerst den Eintrag DNS-Server und tragen hier die IP-Adresse unseres Servers ein.



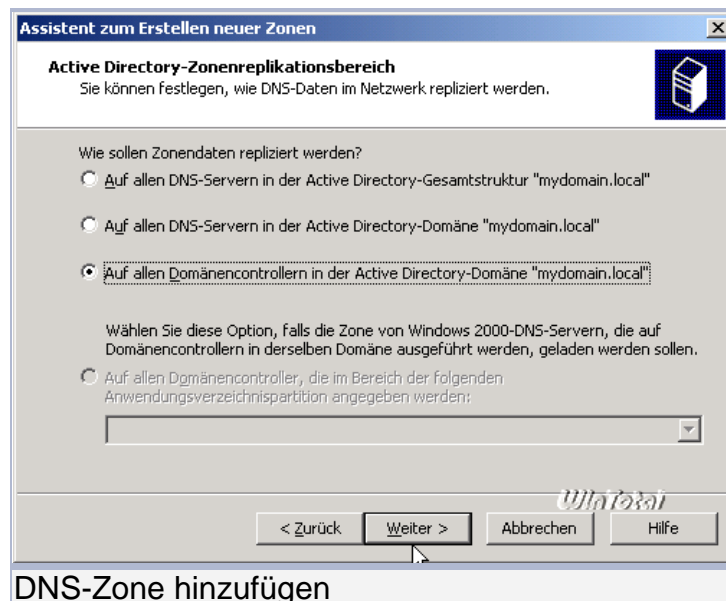
Dann bitte auf "Erweitert" klicken, auf der Registerkarte WINS ebenfalls die IP-Adresse des Servers eintragen und "NetBIOS über TCP/IP aktivieren" anschalten.



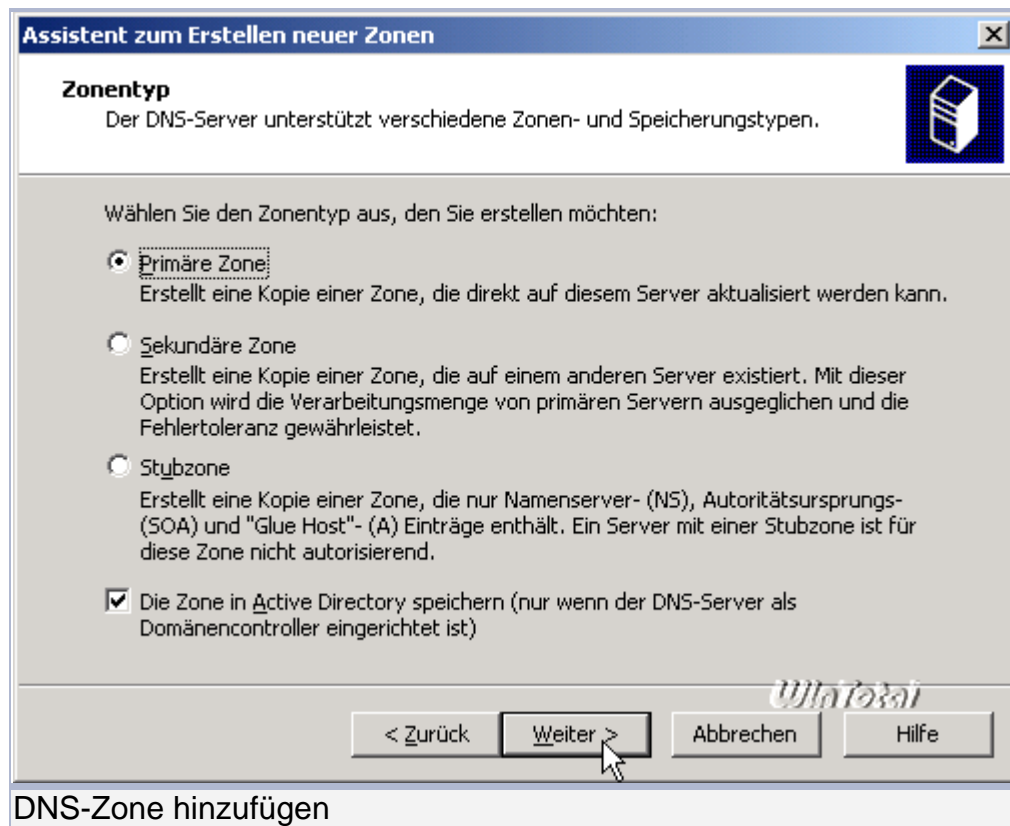
Somit ist sichergestellt, dass später die Namensauflösung sowohl DNS- als auch NetBIOS-technisch problemlos funktioniert. Theoretisch würden XP-Clients und Windows 2003 Server sich zwar auch rein mittels DNS verständigen können, spätestens bei der Einbindung eines Printservers würde das allerdings zu Problemen führen, da diese meist nur NetBIOS beherrschen. Die Einstellungen bitte alle mit OK bestätigen, damit ist die TCP/IP-Konfiguration des Servers soweit erledigt. Bitte einmal rebooten, bevor es weitergeht. Der nächste Schritt ist das Überprüfen und Nachbessern des DNS-Serverdienstes: Bei der Promotion zum DC wurde zwar die korrekte Forward-Lookupzone für unsere Domäne erstellt, die Reverse-Lookupzone müssen wir aber selbst erstellen. Dazu öffnen wir via Start => Verwaltung => DNS die DNS-Serverkonsole, die dann in etwa so aussehen sollte:



Wie unschwer zu erkennen ist, fehlt die Reverse-Lookupzone für unsere Domäne, also ergänzen wir diese durch einen Rechtsklick auf "Reverse-Lookupzone" und Auswahl von "Neue Zone" aus dem Kontextmenü. Damit wird der Assistent zum Hinzufügen von DNS-Zonen gestartet.



Wir erstellen eine primäre, Active-Directory-integrierte Zone, die auf allen Domänencontrollern unserer Domäne verfügbar sein soll (also automatisch repliziert werden würde).



Im nächsten Schritt muss die Netzwerkkennung angegeben werden. Achtung: Auch wenn es sich um eine Reverse-Lookupzone handelt, die Netzwerkkennung muss vorwärts eingegeben werden und nicht, wie oftmals zu lesen ist, rückwärts. Die Abbildung ist also richtig!

Assistent zum Erstellen neuer Zonen

Name der Reverse-Lookupzone
Eine Reverse-Lookupzone übersetzt IP-Adressen in DNS-Namen.

Geben Sie die Netzwerkennung oder den Namen der Reverse-Lookupzone an.

☒ **Netzwerkennung:**
192.168.10

Die Netzwerkennung ist der Teil der IP-Adresse, der dieser Zone angehört. Geben Sie die Netzwerkennung in ihrer normalen Reihenfolge (nicht umgekehrt) ein.

Wenn Sie eine Null in der Netzwerkennung verwenden, wird diese im Zonennamen angezeigt. Beispiel: Netzwerkennung 10 erstellt Zone 10.in-addr.arpa und Netzwerkennung 10.0 erstellt Zone 0.10.in-addr.arpa.

☐ **Name der Reverse-Lookupzone:**
10.168.192.in-addr.arpa

Klicken Sie auf "Hilfe", um weitere Informationen über das Erstellen einer Reverse-Lookupzone erhalten.

< Zurück Weiter > Abbrechen Hilfe

DNS-Zone hinzufügen

Nach Klick auf "Weiter" wählen wir "Nur sichere dynamische Updates zulassen". Dies bewirkt, dass DNS-Einträge zwar dynamisch geändert werden können, allerdings nur von Rechnern, die der Domäne angehören.

Assistent zum Erstellen neuer Zonen

Dynamisches Update
Sie können festlegen, dass diese DNS-Zone sichere, unsichere oder keine dynamische Updates zulässt.

Dynamische Updates ermöglichen DNS-Clientcomputern, sich zu registrieren und die eigenen Ressourceneinträge dynamisch mit einem DNS-Server bei Änderungen zu aktualisieren.

Bestimmen Sie den Typ des dynamischen Updates, der verwendet werden soll.

☒ **Nur sichere dynamische Updates zulassen (Für Active Directory empfohlen)**
Diese Option ist nur für Active Directory-integrierte Zonen verfügbar.

☐ **Nicht sichere und sichere dynamische Updates zulassen**
Dynamische Updates von Ressourceneinträgen werden von allen Clients zugelassen.
⚠ Durch diese Option besteht ein hohes Sicherheitsrisiko, da Updates von nicht vertrauenswürdigen Quellen angenommen werden können.

☐ **Dynamische Updates nicht zulassen**
Dynamische Updates von Ressourceneinträgen werden von dieser Zone nicht zugelassen. Diese Einträge müssen manuell aktualisiert werden.

< Zurück Weiter > Abbrechen Hilfe

DNS-Zone hinzufügen

Damit ist die Reverse-Lookupzone für unsere Domäne angelegt. Nun muss noch ein Zeiger-Eintrag (PTR) für unseren Server gesetzt werden, dazu Rechtsklick auf die

eben angelegte Zone und aus dem Kontextmenü "Neuer Zeiger-Eintrag (PTR)" auswählen.

Neuen Eintrag erstellen

Zeiger (PTR)

Host-IP-Nummer:
192.168.10.254

Vollqualifizierter Domänenname:
254.10.168.192.in-addr.arpa

Hostname:
TESTSERVER Durchsuchen...

☐ Authentifizierte Benutzer können alle DNS-Einträge mit demselben Namen aktualisieren. Diese Einstellung gilt nur für DNS-Einträge für einen neuen Namen.

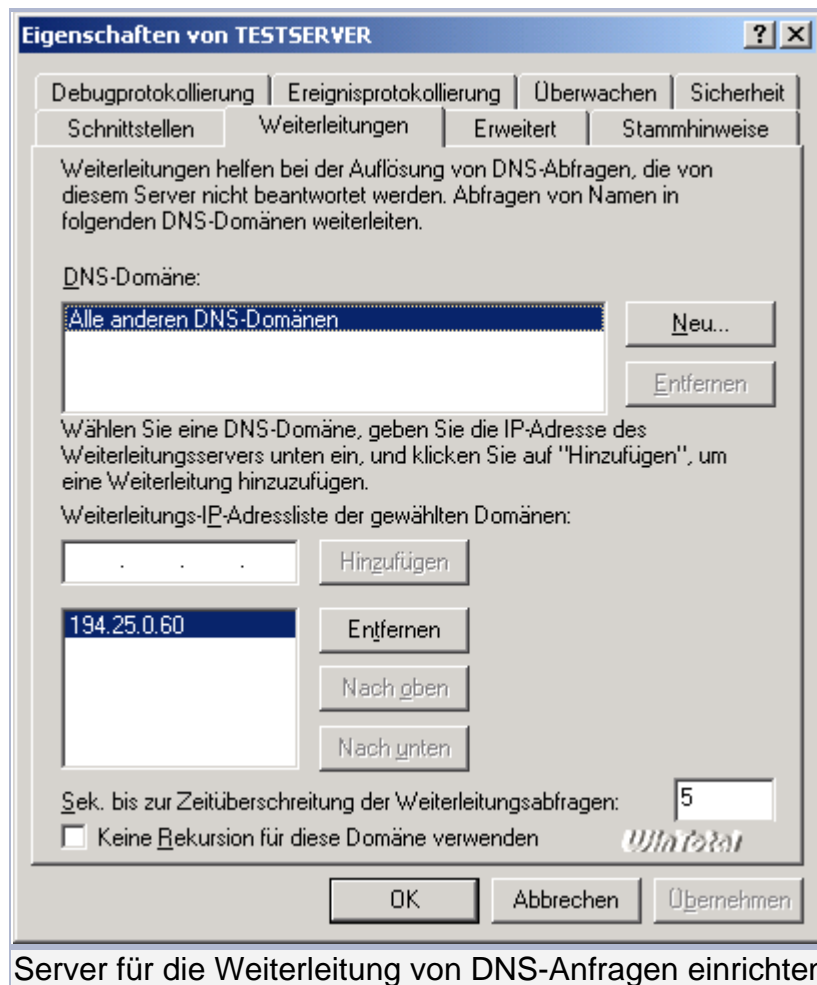
WinStat

OK Abbrechen

Zeiger angeben

Damit ist die lokale DNS-Auflösung soweit eingerichtet, nun muss der Server noch für die Weiterleitung von DNS-Anfragen, die er selbst nicht auflösen kann, konfiguriert werden - z.B. wenn die Clients später im Netz surfen oder Mails holen/senden wollen.

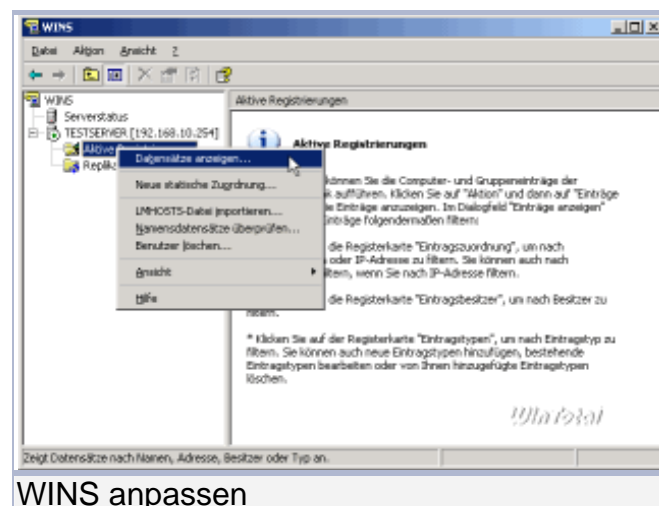
Dazu bitte in der DNS-Serverkonsole einen Rechtsklick auf den Servernamen ausführen und aus dem Kontextmenü "Eigenschaften" wählen, im Dialogfeld auf die Registerkarte "Weiterleitungen" wechseln und dort den DNS-Server eintragen, an den die Anfragen weitergeleitet werden sollen.



Server für die Weiterleitung von DNS-Anfragen einrichten

Ich habe hier die IP-Adresse eines Telekom-DNS-Servers eingetragen, ihr solltet bestenfalls den/die Nameserver eures Providers eintragen (die ihr entweder in der Admin-Oberfläche eures Routers findet oder per `ipconfig /all`, wenn ihr eine DFÜ-Verbindung nutzt). Damit ist die Konfiguration des DNS-Servers abgeschlossen, nun prüfen wir den WINS-Server auf Funktionsfähigkeit: Start => Verwaltung => WINS.

In der WINS-Serverkonsole durch Klick auf das Pluszeichen den Baum erweitern und dann Rechtsklick auf "Aktive Registrierungen".



WINS anpassen

Aus dem Kontextmenü "Datensätze anzeigen..." wählen und im Dialogfeld "Einträge anzeigen" den Haken bei "Nach Einträgen mit diesem Namensmuster filtern" setzen. Um die Funktion zu überprüfen: die ersten drei, vier Buchstaben des Servernamens eingeben und auf "Suche starten" klicken.

Einträge anzeigen

Eintragszuordnung | Eintragsbesitzer | Eintragstypen

☒ Nach Einträgen mit diesem Namensmuster filtern:

Test

☐ Zwischen und Groß-/Kleinschreibung unterscheiden

☐ Nach Einträgen mit dieser IP-Adresse filtern:

☐ IP-Adresse dieser Subnetzmaske zuordnen:

Das Anzeigen von Einträgen der WINS-Datenbank kann sehr zeitaufwendig sein und viele Systemressourcen erfordern. Die Antwortzeit kann durch Datenbankfilterung nach Namenpräfix oder eindeutigem Besitzer erheblich verkürzt werden.

Wenn Sie die Ergebniszwischenspeicherung aktivieren, werden die darauf folgenden Abfragen schneller bearbeitet, aber der Arbeitsspeicherverbrauch steigt.

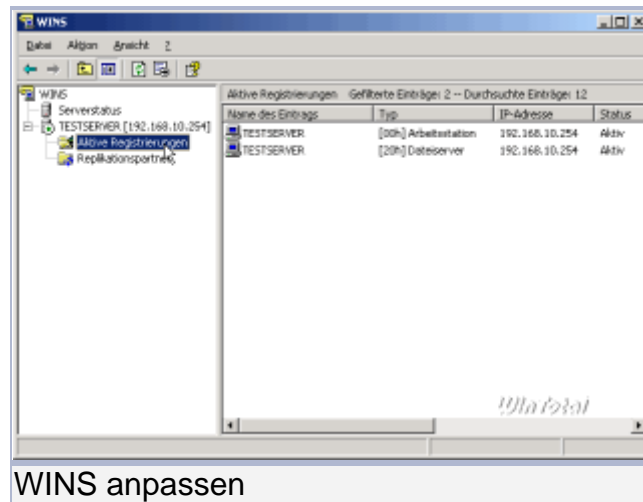
☐ Ergebniszwischenspeicherung aktivieren

Ullatotal

Suche starten Abbrechen

WINS testen

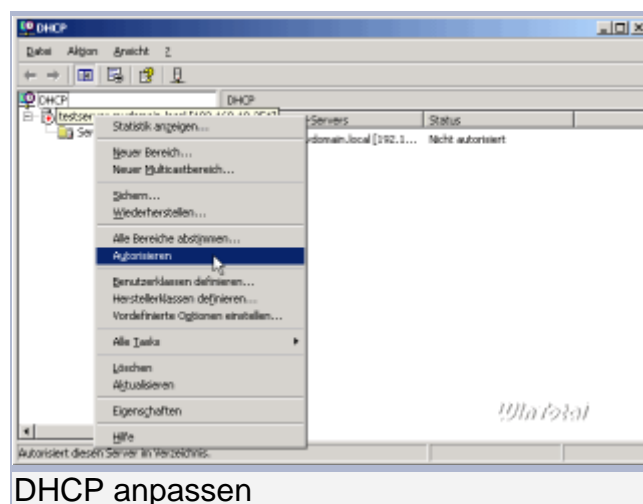
Das Ergebnis sollte so aussehen:



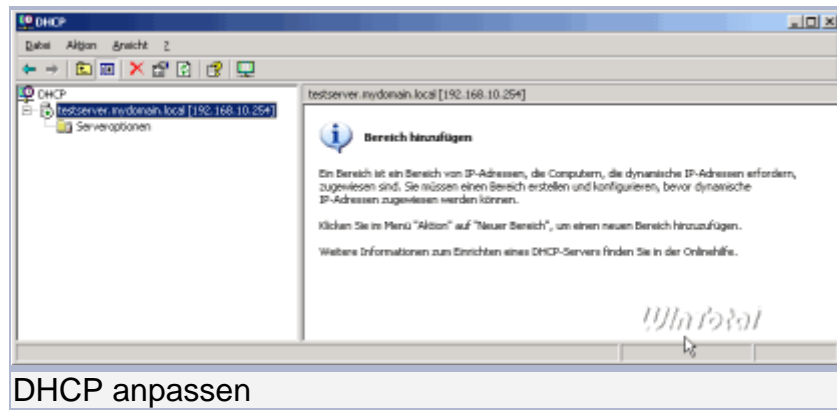
Damit ist der Funktionstest für den WINS-Server auch schon beendet, es bedarf für unsere Zwecke keiner weiteren Einstellungen.

Wenden wir uns nun der Konfiguration des DHCP-Servers zu: Dieser ist dafür verantwortlich, dass jeder Client vom Server eine passende TCP/IP-Konfiguration verpasst bekommt. Für uns wichtig sind die Einträge IP-Adresse, DNS-Server, WINS-Server und Gateway - mehr braucht es für unser kleines Netz nicht. Wichtig: Andere DHCP-Server, so wie sie meist in Routern implementiert sind, müssen abgeschaltet werden!

Die Konsole des DHCP-Servers starten wir über Start => Verwaltung => DHCP und erweitern die Struktur durch Klick auf das Pluszeichen. Noch ist der Server mit einem roten Pfeil gekennzeichnet, da er noch nicht autorisiert ist. Das ändern wir durch Rechtsklick auf den Servernamen und Auswahl von "Autorisieren" aus dem Kontextmenü.

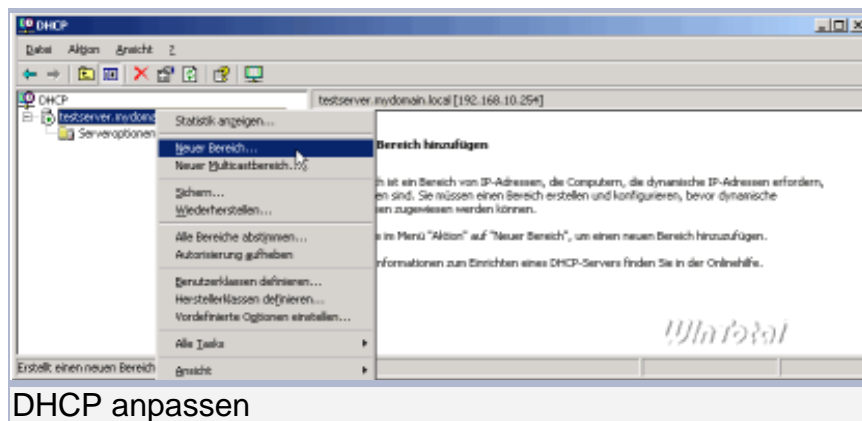


Nach kurzer Wartezeit (oder dem wiederholten Drücken von F5 oder Aktualisieren) springt die Anzeige um und der Server ist nun mit einem grünen Pfeil versehen, d.h. er ist nun autorisiert, in unserer Domäne zu starten.

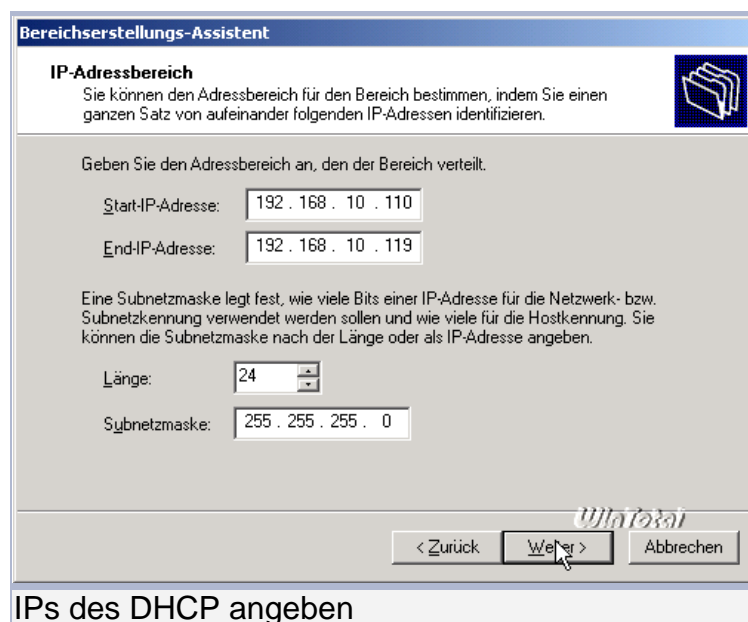


Zuallererst müssen wir nun einen IP-Bereich definieren, aus dem später die Clients ihre Adressen zugewiesen bekommen. Wählt diesen Bereich sorgfältig, nicht zu groß und nicht zu klein, er lässt sich im Nachhinein nicht mehr ändern; die Anzahl der IP-Adressen sollte also in etwa der Anzahl der Clients in eurem Netz entsprechen.

Zur Einrichtung eines Bereichs Rechtsklick auf den Servernamen und aus dem Kontextmenü "Neuer Bereich" auswählen.



Ich habe in meiner Testumgebung nur zehn Adressen gewählt.



Nach Klick auf "Weiter" erscheint der Dialog für Ausschlüsse, d.h. hier könnt ihr aus dem eben erstellten Bereich IP-Adressen ausschließen, bspw. wenn eine der IP-Adressen aus dem Bereich fest vergeben ist.

The screenshot shows the 'Bereichserstellungs-Assistent' (Area Creation Assistant) dialog box. The title bar says 'Bereichserstellungs-Assistent'. The main heading is 'Ausschlüsse hinzufügen' (Add exclusions). Below it, a text box explains: 'Ausschlüsse sind Adressen oder ein Adressbereich, die nicht vom Server verteilt werden.' (Exclusions are addresses or an address range that are not distributed by the server). To the right is a folder icon. The instructions state: 'Geben Sie den IP-Adressbereich an, den Sie ausschließen möchten. Wenn Sie eine einzelne IP-Adresse ausschließen möchten, geben Sie nur "Start-IP-Adresse" an.' (Specify the IP address range you want to exclude. If you want to exclude a single IP address, enter only "Start-IP-Adresse"). There are two input fields: 'Start-IP-Adresse:' and 'End-IP-Adresse:', each followed by a dotted box for IP entry. To the right of these is a 'Hinzufügen' (Add) button. Below these is a large empty box labeled 'Ausgeschlossener Adressbereich:' (Excluded address range). To its right is an 'Entfernen' (Remove) button. At the bottom right, there are three buttons: '< Zurück' (Back), 'Weiter >' (Next), and 'Abbrechen' (Cancel). A mouse cursor is pointing at the 'Weiter >' button. A 'WinTotal' watermark is visible in the bottom right corner of the dialog area.

Bereiche ausschließen

Ich habe keine Ausschlüsse definiert, da dies für mich nicht von Belang ist. Die Empfehlung von Microsoft geht auch dahin, statt mit Ausschlüssen lieber mit Bereichen zu arbeiten, in denen keine Ausschlüsse definiert werden müssen.

Der nächste Dialog betrifft die Leasedauer für die vom DHCP-Server vergebenen Einstellungen. Diese steht in der Standardeinstellung auf 8 Tage und kann für unsere Zwecke durchaus so belassen werden.

The screenshot shows the 'Bereichserstellungs-Assistent' (Area Creation Assistant) dialog box. The title bar says 'Bereichserstellungs-Assistent'. The main heading is 'Leasedauer' (Lease duration). Below it, a text box explains: 'Die Leasedauer bestimmt, für wie lange ein Client eine Adresse aus diesem Bereich verwenden kann.' (The lease duration determines for how long a client can use an address from this range). To the right is a folder icon. The instructions state: 'Die Leasedauer sollte normalerweise mit der durchschnittlichen Zeit übereinstimmen, die der Computer mit demselben Netzwerk verbunden ist. Für mobile Netzwerke, die überwiegend aus tragbaren Computern oder DFO-Clients bestehen, kann eine kürzere Leasedauer sinnvoll sein. Für ein stabiles Netzwerk hingegen, das überwiegend aus nicht-tragbaren Desktopcomputern besteht, ist eine längere Leasedauer angebracht. Legen Sie die Bereichsleasedauer für diesen Server fest.' (The lease duration should normally match the average time the computer is connected to the same network. For mobile networks, which consist mostly of portable computers or DFO clients, a shorter lease duration may be useful. For a stable network, however, which consists mostly of non-portable desktop computers, a longer lease duration is appropriate. Set the range lease duration for this server). Below this is the label 'Begrenzt auf:' (Limited to:). There are three spin boxes: 'Tage:' (Days) with the value '8', 'Stunden:' (Hours) with the value '0', and 'Minuten:' (Minutes) with the value '0'. At the bottom right, there are three buttons: '< Zurück' (Back), 'Weiter >' (Next), and 'Abbrechen' (Cancel). A mouse cursor is pointing at the 'Weiter >' button. A 'WinTotal' watermark is visible in the bottom right corner of the dialog area.

Gültigkeit festlegen

Nun kommen wir zu den interessanten Einstellungen, den DHCP-Optionen - ja, die möchten wir konfigurieren.

Bereichserstellungs-Assistent

DHCP-Optionen konfigurieren

Sie müssen die am häufigsten verwendeten DHCP-Optionen konfigurieren, bevor Clients diesen Bereich verwenden können.

Wenn Clients eine Adresse beziehen, erhalten sie DHCP-Optionen, wie z.B. Router-IP-Adressen (Standardgateways), DNS-Server und WINS-Einstellungen, für diesen Bereich.

Die Einstellungen, die Sie hier gewählt haben, gelten für diesen Bereich und überschreiben die Einstellungen, die im Ordner "Serveroptionen" für diesen Server konfiguriert wurden.

Möchten Sie jetzt die DHCP-Optionen für diesen Bereich konfigurieren?

☒ Ja, diese Optionen jetzt konfigurieren

☐ Nein, diese Optionen später konfigurieren

< Zurück Weiter > Abbrechen

DHCP-Optionen festlegen

Los geht es mit dem Eintrag für den Router (Standardgateway); hier trägt ihr die IP-Adresse eures Routers ein.

Bereichserstellungs-Assistent

Router (Standardgateway)

Sie können die Router oder Standardgateways angeben, die von diesem Bereich verteilt werden sollen.

Geben Sie eine IP-Adresse unten an, um die Adresse für einen Router, der von Clients verwendet wird, hinzuzufügen.

IP-Adresse:

192.168.10.100

Hinzufügen Entfernen Nach oben Nach unten

< Zurück Weiter > Abbrechen

Gateway angeben

Als Nächstes kommt der DNS-Server an die Reihe: Tragt bei "Servername" den voll qualifizierten Domainnamen (FQDN) des Servers (also servername.domain.tld, s. Abbildung) ein und klickt auf "Auflösen" - dies sollte die IP-Adresse des Servers als Ergebnis liefern, die wir dann auch übernehmen.

Bereichserstellungs-Assistent

Domänenname und DNS-Server
Das DNS (Domain Name System) ordnet Domännennamen zu und übersetzt die von Clients im Netzwerk verwendeten Domännennamen.

Sie können die übergeordnete Domäne festlegen, die die Clientcomputer im Netzwerk für die DNS-Namensauflösung verwenden sollen.

Übergeordnete Domäne:

Geben Sie die IP-Adresse für die Server an, um Bereichsclients zur Verwendung von DNS-Servern im Netzwerk zu konfigurieren.

Servername: IP-Adresse:

< Zurück Weiter > Abbrechen

Ullatotal

Domäne und DNS

Nach dem DNS- kommt der WINS-Server an die Reihe, hier funktioniert das ähnlich. Bei "Servername" tragt ihr den NetBIOS-Namen des Servers ein und klickt auf Auflösen, das liefert wieder die IP-Adresse des Servers zurück, die wir übernehmen.

Bereichserstellungs-Assistent

WINS-Server
Computer, auf denen Windows ausgeführt wird, können WINS-Server dazu verwenden, NetBIOS-Computernamen in IP-Adressen umzuwandeln.

Die Angabe von Server-IP-Adressen ermöglicht Windows Clients, WINS abzufragen, bevor Broadcasts zur Registrierung und Auflösung von NetBIOS-Namen verwendet werden.

Servername: IP-Adresse:

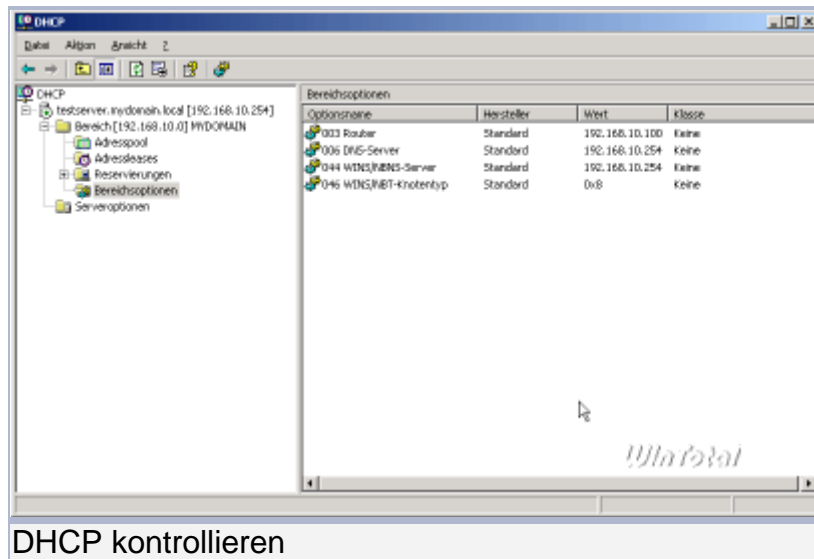
Ändern Sie die Option 046, Knotentyp WINS/NBT, in den Bereichsoptionen, um dieses Verhalten für Windows DHCP-Clients zu ändern.

< Zurück Weiter > Abbrechen

Ullatotal

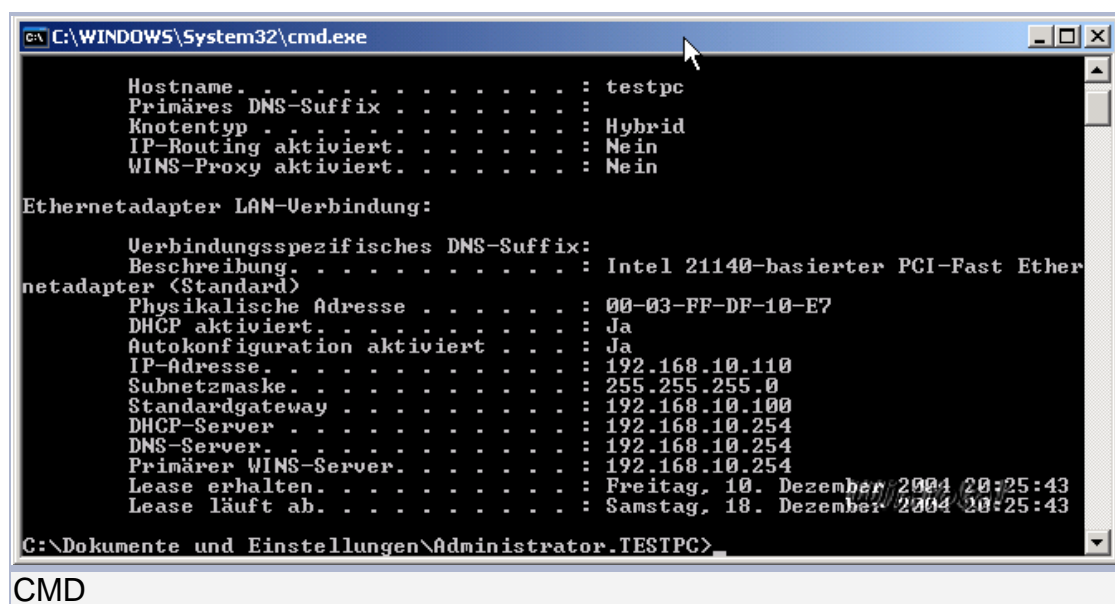
WINS

Damit sind alle für uns relevanten Einstellungen getätigt, der DHCP-Server ist erstmal funktionstüchtig. Klickt im linken Baum auf den Eintrag "Bereichsoptionen", um die eben gemachten Einstellungen zu kontrollieren.



Nun können wir den ersten Client in die Domäne heben. Ich gehe hier von XP-Clients aus, Win2000 funktioniert aber beinahe analog. Die Clients sollten für die Verwendung von DHCP konfiguriert sein, d.h. in den TCP/IP-Eigenschaften sollte "IP-Adresse automatisch beziehen" und "DNS-Serveradresse automatisch beziehen" angehakt sein. Die Clients funktionieren natürlich auch mit statischen IP-Adressen innerhalb der Domäne - dazu hätten wir aber den DHCP-Server nicht konfigurieren müssen. Verbindet also einen Client mit dem Switch/Hub, an dem auch der Server hängt und startet ihn. Nach der - noch lokalen - Anmeldung könnt ihr kontrollieren, ob der DHCP-Server ordentlich seine Arbeit macht: einmal am Server selbst in der DHCP-Serverkonsole und einmal mittels ipconfig /all direkt am Client. Wichtig ist neben der passenden IP-Adresse, dass als primärer DNS-Server die IP-Adresse des DC eingetragen ist.

So sieht das dann bei mir aus:



Wenn die Einstellungen stimmen, geht am Client wie folgt vor:
Start => Systemsteuerung => System => Registerkarte "Computernamen" => Ändern
Bei "Mitglied von" aktiviert ihr "Domäne" und tragt dann den Namen eurer Domäne ein - entweder als NetBIOS-Namen in der Form MYDOMAIN oder als FQDN in der Form mydomain.local.

Computernamen ändern

Sie können den Namen und Mitgliedschaft dieses Computers ändern. Dies kann Auswirkungen auf Zugriffsrechte auf Netzwerkressourcen haben.

Computername:
testpc

Vollständiger Computername:
testpc.

Weitere...

Mitglied von:

☒ Domäne:
mydomain.local

☐ Arbeitsgruppe:
ARBEITSGRUPPE

OK Abbrechen

Client in die Domäne setzen

Nun müsst ihr einen Benutzer angeben, der den Rechner in die Domäne heben darf, wählt hier bitte DOMAIN\Administrator.

Computernamen ändern

Geben Sie Namen und Kennwort eines Kontos mit der Berechtigung dieser Domäne beizutreten ein.

Benutzername: MYDOMAIN\Administrator

Kennwort:

OK Abbrechen

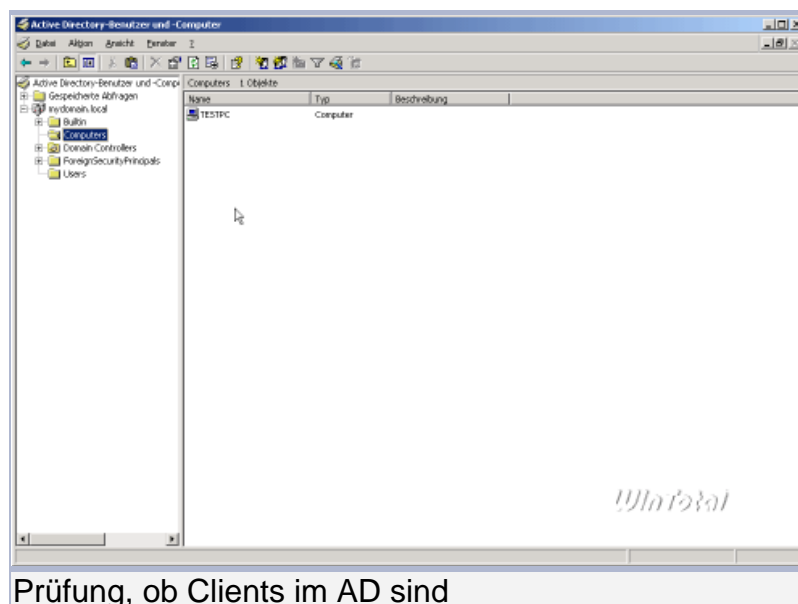
Client in die Domäne setzen

Das bestätigt ihr mit OK, dann erhaltet ihr den Hinweis "Willkommen in der Domäne DOMAINNAME". Nach Bestätigung aller Dialoge mit OK muss der fällige Neustart erstmal durchgeführt werden. Hinweis: Ändert niemals Computernamen und Domain-Zugehörigkeit in einem Schritt, das führt zwangsläufig zu Problemen, weil Windows den Client erst mit seinem alten Namen in der Domäne registriert und ihn dann umbenennt. Das führt dann dazu, dass nach dem Reboot keine Anmeldung an der Domäne möglich ist, da es kein passendes Computerkonto gibt. Umbenennen eines Clients also bitte vor dem Hineinheben in die Domäne durchführen oder danach, beides geht problemlos. Nach dem Reboot klickt ihr im Anmeldedialog nach STRG+ALT+ENTF bitte unten rechts auf "Optionen" - es erscheint nun ein drittes Feld im Login-Dialog: Anmelden an. Die erste Domänen-Anmeldung machen wir in diesem Fall mit dem Administrator-Account, da wir ja noch keine User angelegt haben. Gebt also als Benutzername Administrator ein, das entsprechende Kennwort und wählt bei "Anmelden an" euren Domänennamen aus (der hier nur im NetBIOS-Format erscheint).



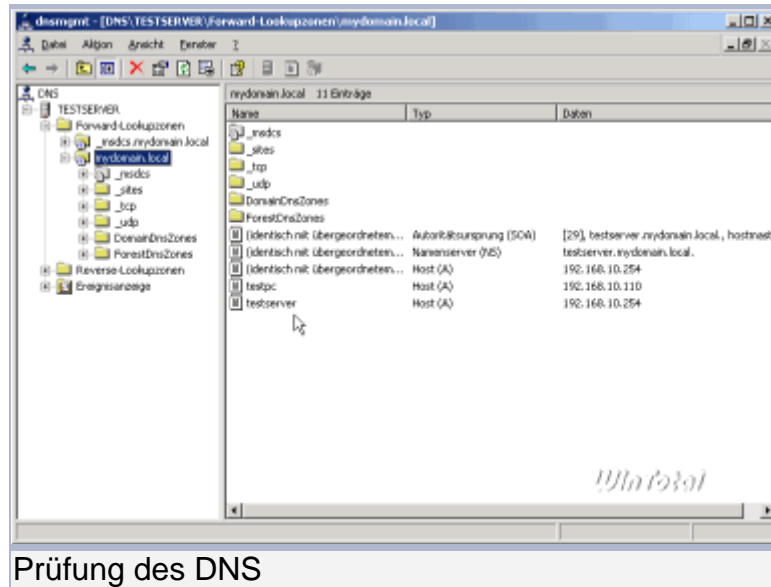
Anmeldung an der Domäne

Damit ist dieser Client nun Mitglied eurer Domäne, was ihr natürlich auch kontrollieren könnt: Startet am Server das MMC-SnapIn "Active Directory Benutzer- und Computer" (Start => Verwaltung), erweitert euren Domänenbaum und schaut in den Container "Computers" - hier ist das Computerkonto des Clients zu finden, welches beim Hineinheben in die Domäne automatisch erstellt wurde.



Prüfung, ob Clients im AD sind

Wenn ihr über Start => Verwaltung => DNS die DNS-Serverkonsole startet und die Zonen für eure Domäne überprüft, werdet ihr dort ebenfalls einen neuen Eintrag mit dem Hostnamen eures Clients finden. Der Client aktualisiert diese DNS-Einträge automatisch, wenn ihr den Client also jetzt umbenennt, wird er nach dem Reboot mit dem neuen Namen automatisch in DNS registriert.



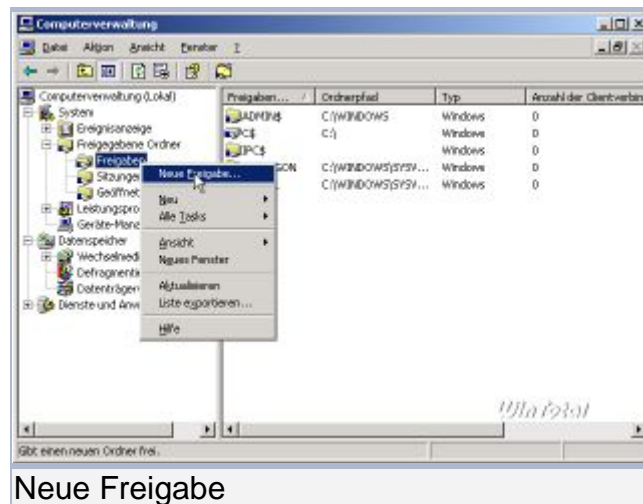
Damit ist Teil 3 des Artikels abgeschlossen. Teil 4 beschreibt dann das Anlegen von Usern, Zuweisen von Berechtigungen, DHCP-Reservierungen, servergespeicherte Profile usw.

Teil 4

Erstellen der benötigten Freigaben, Anlegen von Usern Zuweisen Basis- und Profilordner Einführung Gruppenrichtlinien

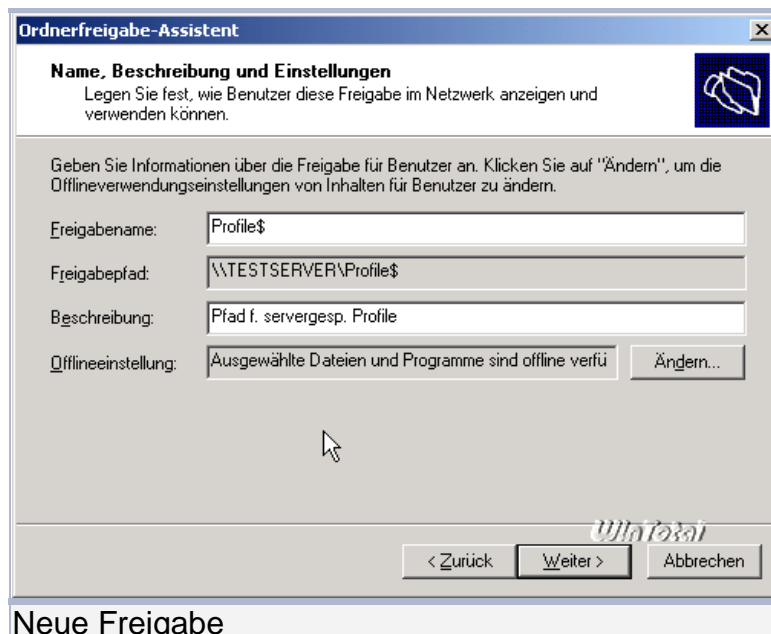
Wir beginnen Teil 4 mit der Vorbereitung für das Anlegen der User, d.h. wir erstellen die Freigaben für die Profile und das Home-Laufwerk der User. Ich habe mich in diesem Fall für versteckte Freigaben entschieden, die später in der Netzwerkumgebung bzw. mit net view an der Konsole nicht sichtbar sind. Versteckte Freigaben tragen ein \$-Zeichen am Ende des Freigabennamens.

Legt auf einem Laufwerk eures Servers zwei Verzeichnisse an, eines mit dem Namen Profile und eines mit dem Namen User. Zum Freigeben dieser Verzeichnisse öffnen wir über "Start" => "Verwaltung" die Computerverwaltung und navigieren im linken Baum zu "Freigegebene Ordner" => "Freigaben". Ein Rechtsklick auf "Freigaben" fördert das Kontextmenü zu Tage.



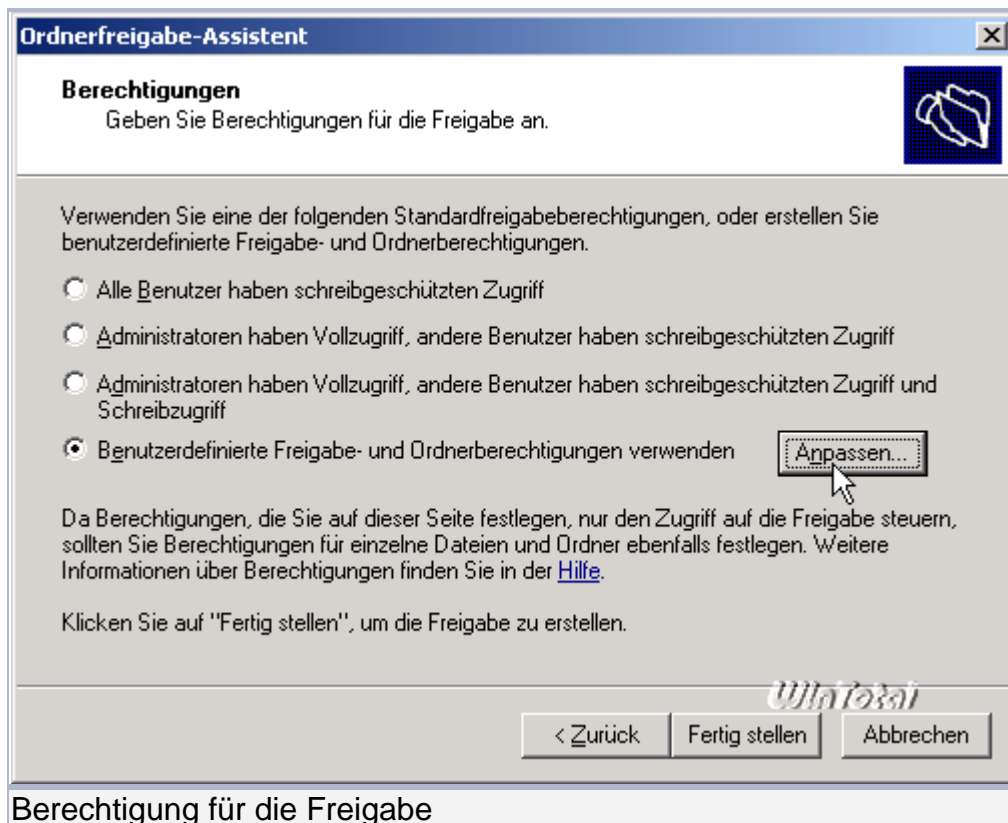
Neue Freigabe

Gebt nun die benötigten Daten ein.



Neue Freigabe

Dann setzen wir die Berechtigungen für diese Freigabe.

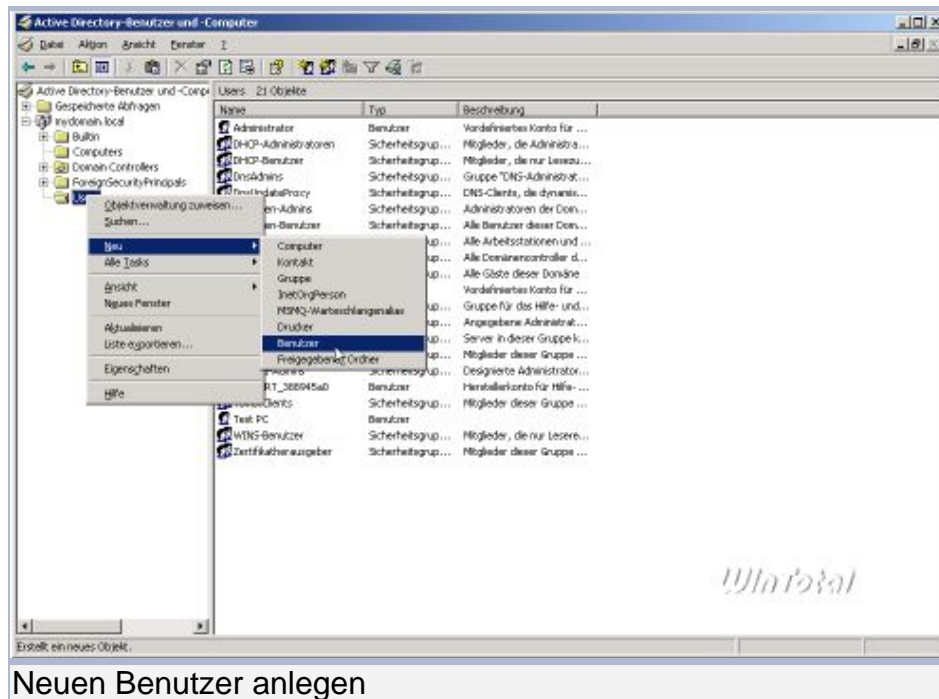


Fügt "Domänen-Benutzer" und "Domänen-Admin" hinzu und gebt beiden Gruppen Vollzugriff. Erst dann entfernt ihr "JEDER" aus den Freigabeberechtigungen und klickt of OK.



Das wiederholt ihr nun mit dem Verzeichnis "User" und setzt die Berechtigungen genau wie auch für das Profilverzeichnis.

Nun können wir den ersten User im [Active Directory](#) anlegen. Dazu starten wir über "Start" => "Verwaltung" das SnapIn "Active Directory Benutzer- und Computer" und navigieren im linken Baum zu "Users". Auf den Eintrag "Users" einen Rechtsklick und aus dem Kontextmenü dann "Neu" => "Benutzer" auswählen.



Das Anlegen eines Users ist beinahe selbsterklärend. Ihr ändert natürlich "TestUser" in einen brauchbaren Benutzernamen.

The screenshot shows the 'Neues Objekt - Benutzer' dialog box. It contains fields for creating a new user. The 'Erstellen in:' field is set to 'mydomain.local/Users'. The 'Vorname:' field is 'Test', 'Nachname:' is 'User', and 'Vollständiger Name:' is 'Test User'. The 'Benutzeranmeldename:' field is 'TestUser' and the domain dropdown is '@mydomain.local'. The 'Benutzeranmeldename (Prä-Windows 2000):' field is 'MYDOMAIN\'. The 'Weiter >' button is highlighted.

Erstellen in: mydomain.local/Users

Vorname: Test Initialen:

Nachname: User

Vollständiger Name: Test User

Benutzeranmeldename: TestUser @mydomain.local

Benutzeranmeldename (Prä-Windows 2000): MYDOMAIN\ TestUser

< Zurück Weiter > Abbrechen

Neuer Account

Nun noch ein Kennwort vergeben, dieses sollte mindestens 7 Zeichen lang sein und einen Großbuchstaben und/oder eine Zahl enthalten. Namensbestandteile sind nicht erlaubt, so will es die Kennwort-Komplexitäts-Richtlinie von Windows Server 2003.

Neues Objekt - Benutzer

Erstellen in: mydomain.local/Users

Kennwort:

Kennwort bestätigen:

☒ Benutzer muss Kennwort bei der nächsten Anmeldung ändern

☐ Benutzer kann Kennwort nicht ändern

☐ Kennwort läuft nie ab

☐ Konto ist deaktiviert

< Zurück Weiter > Abbrechen

Passwort vergeben

Nachdem der User angelegt ist, erscheint er im Container "Users" auf der rechten Seite. Ein Doppelklick auf den User öffnet den Eigenschaften-Dialog, in dem ihr auf die Registerkarte "Profil" wechselt und folgende Einstellungen vornehmt.

Eigenschaften von Test User

Mitglied von | Einwählen | Umgebung | Sitzungen

Remoteüberwachung | Terminaldienstprofile | COM+

Allgemein | Adresse | Konto | Profil | Rufnummern | Organisation

Benutzerprofil

Profilpfad: \\TESTSERVER\\PROFILE\$\\%USERNAME%

Anmeldeskript:

Basisordner

☐ Lokaler Pfad:

☒ Verbinden von: U: mit: RVER\\USER\$\\%USERNAME%

OK Abbrechen Übernehmen

Profilpfad und Basisordner vorgeben

Die Variable %USERNAME% wird dabei durch den eigentlichen Usernamen ersetzt, was ihr durch erneutes Aufrufen der Eigenschaften des Users kontrollieren könnt.

Mit OK speichert ihr diese Einstellungen ab, die Einrichtung des ersten Users ist damit erstmal abgeschlossen: Der Profilpfad ermöglicht das Anmelden an jedem x-beliebigen Rechner im Netz, da der User nun ein servergespeichertes Profil besitzt. Der Basisordner ist ebenfalls von jedem Rechner im Netz aus verfügbar, im nächsten Schritt wird dann z.B. der Ordner "Eigene Dateien" via Gruppenrichtlinie in diesen Pfad umgeleitet (da er standardmäßig im Profilpfad gespeichert wird und somit die An-/Abmeldung mitunter recht lange dauern kann).

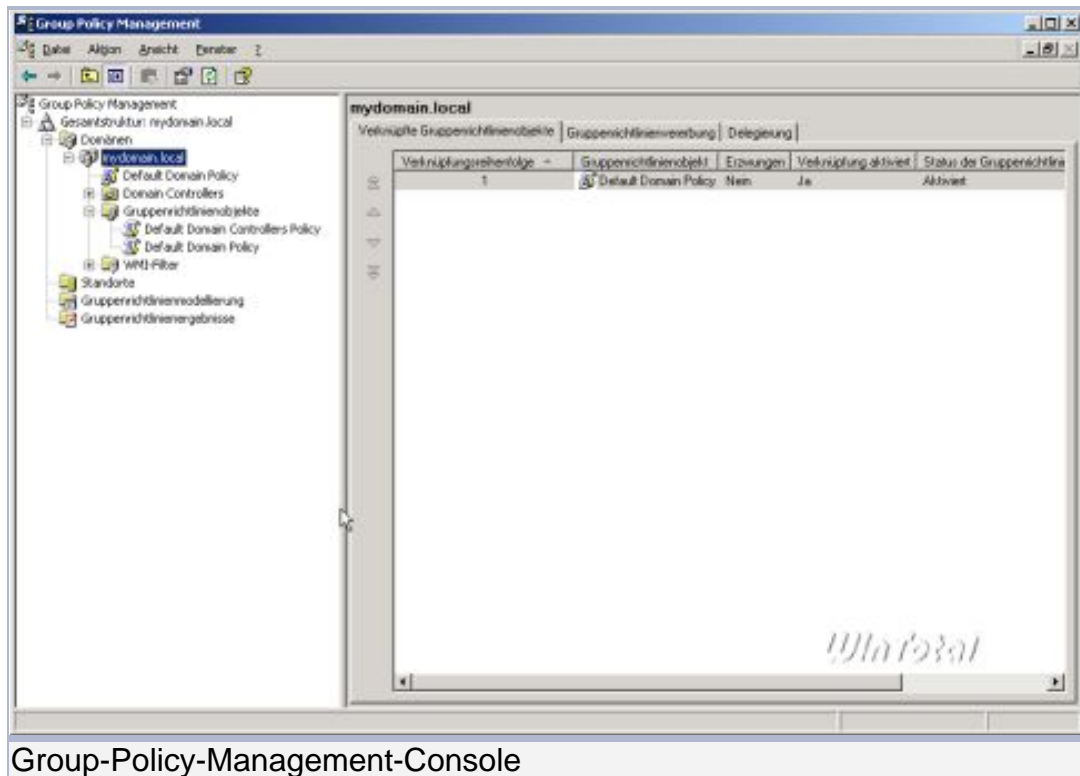
Des Weiteren werden wir über Gruppenrichtlinien die Berechtigungen der User an den Clients definieren, d.h. via Gruppenrichtlinie wird definiert, ob und welcher User an welchem Client Admin-Rechte bekommt usw.

Das Bearbeiten der Gruppenrichtlinien realisiert man am besten mit der Group-Policy-Management-Console, kurz GPMC. Diese ist bei Microsoft zum Download erhältlich, aber aufgepasst, es gibt sie in verschiedenen Sprachen und Versionen. Die aktuell für uns benötigte Version ist die GPMC 1.01 SP1 deutsch. Hier der Download-Link: <http://WinTotal.de/softw/index.php?id=2545>

Installiert diese bitte direkt auf dem Server. Wie man von einem Client aus die Domäne administriert, wird Thema eines der nächsten Artikelteile werden.

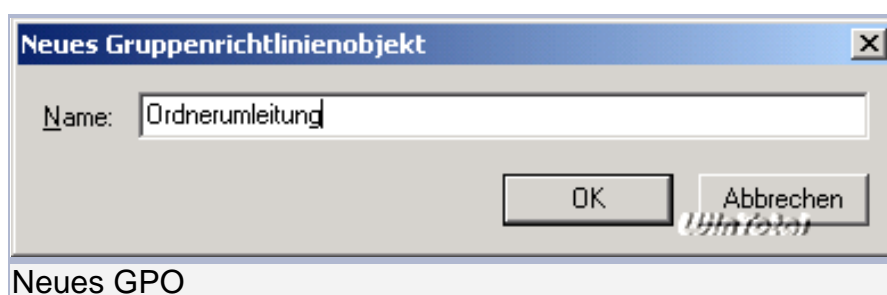


Ihr findet die GPMC nach der Installation unter Start => Verwaltung => Gruppenrichtlinienverwaltung.

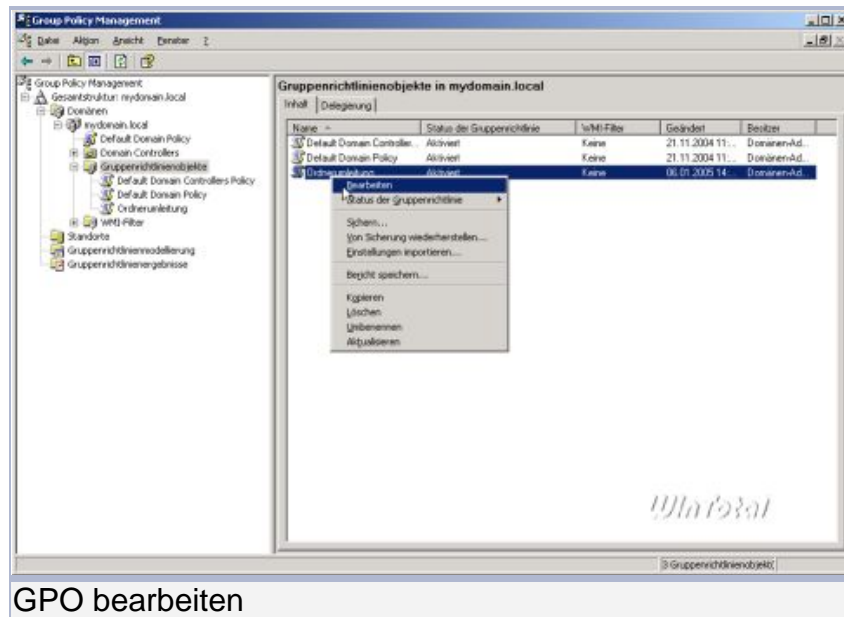


Finger weg von der "Default Domain Policy" und der "Default Domain Controllers Policy" - falsche Einstellungen können die komplette Domäne lahm legen. Einzig die Kennwort-Komplexität muss und kann ausschließlich über die "Default Domain Policy" gesteuert werden, für alles andere erstellen wir uns eigene Gruppenrichtlinien-Objekte, kurz GPOs.

Zum Erstellen einer neuen Richtlinie Rechtsklick auf den Container "Gruppenrichtlinienobjekte" => "Neu". Benennt das neue GPO nach dessen Funktion:

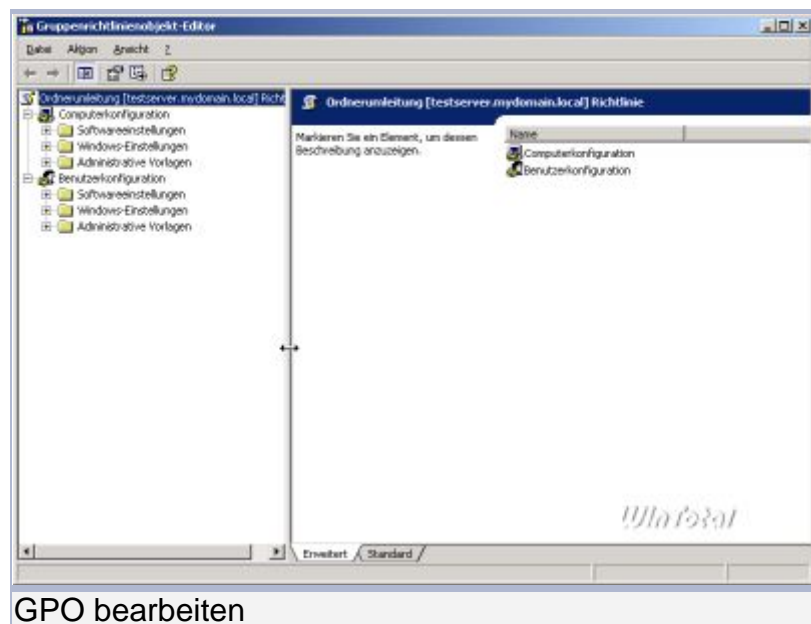


Zum Bearbeiten des GPO in der Auflistung auf der rechten Seite das Objekt "Ordnerumleitung" rechts anklicken und "Bearbeiten" wählen.



GPO bearbeiten

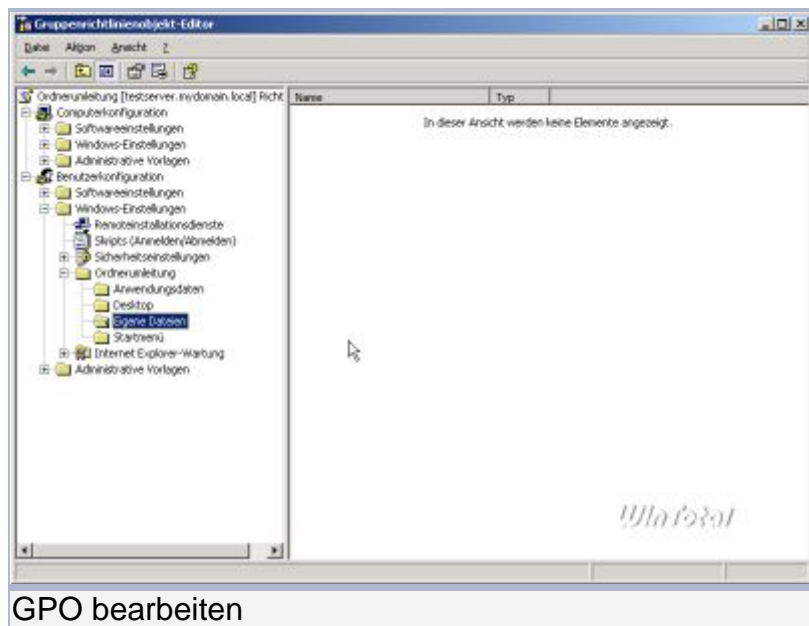
Wie ihr seht, sind die Gruppenrichtlinien unterteilt in Computer- und Benutzerkonfiguration, soll heißen: Richtlinien, die unter Computerkonfiguration eingestellt werden, wirken sich unabhängig vom angemeldeten Benutzer auf jeden Rechner aus, für den dieses GPO gültig ist.



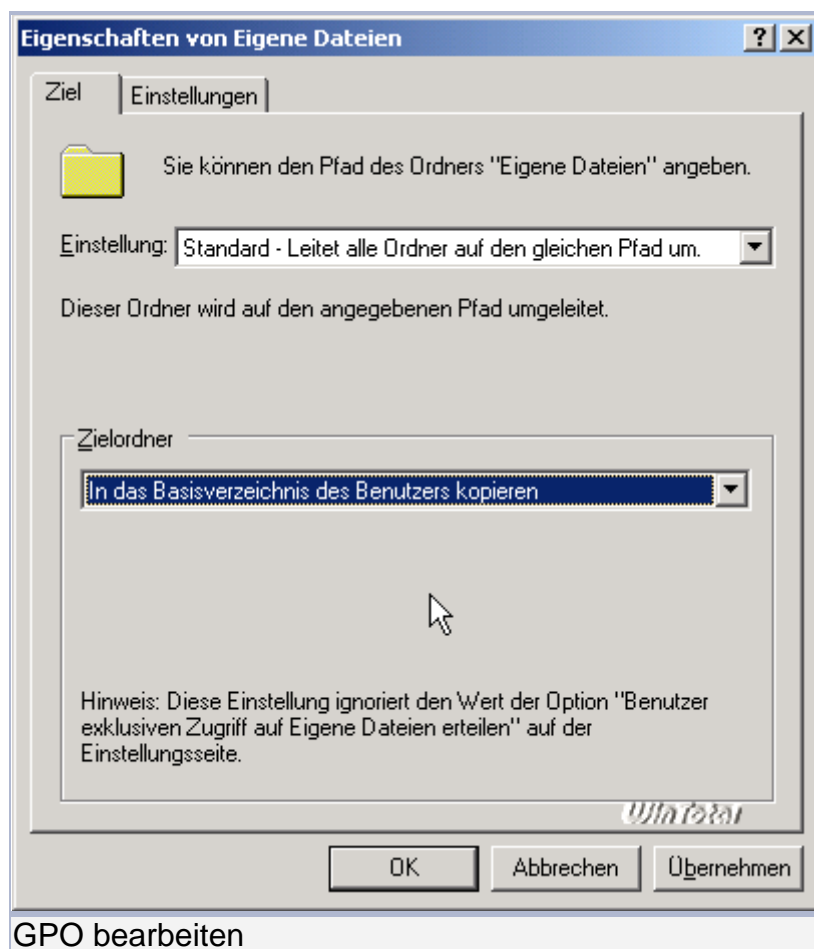
GPO bearbeiten

Die unter Benutzerkonfiguration eingestellten Richtlinien greifen an jedem Rechner, an dem sich ein bestimmter Benutzer anmeldet und zwar nur für ihn.

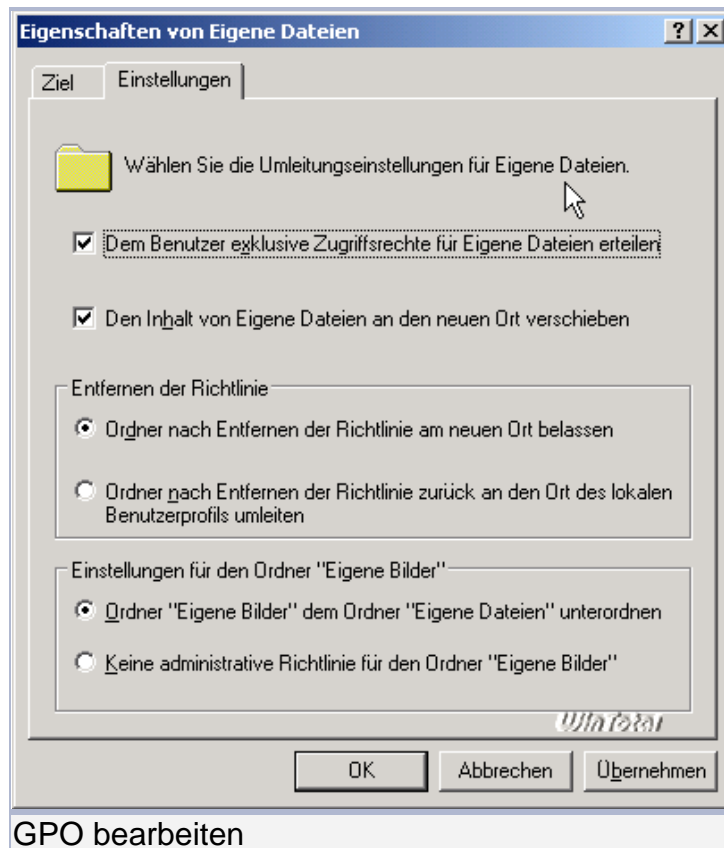
Wir wollen hier eine Ordnerumleitung konfigurieren, das ist eine Benutzereinstellung:



Ein Rechtsklick auf "Eigene Dateien" => "Eigenschaften" fördert den Optionen-Dialog zu Tage, den ihr wie folgt einstellt:

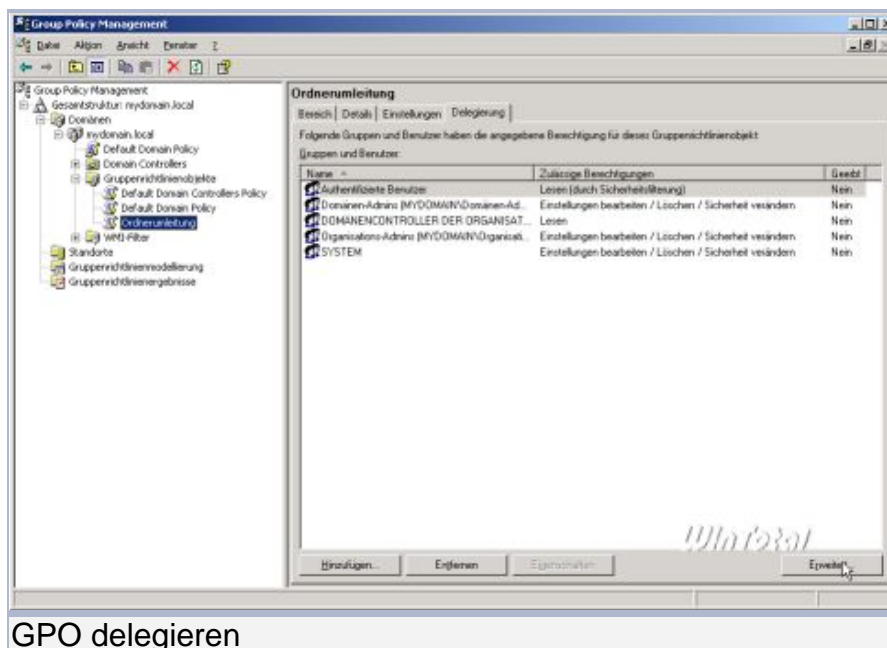


Auf der Registerkarte "Einstellungen" nehmt ihr folgende Einstellungen vor und bestätigt mit OK.

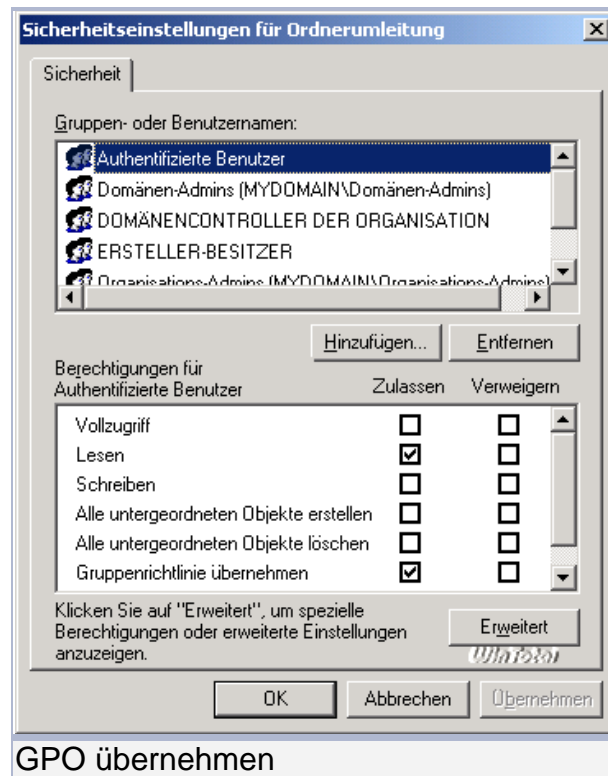


Nun schließt ihr den Gruppentrichtlinienobjekte-Editor und gelangt wieder in die GPMC zurück. Hier müssen wir nun noch das neue GPO verknüpfen und festlegen, für wen es gültig sein soll.

Markiert im Container "Gruppenrichtlinienobjekte" den Eintrag "Ordnerumleitung" und klickt dann im rechten Fenster die Registerkarte "Delegation" an.

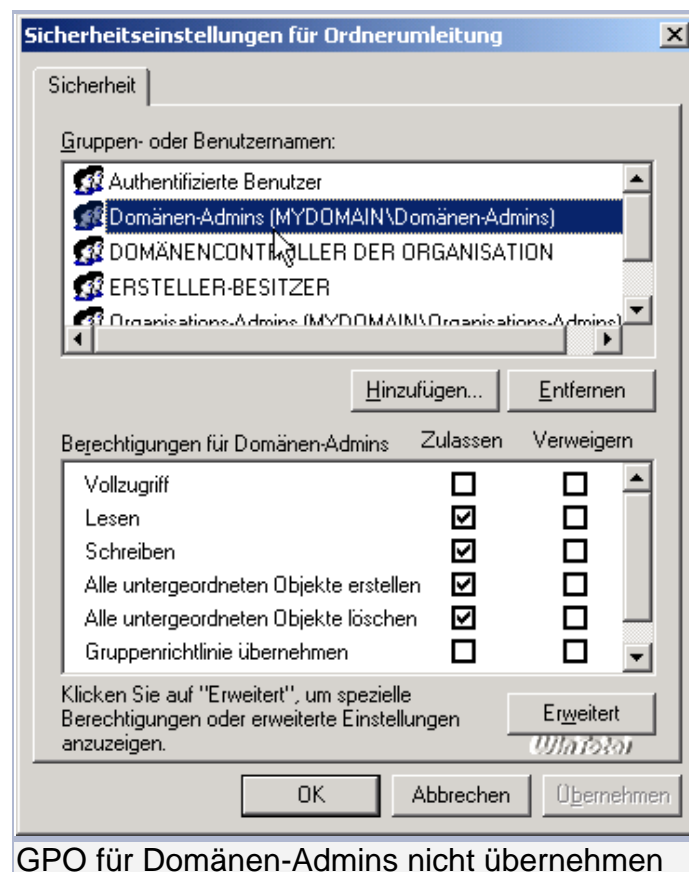


Nun klickt unten rechts auf "Erweitert". Achtet darauf, dass bei "Authentifizierte Benutzer" der Haken bei "Gruppenrichtlinie übernehmen" bei "Zulassen" gesetzt ist.



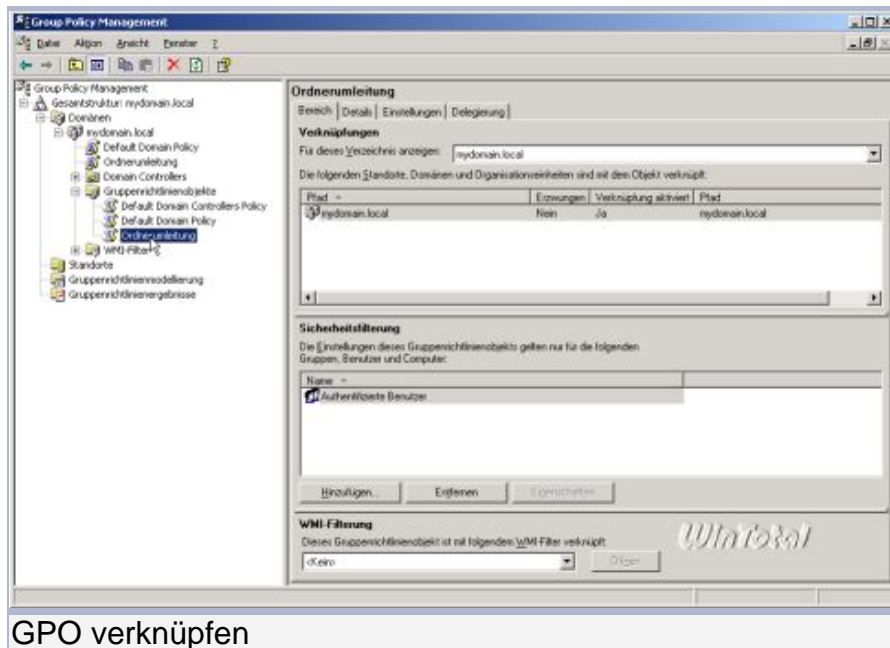
GPO übernehmen

Für die Domänen-Administratoren darf der Haken hingegen nicht gesetzt sein.



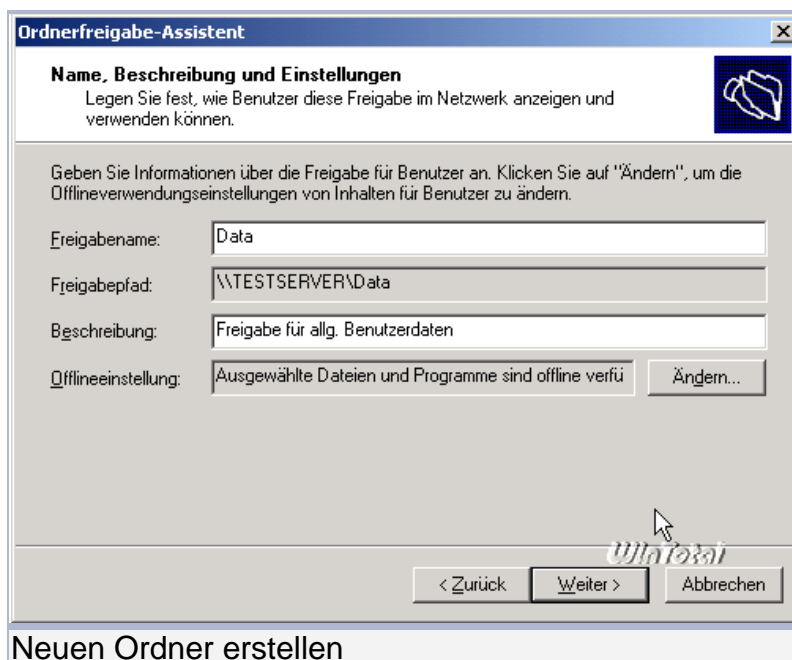
GPO für Domänen-Admins nicht übernehmen

Nun ist das GPO fertig eingerichtet, aber noch nicht verknüpft, d.h. noch nicht aktiv. Um es zu verknüpfen, nehmt ihr das GPO "Ordnerumleitung" und zieht es bei gedrückter linker Maustaste auf den Eintrag "mydomain.local" bzw. auf den Eintrag, der eurem Domainnamen entspricht.



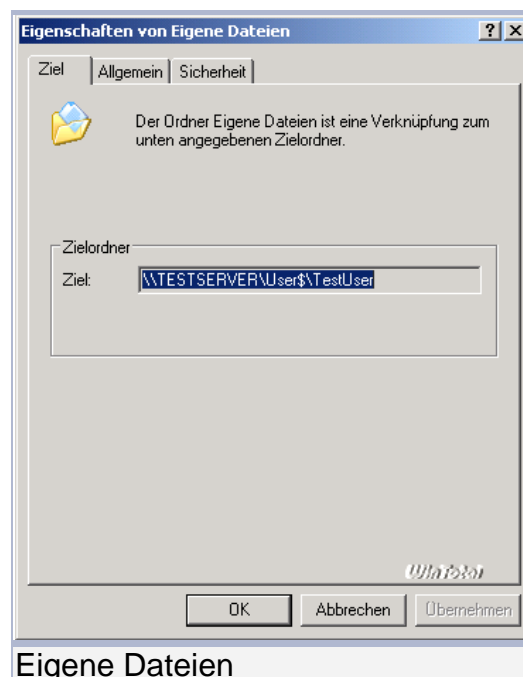
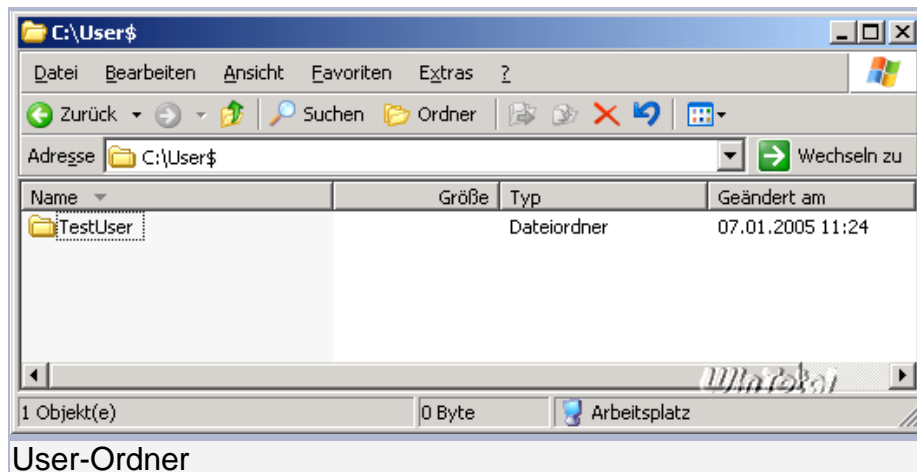
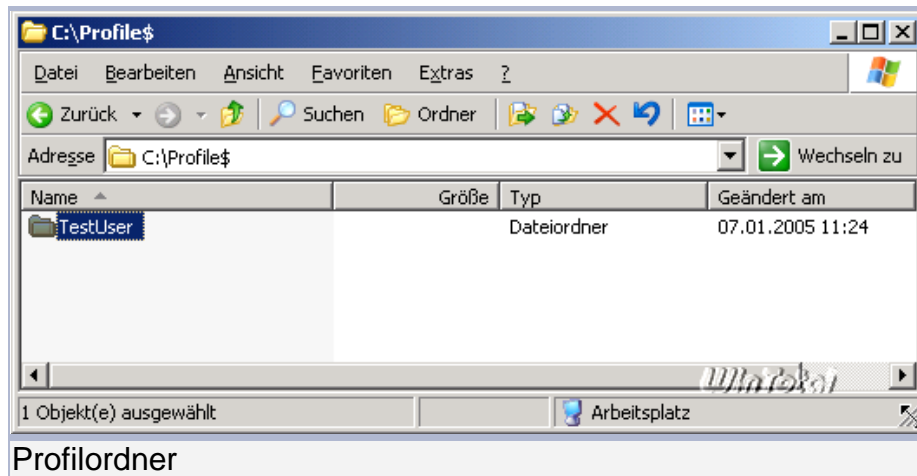
GPO verknüpfen

Bevor wir uns nun mit dem neu angelegten User erstmalig von einem Client aus anmelden, muss auf dem Server noch eine Datenfreigabe (oder gleich mehrere) erstellt werden, die dann später vom Client aus via "Netzlaufwerk verbinden" bzw. via Anmeldeskript zur Verfügung gestellt wird. Dazu erstellen wir auf dem Server einen neuen Ordner (den wir dann freigeben werden) und nennen ihn z.B. Data, dann starten wir die Computerverwaltung und navigieren im linken Baum zu "Freigegebene Ordner" => "Freigaben". Das Erstellen einer neuen Freigabe für den Ordner "Data" erfolgt analog zur Freigabe der Profil- und Basisordner, einziger Unterschied: Der Freigabename bekommt jetzt KEIN \$-Zeichen angehängt.



Neuen Ordner erstellen

Die Freigabeberechtigungen setzt ihr genau wie für Profil- und Basisordner auch. Nun ist es an der Zeit, sich das erste Mal vom Client aus mit dem neu angelegten User an der Domäne anzumelden. Nach der erfolgten Anmeldung sehen die Verzeichnisse auf dem Server so aus:



Des Weiteren seht ihr auf dem Client im Arbeitsplatz/Explorer ein Laufwerk U:, das direkt auf den Server verbunden ist - dies ist der Basisordner, den wir in den Eigenschaften des Users beim Anlegen eingetragen haben.

Für euch wird es nun Sinn machen, die hier gezeigten Schritte zu wiederholen und erstmal alle für euer Netz benötigten Benutzer anzulegen sowie die benötigten Datenfreigaben auf dem Server. Des Weiteren solltet ihr euch Gedanken darüber machen, welcher User auf welchem Rechner welche Berechtigungen bekommt und welche Netzlaufwerke pro User verbunden werden sollen - alles Punkte, die in Teil 5 via Gruppenrichtlinie eingestellt werden.

Bis dahin sei euch die Lektüre von Mark Heitbrinks Webprojekt www.gruppenrichtlinien.de ans Herz gelegt - zumindest denjenigen, die künftig mehr über GPOs regeln wollen.

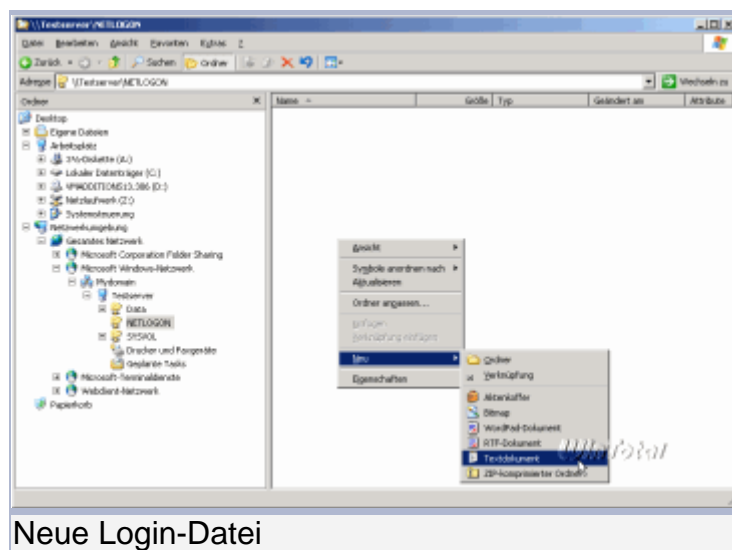
Teil 5

Erstellen und Verknüpfen eines Login-Skripts Setzen von lokalen Berechtigungen DHCP-Reservierungen für die Clients

Erstellen und Verknüpfen eines Login-Skripts

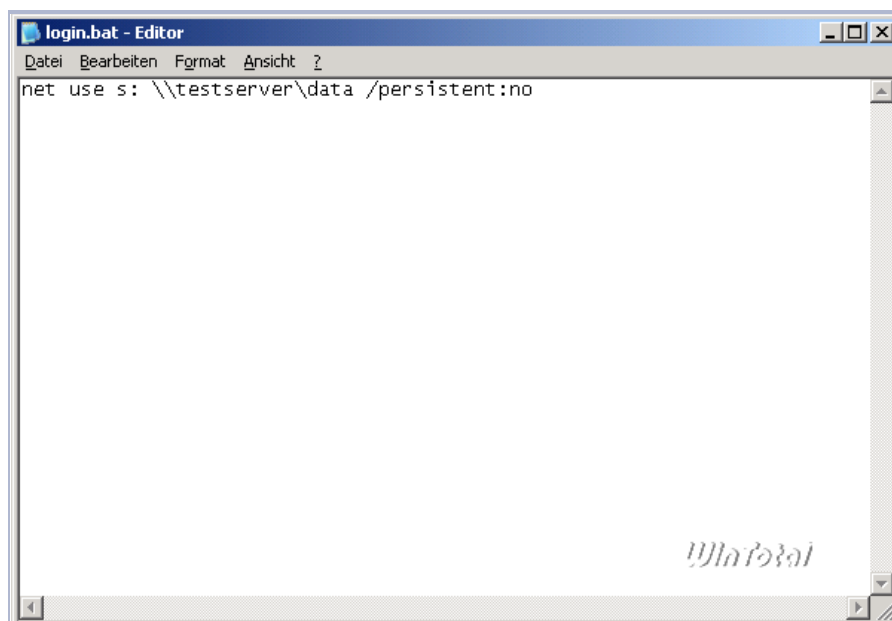
Dieser Teil beginnt mit der Erstellung eines einfachen Login-Skripts, welches bei der Anmeldung eines Users den Laufwerksbuchstaben S: mit der Freigabe DATA auf dem Server verbindet.

Dazu öffnen wir auf dem Server den Explorer, navigieren zum Ordner NETLOGON und erstellen dort eine neue Textdatei namens login.bat.

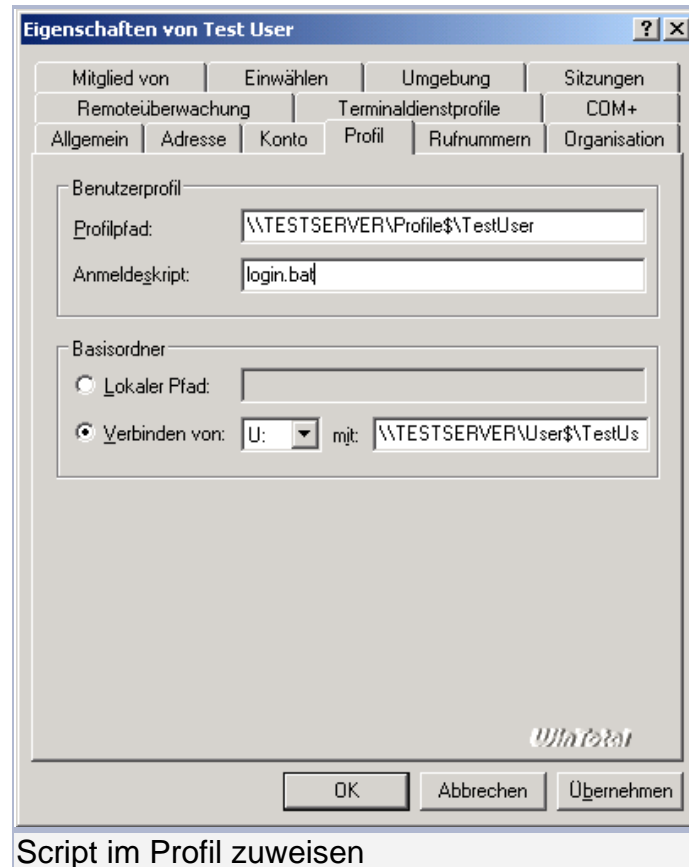


Neue Login-Datei

Achtet darauf, dass ihr unter Ordneroptionen den Haken bei "Erweiterungen bei bekannten Dateitypen ausblenden" entfernt habt, sonst heißt euer Skript login.bat.txt und wird nicht funktionieren. Das Skript selbst ist sehr einfach:

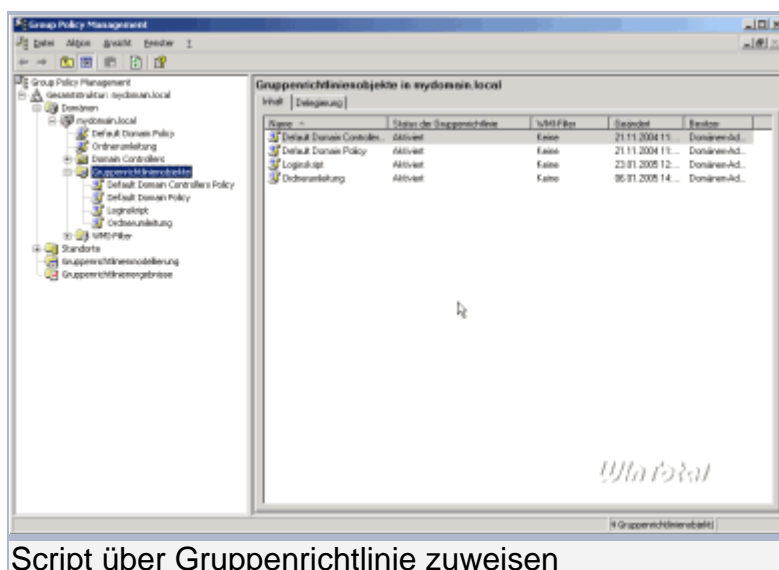


Nach dem Speichern des Skripts gilt es nun, dieses den Usern zuzuordnen, dazu gibt es zwei Wege: Der "klassische" Weg - der diejenigen, die mal mit NT gearbeitet haben, bekannt sein dürfte - ist der, das Skript bei jedem User einzeln in den Eigenschaften des Kontos einzutragen. Das geht mittels des SnapIns "Active Directory Benutzer- und Computer" => Doppelklick auf das User-Konto => Registerkarte Profil.



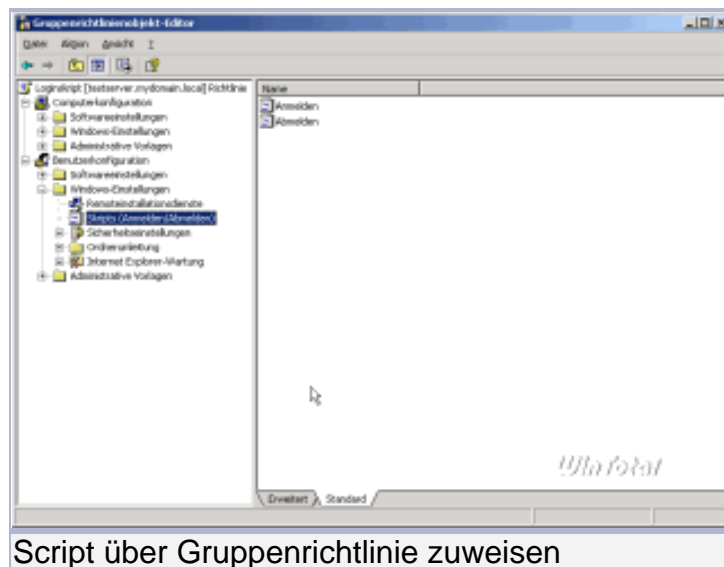
Script im Profil zuweisen

Bei einer Hand voll User ist das sicherlich nicht das Problem, aber es geht auch geschickter, indem man das Login-Skript via Gruppenrichtlinie einbindet. Dazu starten wir die GPMC und erstellen uns ein neues GPO mit dem Namen Loginskript.



Script über Gruppenrichtlinie zuweisen

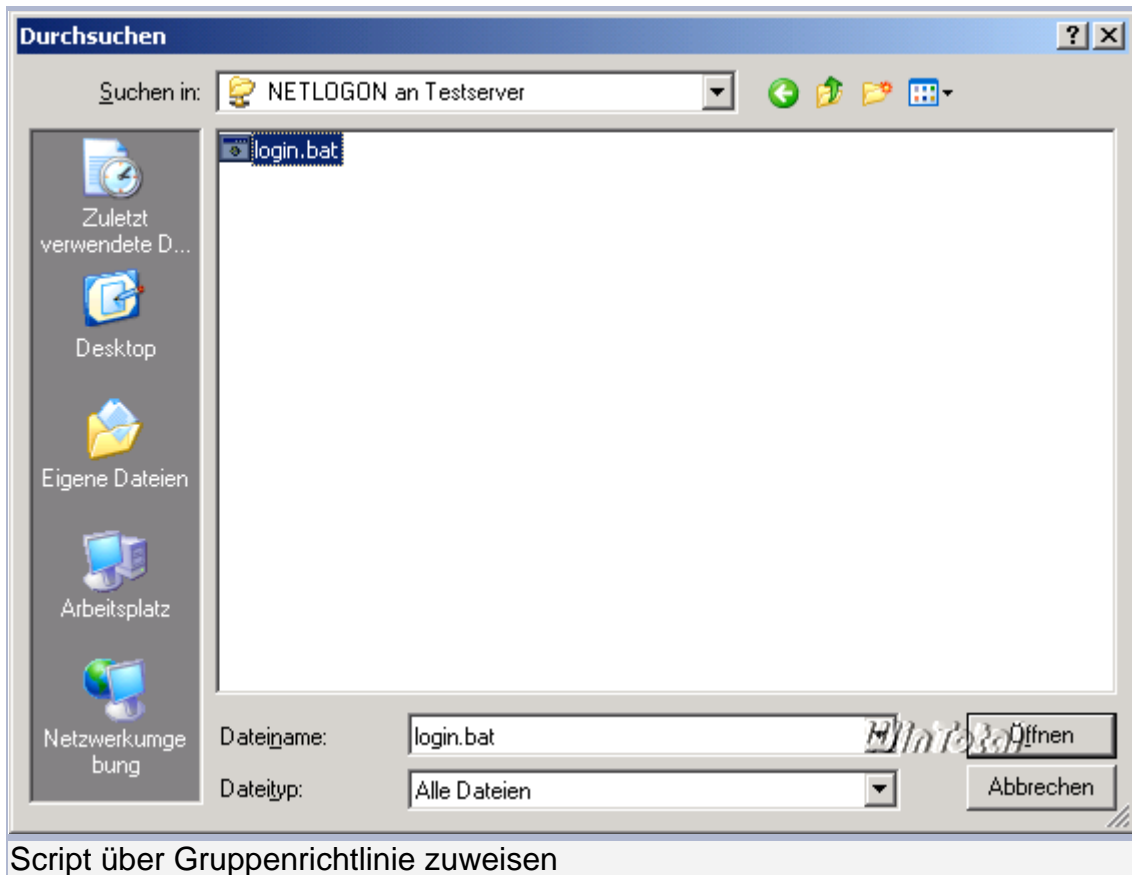
Dieses neue GPO klicken wir mit der rechten Maustaste an, wählen "Bearbeiten" und navigieren zu Benutzerkonfiguration => Windows-Einstellungen => Skripts (Anmelden/Abmelden).



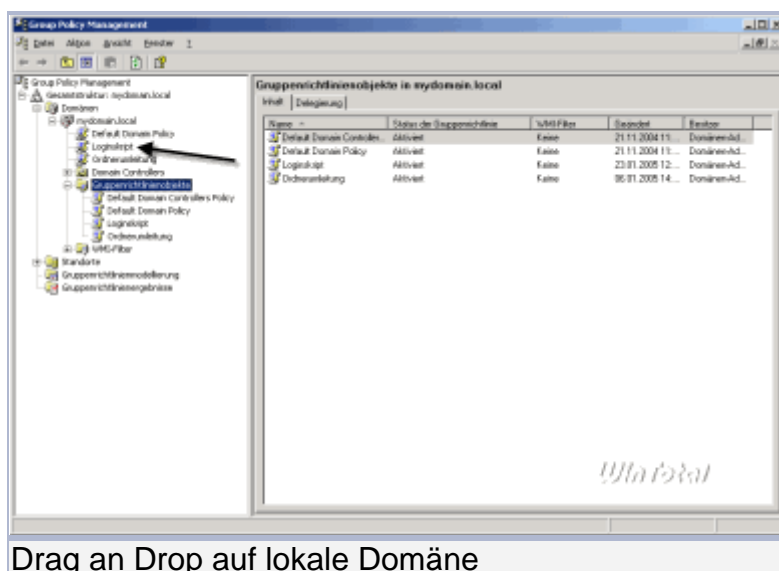
Durch einen Doppelklick auf "Anmelden" öffnet sich der Dialog "Eigenschaften von Anmelden".



Hier klicken wir nun auf "Hinzufügen", dann auf "Durchsuchen" und navigieren in den Ordner NETLOGON (das geht am besten über Netzwerkumgebung => Gesamtes Netzwerk => Microsoft Windows-Netzwerk => MyDomain => Testserver => NETLOGON oder durch direkt Eingabe von \\Testserver\NETLOGON).



Nun bestätigen wir noch alle Dialoge mit OK und voilà, die login.bat ist eingebunden. Wir schließen nun den Gruppenrichtlinien-Editor und verknüpfen das neue GPO via Drag&Drop mit unserer Domain (wie in Teil 4 für das GPO Ordnerumleitung beschrieben).



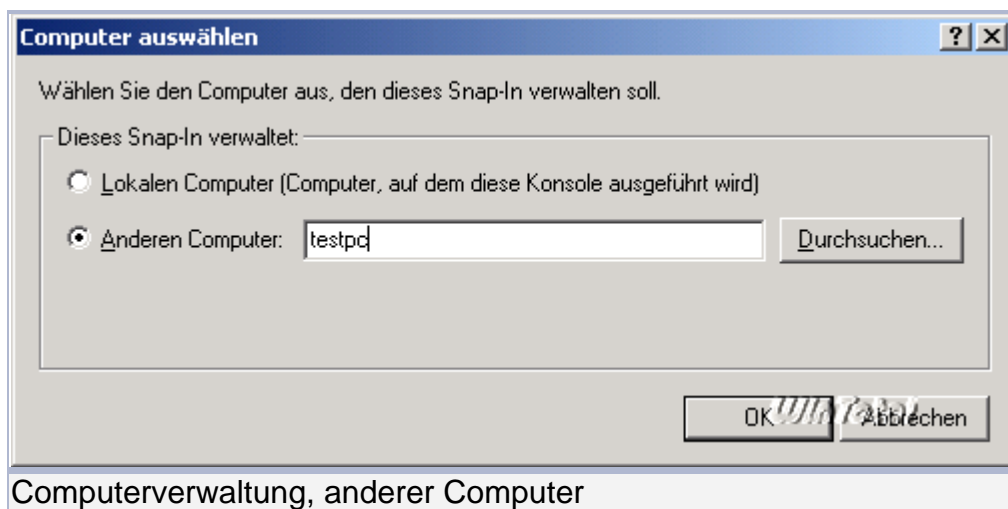
Hinweise:

Verwendet niemals beide Methoden gleichzeitig, das führt zwangsläufig zu Problemen. Ich nutze aufgrund der einfacheren Verteilung an die User mittlerweile nur noch die Variante über die Gruppenrichtlinien. Das Login-Skript ist sehr einfach gehalten, man kann mit Login-Skripts selbstverständlich wesentlich mehr machen. Schaut doch einfach mal in die Skriptsammlung des WinTotal-Softwarearchivs:

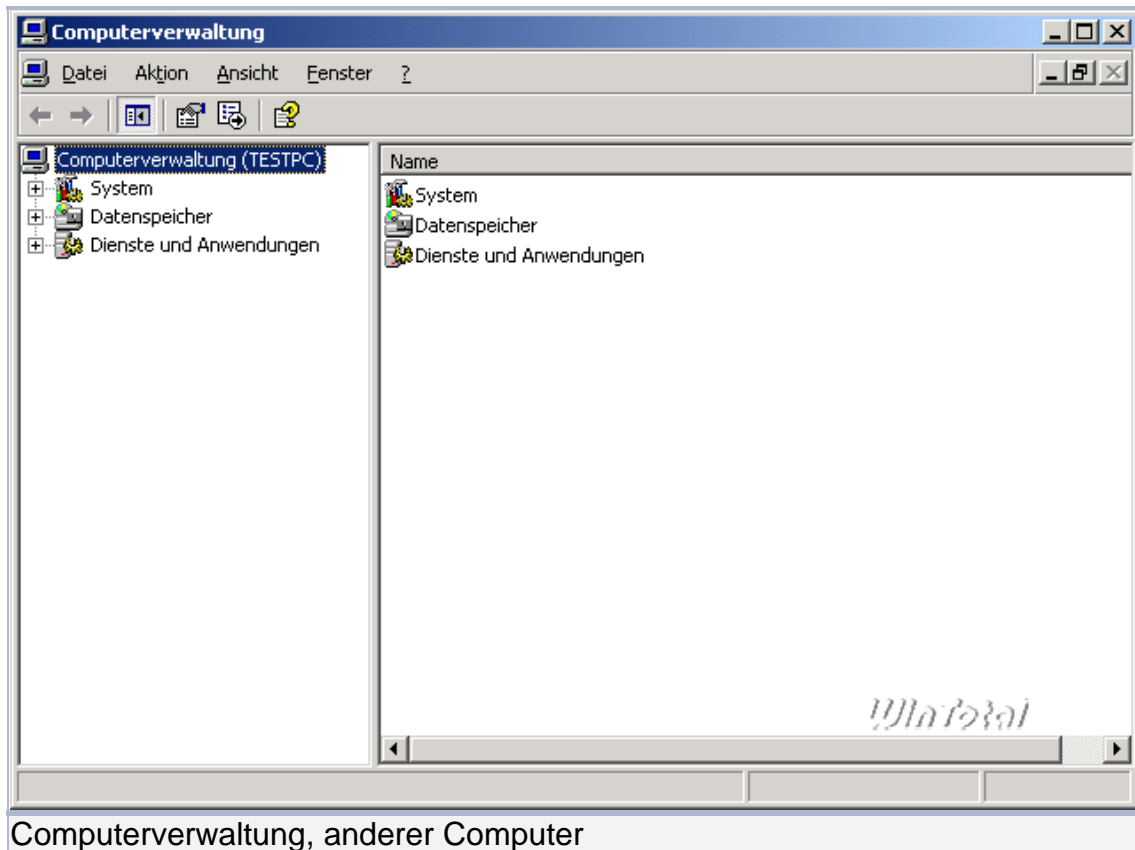
<http://www.WinTotal.de/Software/index.php?rb=1054>

Setzen von lokalen Berechtigungen

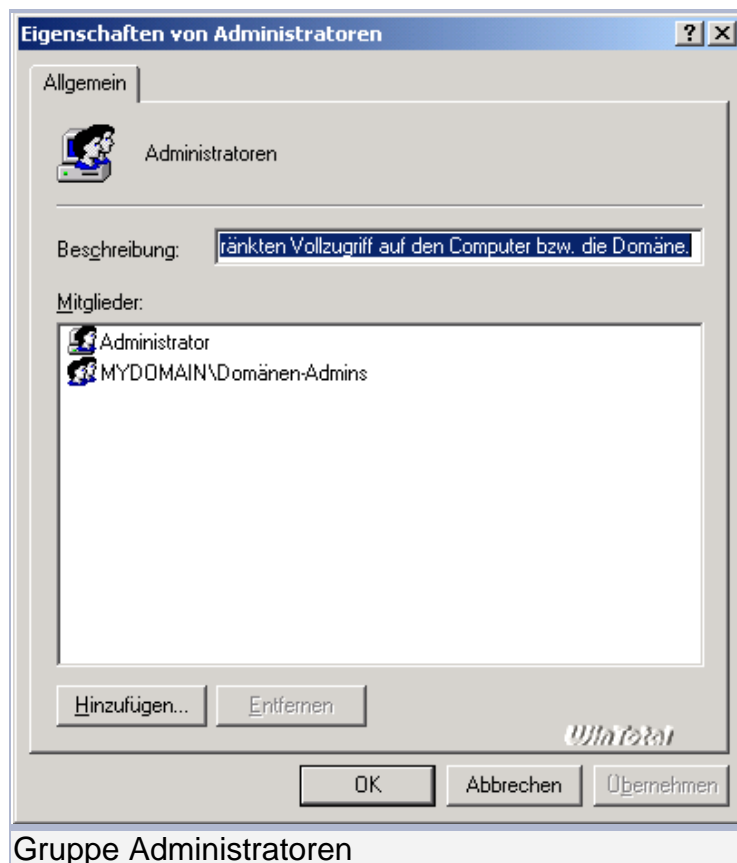
Kommen wir nun zum Setzen von lokalen Berechtigungen: Per default werden Domänen-Benutzer auf den Clients, an denen sie sich anmelden, in der (lokalen) Gruppe Benutzer geführt, d.h. sie dürfen erstmal fast gar nichts, außer mit den vom Administrator bereitgestellten Anwendungen arbeiten. Nun mag es aber Sinn machen, dass z.B. der Administrator selbst an jedem Rechner im Netz lokale Adminrechte haben möchte, OHNE sich dafür als Domänen-Administrator anzumelden - einfach mit seiner "normalen" Benutzeranmeldung. Auch hier gibt es wieder zwei Wege, dies zu erreichen: einen "manuellen" Weg über die Computerverwaltung und einen via Gruppenrichtlinie. Da der Weg via Gruppenrichtlinie nicht mehr ganz trivial ist und eine Fehlkonfiguration bzw. eine nicht vollständige Übernahme der GPOs durch die Clients dazu führen kann, dass dann gar nichts mehr geht, werde ich diesen Weg hier nicht näher erläutern. Für eine Hand voll Rechner ist der Weg über die Computerverwaltung durchaus brauchbar, zumal man damit dann noch mehr machen kann, als nur Berechtigungen zu setzen. Um via Netzwerk die anderen Rechner direkt zu administrieren, müssen diese natürlich eingeschaltet sein; ein Benutzer hingegen muss nicht angemeldet sein. Wir starten auf dem Server die Computerverwaltung (Start => Verwaltung => Computerverwaltung), klicken mit der rechten Maustaste auf den obersten Eintrag "Computerverwaltung (Lokal)" und wählen "Verbindung mit einem anderen Computer herstellen". Hier geben wir nun den Namen des zu administrierenden Rechners ein.



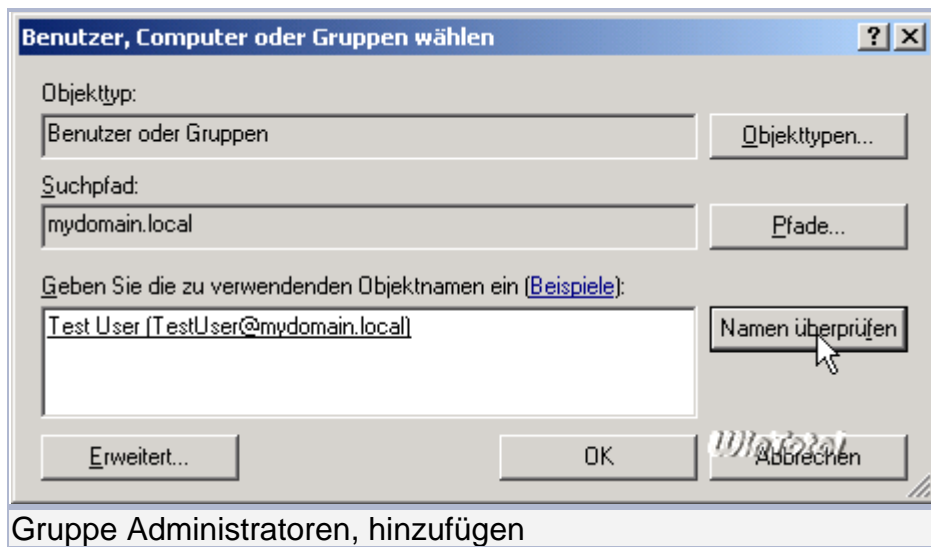
Nach Klick auf OK erscheint nach kurzer Zeit die Computerverwaltungs-Konsole des remoten Rechners.



Hier navigieren wir zu System => Lokale Benutzer und Gruppen => Gruppen und machen einen Doppelklick auf die Gruppe Administratoren.



Nun fügen wir den gewünschten User der lokalen Gruppe Administratoren hinzu.

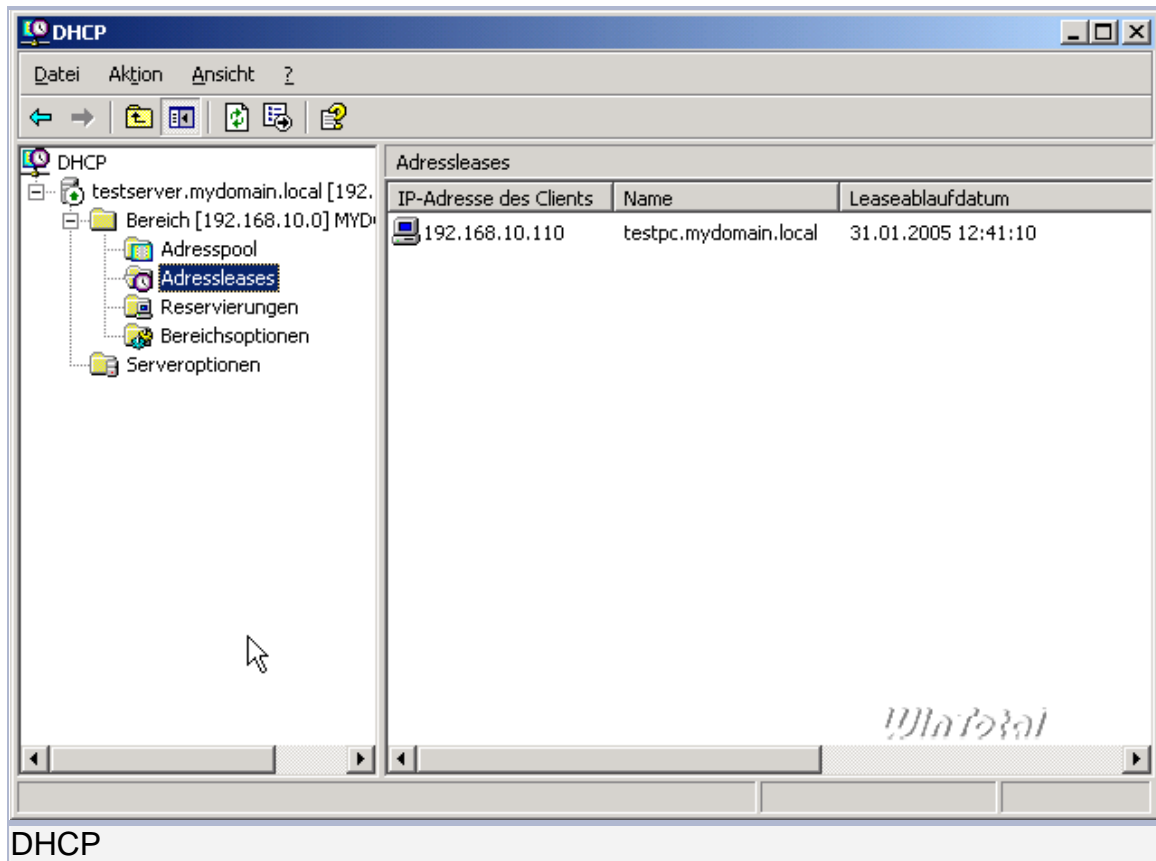


Nach Bestätigung mit OK hat dieser User nun ab dem Zeitpunkt der nächsten Anmeldung an diesem Client Administrator-Rechte auf der Maschine. Bedenkt bitte, dass es nicht immer gleich Admin-Rechte sein müssen, wenn z.B. eine Anwendung unter einem normalen Benutzerkonto nicht funktioniert - hier kann u.U. schon das Hinzufügen des Benutzers zur Gruppe "Hauptbenutzer" Abhilfe schaffen.

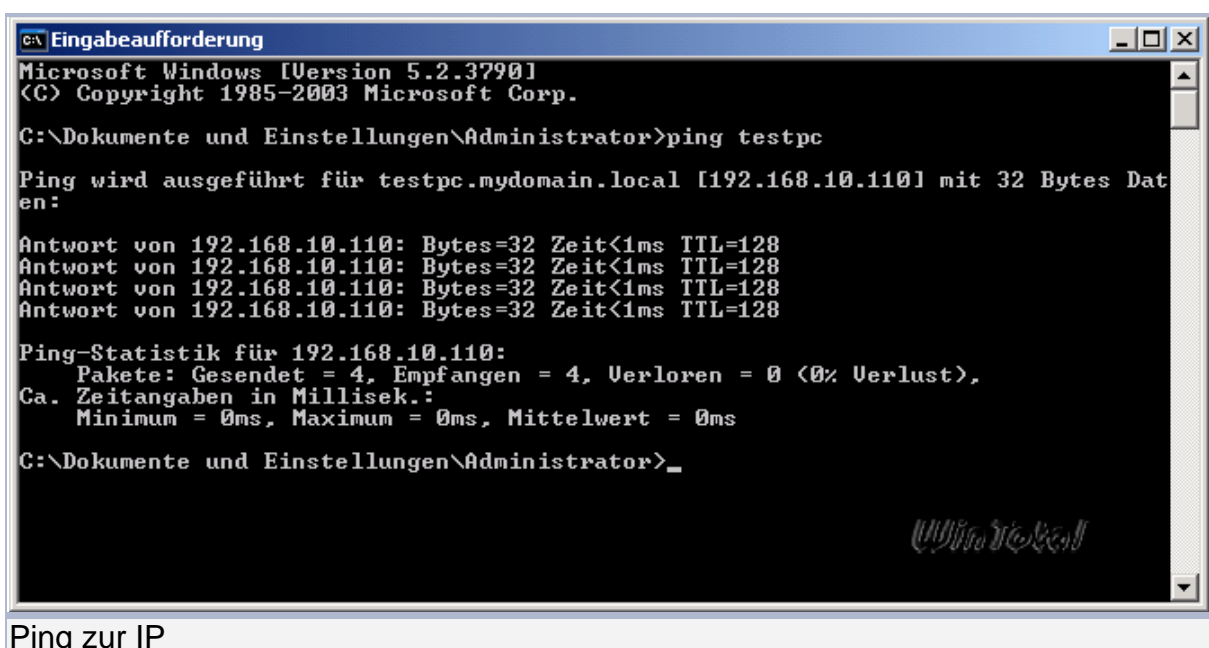
DHCP-Reservierungen für die Clients

Wenden wir uns nun dem letzten Abschnitt dieses Teils zu, den DHCP-Reservierungen. Was ist das eigentlich, eine DHCP-Reservierung, und welchen Sinn macht sie? [Wie in Teil 3 erläutert](#), erhalten die Clients in unserem Netz ihre IP-Adressen automatisch vom Server bzw. von dessen DHCP-Server zugeteilt. Ist eine Lease abgelaufen, fordert der Client eine neue Lease an und erhält somit entweder dieselbe IP-Adresse wieder oder eben eine andere aus dem definierten Bereich. Kurz gesagt: Der Client kann heute unter einer anderen IP-Adresse erreichbar sein, als er das gestern war. Die eigentliche Funktionalität des Netzwerks bleibt davon unberührt, aber wer z.B. auf seinem Router ein Port-Forwarding für bestimmte Dienste eingerichtet hat, dem dürfte genau dieser Umstand der wechselnden IP-Adressen missfallen. Genau hier setzen die DHCP-Reservierungen an: Mit ihrer Hilfe erhält der Client nach wie vor via DHCP seine IP-Adresse, aber immer dieselbe, da der Server den Client anhand der MAC-Adresse seiner Netzwerkkarte erkennt und für ihn die definierte IP-Adresse reserviert, sie also nur diesem einen Client zuweist.

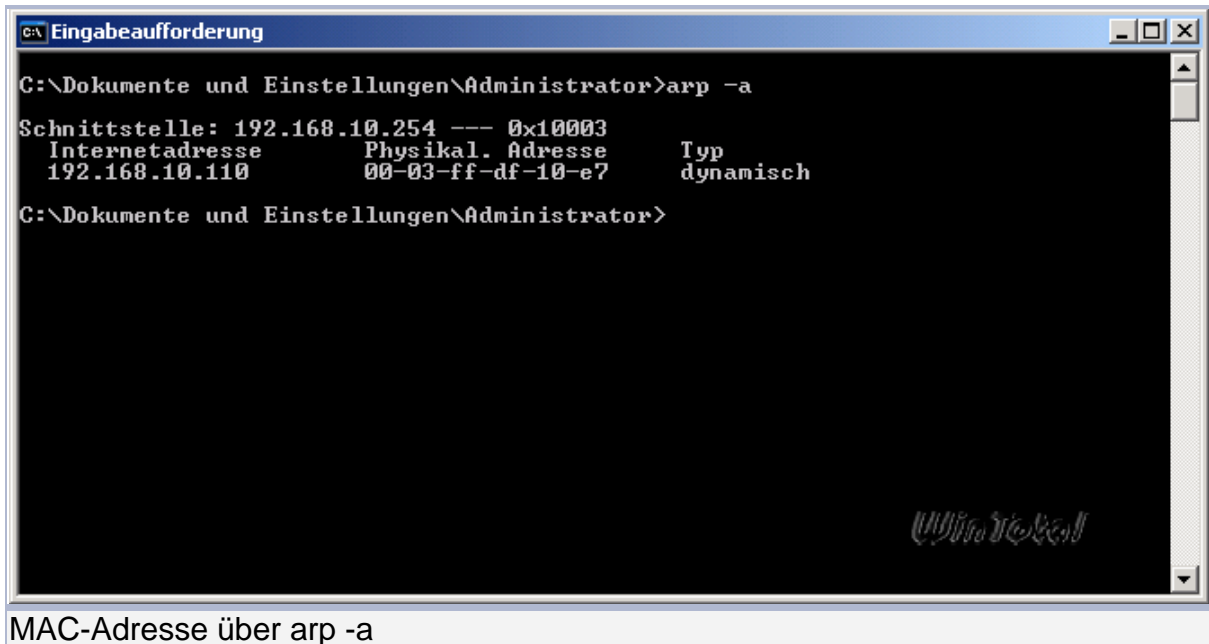
Zum Einrichten der Reservierungen öffnen wir auf dem Server über Start => Verwaltung => DHCP die entsprechende Konsole und navigieren zu "Adressleases".



Hier sehen wir, dass der Rechner "Testpc" die IP-Adresse 192.168.1.110 aus dem von uns definierten Adresspool erhalten hat und damit im Netzwerk erreichbar ist. Wir möchten diesem Rechner nun aber die IP-Adresse 192.168.1.80 zuordnen und müssen dafür eine Reservierung erstellen. Die IP-Adressen, die für die Reservierungen verwendet werden, dürfen NICHT aus dem Adresspool stammen! Das Ermitteln der MAC-Adresse dieses Rechners ist recht einfach, wir öffnen auf dem Server eine Kommandozeile und pingen den Rechner an.



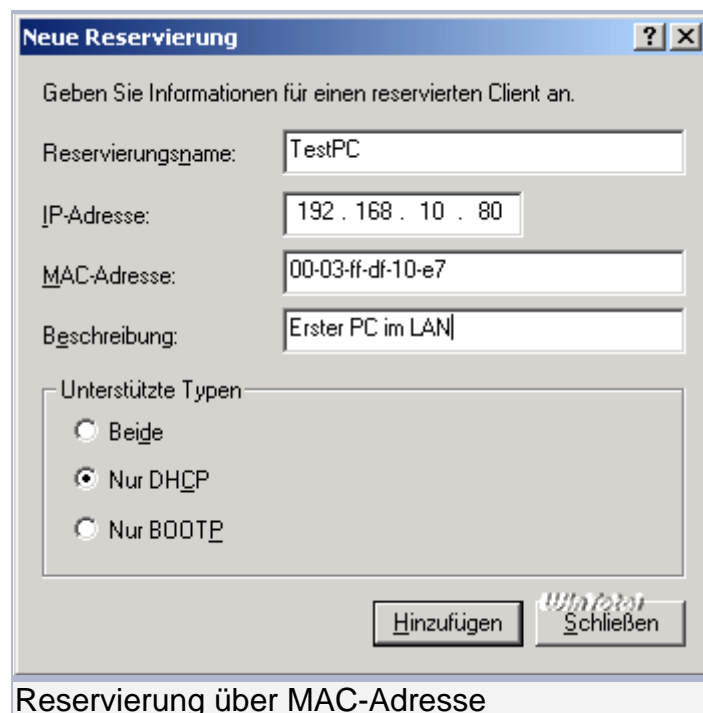
Nach dem Pingen führen wir in derselben Kommandozeile ein `arp -a` durch; der etwas kryptisch aussehende Teil unterhalb "Physikal. Adresse" ist die MAC-Adresse.



MAC-Adresse über `arp -a`

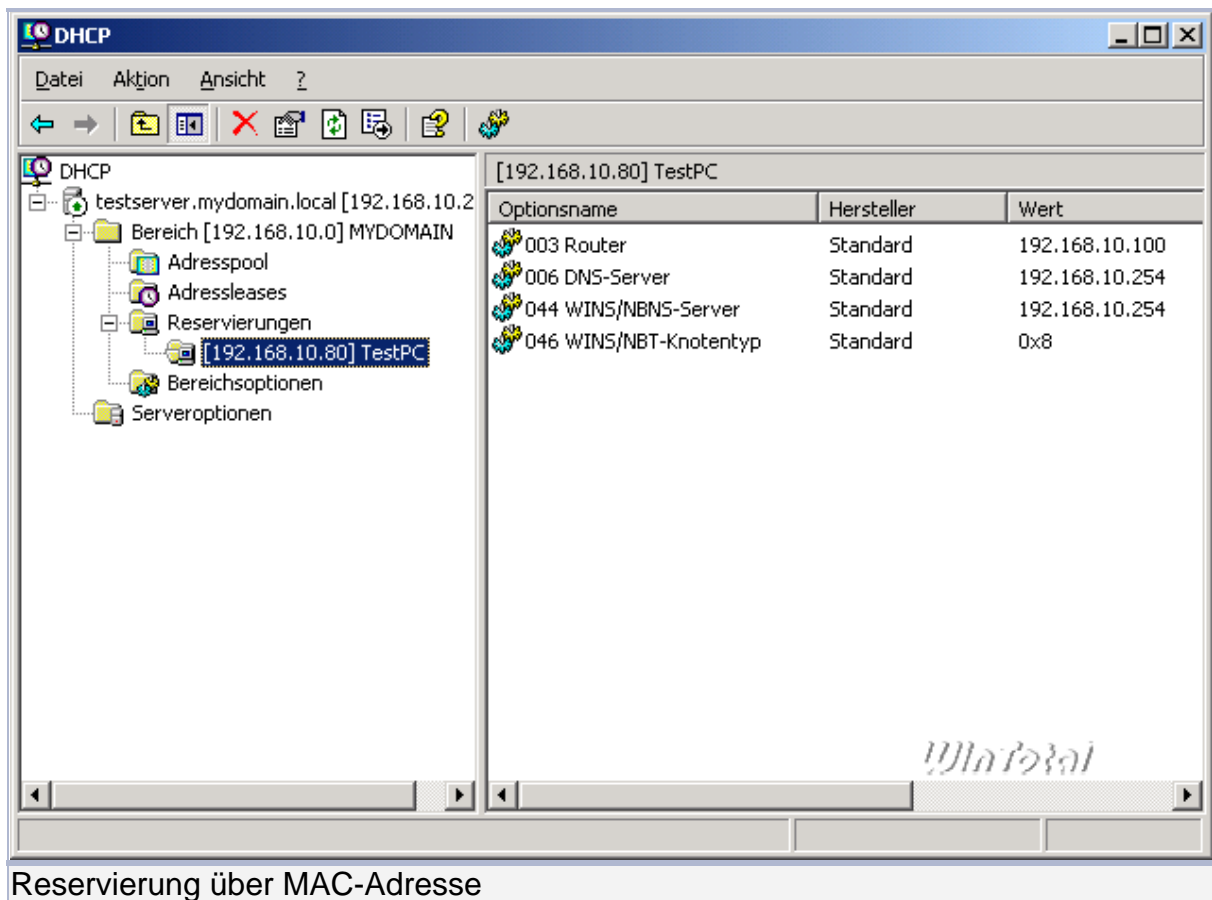
Diese MAC-Adresse kopieren wir uns in die Zwischenablage (bei gedrückter linker Maustaste markieren und dann Enter drücken) und wechseln in die DHCP-Konsole. Hier führen wir einen Rechtsklick auf "Reservierungen" aus und wählen "Neue Reservierung" aus.

Den Dialog "Neue Reservierung" füttern wir mit den benötigten Daten, die MAC-Adresse fügen wir mittels STRG+V in das Feld MAC-Adresse ein und wählen bei "Unterstützte Typen" hier "Nur DHCP" aus.

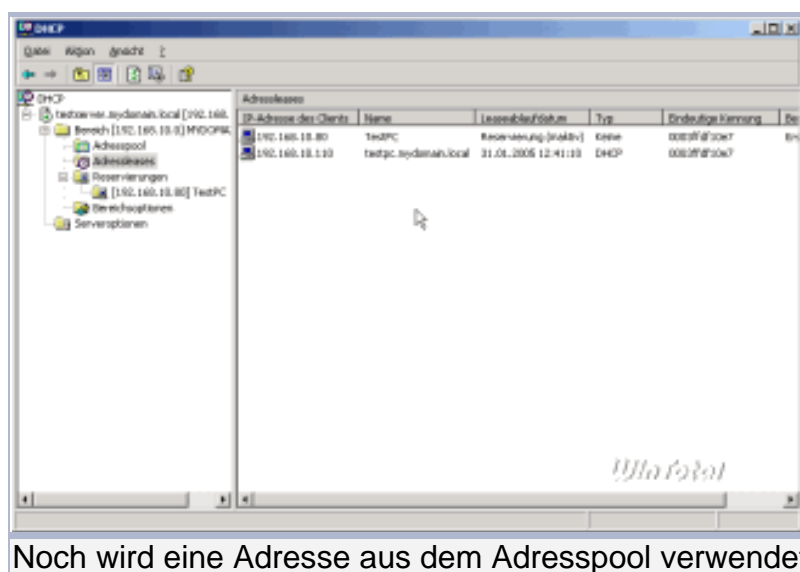


Reservierung über MAC-Adresse

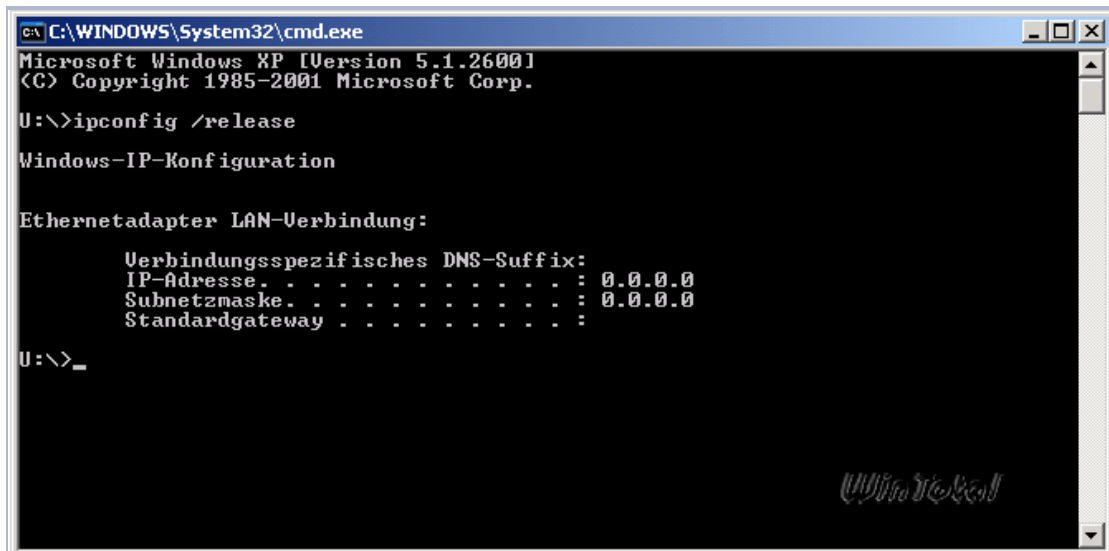
Nach Klicken von OK sollte das in etwa so aussehen:



Damit bekommt unser Client "TestPC" von nun an immer die IP-Adresse 192.168.1.80 zugeordnet und ist somit auch immer unter diese IP-Adresse erreichbar. Noch allerdings verwendet der Client die aus dem Adresspool zugewiesene IP-Adresse.



Das ändert sich spätestens nach einem Reboot, kann aber auf dem Client auch durch `ipconfig /release` bzw. `/renew` an der Konsole erreicht werden.



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

U:\>ipconfig /release

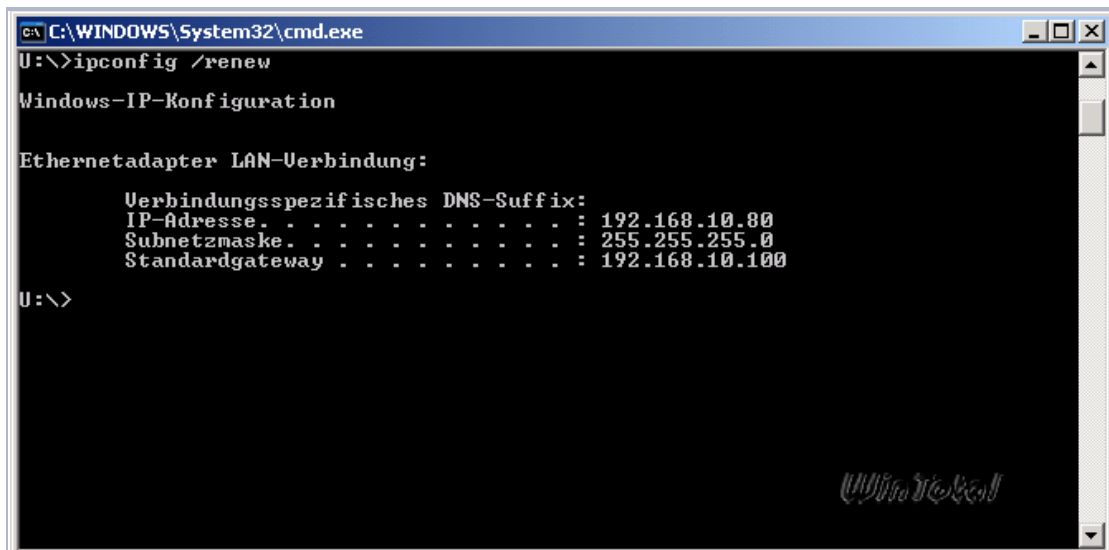
Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 0.0.0.0
    Subnetzmaske. . . . . : 0.0.0.0
    Standardgateway . . . . . :

U:\>
```

Lösen der IP



```
C:\WINDOWS\System32\cmd.exe
U:\>ipconfig /renew

Windows-IP-Konfiguration

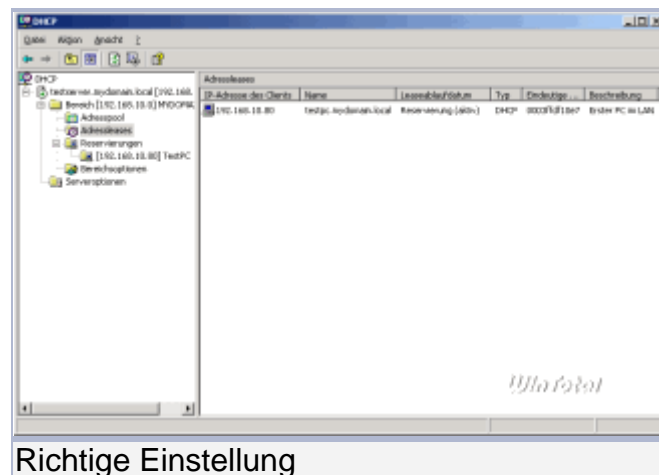
Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.10.80
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.10.100

U:\>
```

Neue IP

In der DHCP-Konsole stellt sich das dann so dar.



Richtige Einstellung

Dieses Vorgehen müsst ihr für jeden Client im Netz, der via DHCP immer dieselbe IP-Adresse erhalten soll, wiederholen. Um die MAC-Adressen mehrerer Rechner auf einmal herauszufinden, könnt ihr auch das kleine [Skript GetMac](#) verwenden:

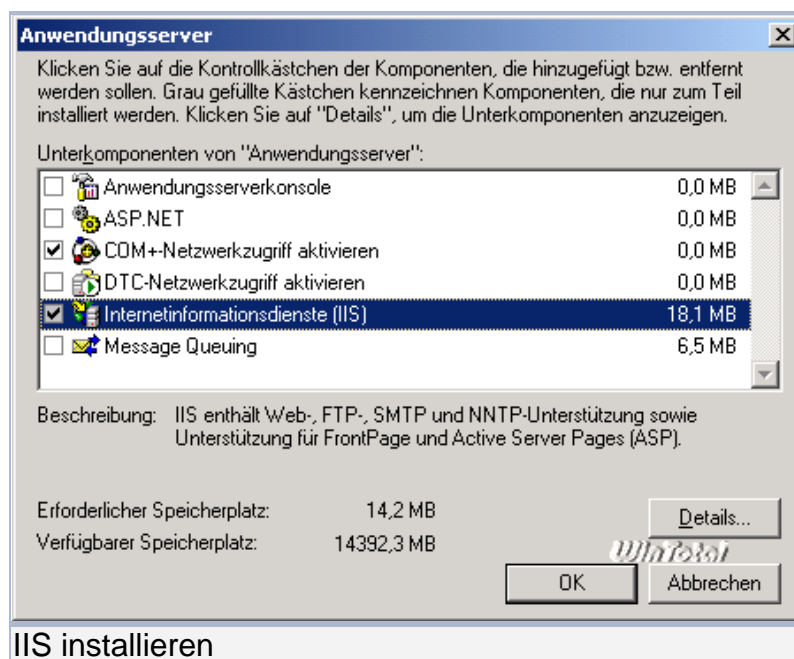
Teil 6 wird sich ausschließlich mit dem Thema Software Update Services (SUS) beschäftigen, also einer Möglichkeit, alle Rechner im Netz (ab Win2000 aufwärts) automatisch mit den wichtigsten Updates zu versorgen, wobei der Download aus dem Internet nur einmal auf dem Server erfolgt und die Clients sich die Updates dann lokal vom Server ziehen.

Teil 6

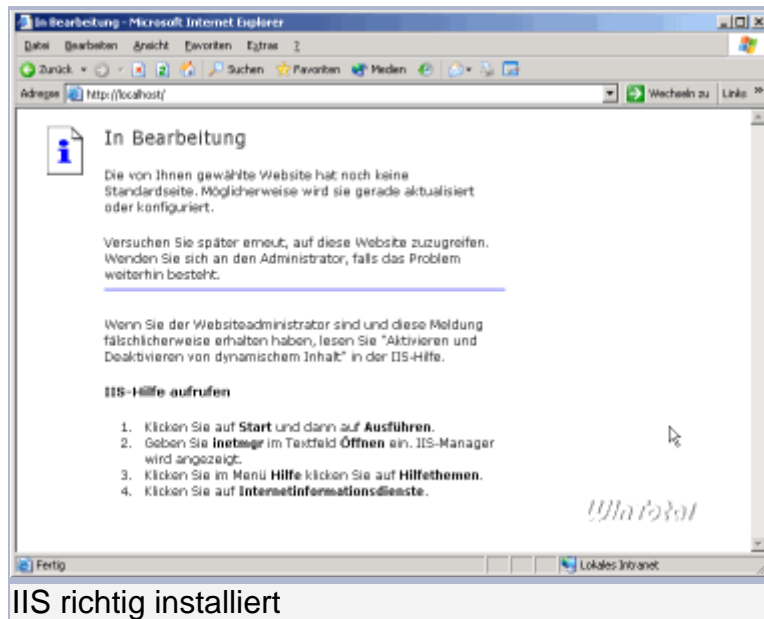
Installation und Konfiguration der Software Update Services (SUS)

Im Rahmen des Patchmanagements hat Microsoft die Software Update Services entwickelt, die kostenlos aus dem Internet heruntergeladen werden können. Sinn und Zweck von SUS ist es, einen lokalen Update-Server zu betreiben, der zentral die von Microsoft bereitgestellten Updates aus dem Internet lädt und an die im LAN vorhandenen Clients verteilt. Als Administrator bekommt man so die volle Kontrolle darüber, wann welche Clients welche Updates installieren (sollen), denn die Verteilung erfolgt via Gruppenrichtlinien. Aber der Reihe nach: Am Anfang steht immer erst der Download (<http://www.wintotal.de/Artikel/w2003server6/w2003server6.php>). Die SUS-Software kann man bei Microsoft downloaden, die aktuelle Version ist SUSP1: <http://www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en> Die Abarbeitung der im Artikel beschriebenen Vorgehensweise richtet sich eigentlich ausschließlich an DSL-Nutzer mit einer Flatrate - die 33MB Installation für den SUS-Server an sich wären auch mit ISDN noch vertretbar, die > 2GB an Patches, die der SUS-Server dann herunterlädt, allerdings nicht mehr. Voraussetzung für die Installation ist (lt. offiziellen Microsoft-Angaben) ein Windows 2000 bzw. Windows 2003 Server mit installiertem IIS (Internet Information Server). Mit ein paar Tricks lässt sich der SUS-Server aber z.B. auch auf einem Notebook unter XP installieren und betreiben, so dass man alle aktuellen Patches immer dabei hat und z.B. bei Freunden im Netz mal schnell für Ordnung sorgen kann. Dazu wird ein eigener Artikel erscheinen, da es den Rahmen dieses Artikels sprengen würde. Zurück zum Thema:

Nach dem Download folgt die Installation - da der IIS Grundvoraussetzung für den SUS-Server ist, müssen wir zuerst diesen nachinstallieren. Also Windows 2003 Server-CD einlegen und über Start => Systemsteuerung => Software => Komponenten hinzufügen/entfernen => Anwendungsserver => Details den IIS installieren.



Nach der Installation des IIS kontrollieren wir, ob er korrekt ausgeführt wird. Dazu einfach den Browser öffnen und `http://localhost` in der Adresszeile eingeben. Das sollte dann so aussehen:



Nun können wir mit der Installation des SUS-Servers beginnen, dazu einfach die Datei `SUS10SP1.exe` doppelklicken, dadurch wird das Paket extrahiert und die Installation gestartet.



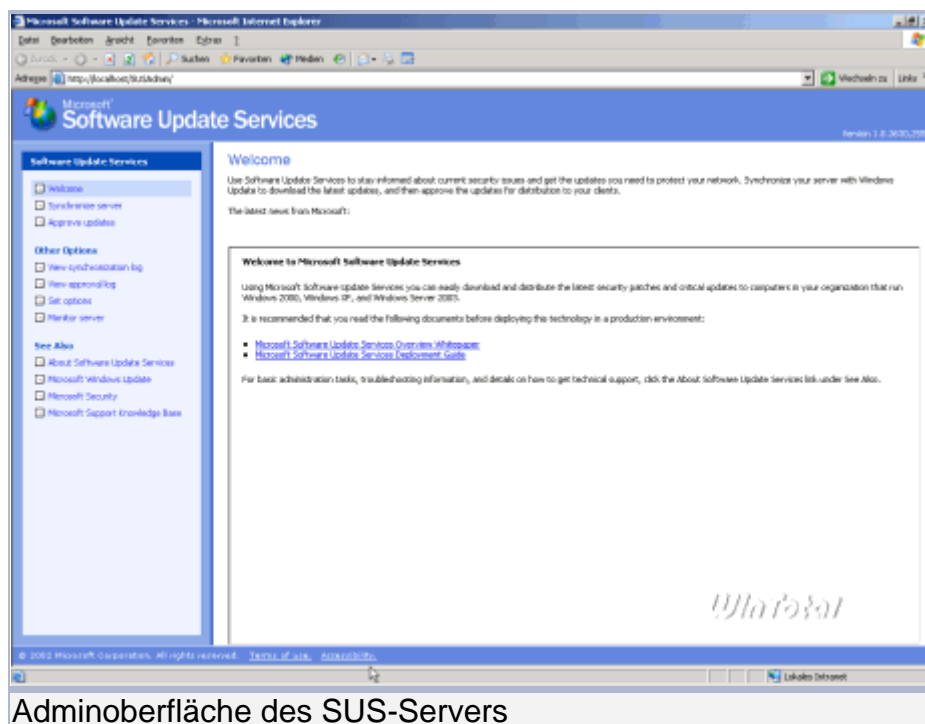
Im Installations-Dialog bitte "Typical" auswählen und auf NEXT klicken, der Rest geht dann von alleine, der SUS-Server wird auf Laufwerk C: im Verzeichnis `\SUS` installiert und speichert auch dort die Updates, die Administrations-Oberfläche unter `/wwwroot`.

Wenn ihr hier andere Werte eintragen wollt, könnt ihr dies durch Auswahl von

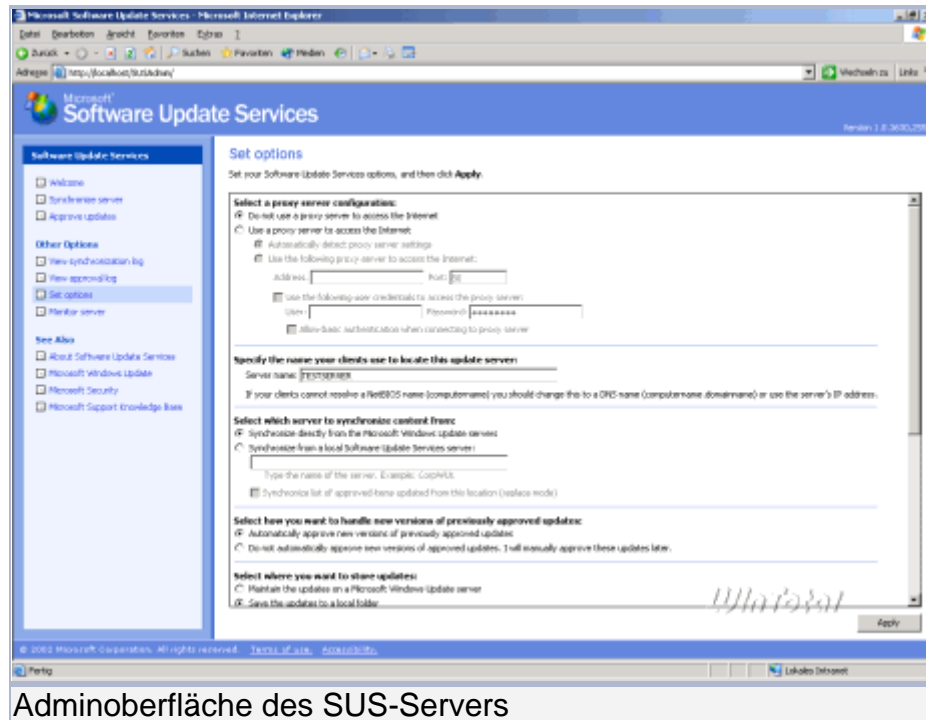
"Custom" während der Installation tun. Dies empfiehlt sich z.B. dann, wenn ihr Laufwerk C: nur als Systempartition gedacht habt und eure Datenbestände z.B. auf Laufwerk D: liegen. Der Abschluss der Installation wird durch diesen Dialog angezeigt, hier seht ihr auch gleich, unter welchem Namen euer Update-Server später erreichbar sein wird.



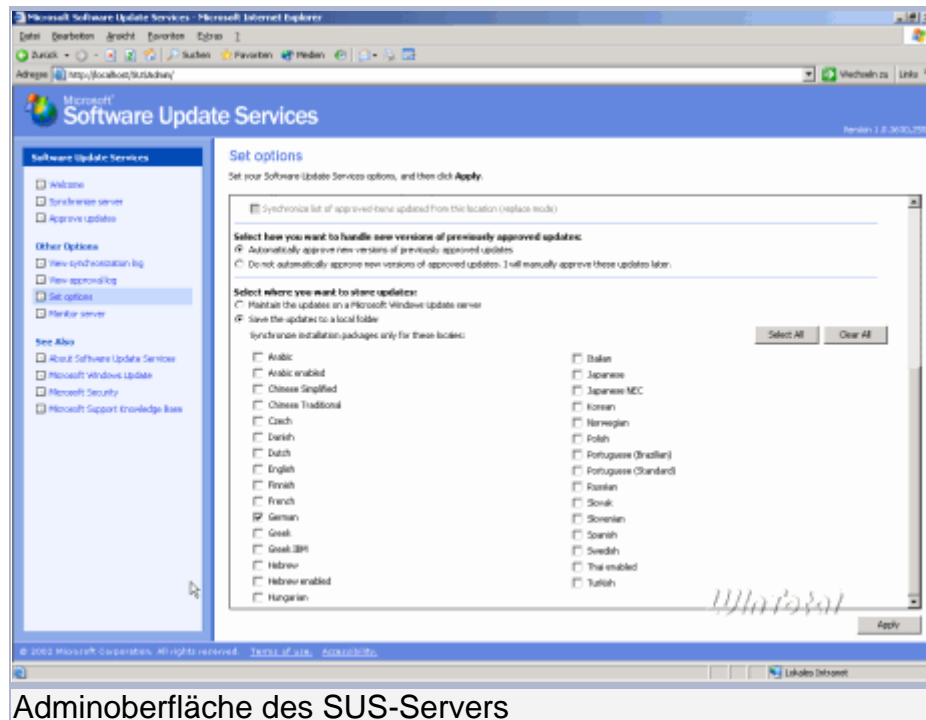
Nach dem Klick auf „Finish“ startet automatisch die Administrationsoberfläche des SUS-Servers:



Klickt nun auf "Set Options", um den Server für euer Netz zu konfigurieren. Der Dialog ist recht lang, daher zwei Bilder, wie es aussehen könnte/sollte:



Adminoberfläche des SUS-Servers

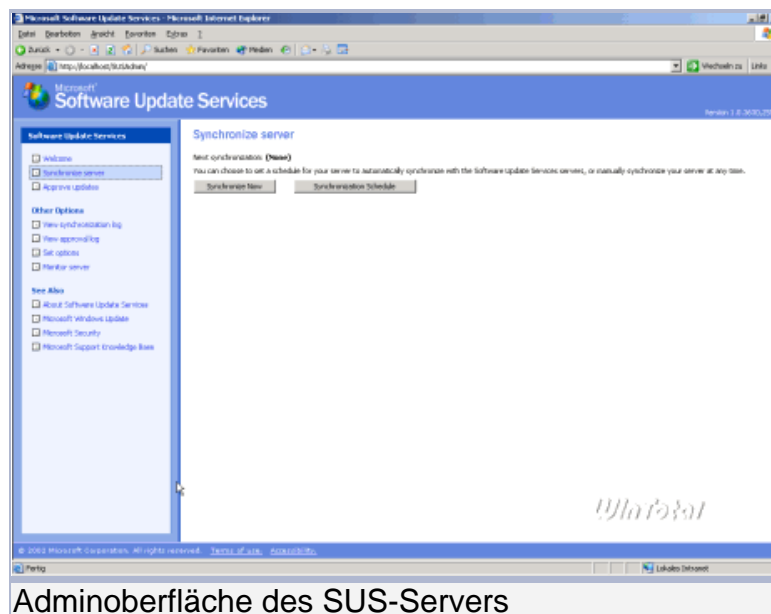


Adminoberfläche des SUS-Servers

Die Einstellungen im Einzelnen:

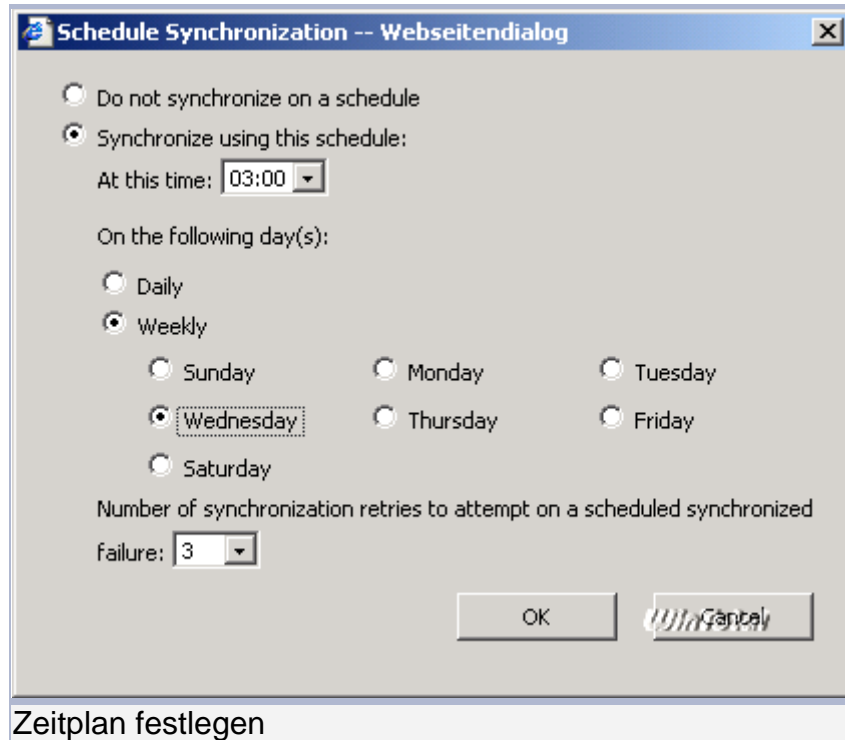
- Select a proxy server configuration:
Falls ihr für den Internetzugang einen Proxy-Server verwendet, tragt ihn bitte hier ein (ggf. mit Authentifizierung).
- Specify the Name your clients use to locate this update server:
Hier gebt ihr den Namen an, unter dem die Clients im Netz den Server später finden werden. Prinzipiell braucht ihr hier nichts zu ändern, der NetBIOS-Name des Servers steht hier ja schon drin.
- Select which server to synchronize content from:
Hier wird eingestellt, ob die Updates direkt von den Microsoft-Servern oder von einem anderen, im LAN schon vorhandenen SUS-Server gezogen werden sollen. Hier stellt ihr "directly from Microsoft" ein - in unserem LAN gibt's ja keinen weiteren SUS-Server.
- Select how you want to handle new versions of previously approved Updates:
Microsoft stellt korrigierte Versionen von bereits veröffentlichten Patches zum Download zur Verfügung - hier könnt ihr nun einstellen, ob diese Versionen automatisch installiert werden sollen oder ob ihr diese manuell freigeben wollt. Die automatische Freigabe ("automatically approve") ist empfohlen.
- Select where you want to store Updates:
Hier lässt sich einstellen, ob der SUS-Server die Updates einmal selbst herunterlädt und local speichert oder die Zugriffe der Clients direkt auf die MS-Server laufen sollen. Letzteres würde unnötigen Datenverkehr erzeugen, da dann doch wieder jeder Client direkt von Microsoft herunterlädt, wir wählen also "Save Updates to a local folder".

Weiterhin lassen sich hier die Sprachversionen der herunterzuladenden Updates festlegen - da ich von deutschen Systemen ausgehe, genügt hier der Haken bei "German" (wobei z.B. das .NET-Framework ungeachtet dieser Einstellung in allen Sprachen heruntergeladen wird). Zum Abschluss der Konfiguration klicken wir unten rechts auf "Apply" um die getätigten Einstellungen abzuspeichern. Nachdem der Server nun konfiguriert ist, können wir mit dem ersten Download beginnen. Wie eingangs schon erwähnt, sind das aktuell > 2GB, könnte also eine Weile dauern. Dazu klicken wir auf "Synchronize Server":



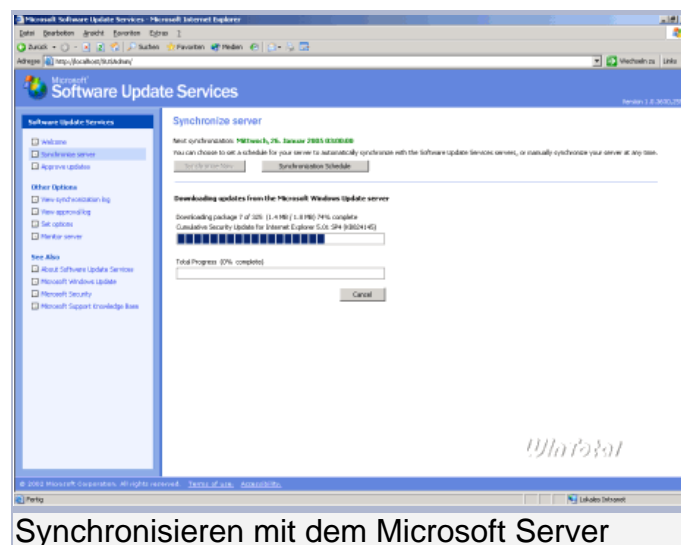
Adminoberfläche des SUS-Servers

"Synchronize Now" startet einen sofortigen Synchronisierungsvorgang mit Microsoft, "Synchronization Schedule" erlaubt das Planen der Synchronisierung. Wir stellen nun erstmal einen Plan auf, wann unser SUS-Server Updates aus dem Netz laden soll. Da Microsoft einmal im Monat, nämlich immer am zweiten Dienstag eines Monats, "Patchday" hat, wählen wir "Weekly" und "Wednesday".



Zeitplan festlegen

Da unser Server ja rund um die Uhr läuft und wir uns mit dem Download von Updates nicht die Internet-Leitung zuballern wollen, ist 03.00 Uhr nachts eine gute Uhrzeit für diese Downloads. Die Einstellung von drei Neu-Versuchen bei Synchronisations-Fehlern sollte ebenfalls so bleiben. Zum sofortigen Synchronisieren des Servers klicken wir nun auf "Synchronize Now" und warten, bis der Server alle Updates heruntergeladen hat.

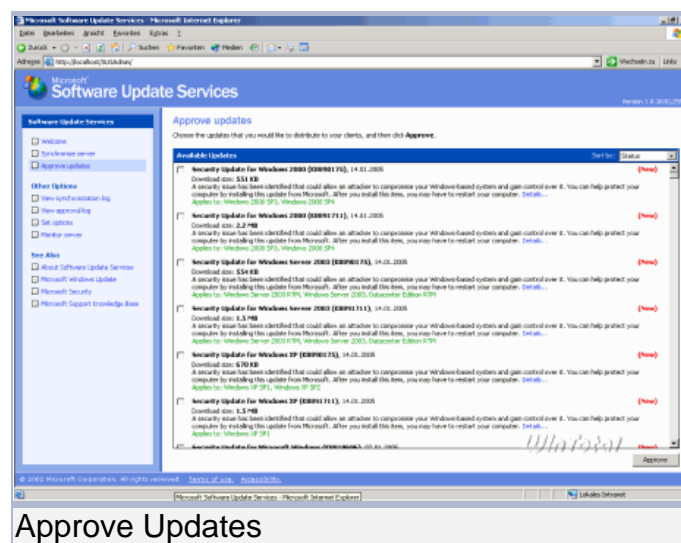


Synchronisieren mit dem Microsoft Server

Nachdem alle Updates heruntergeladen wurden, gibt der SUS-Server eine entsprechende Meldung aus:



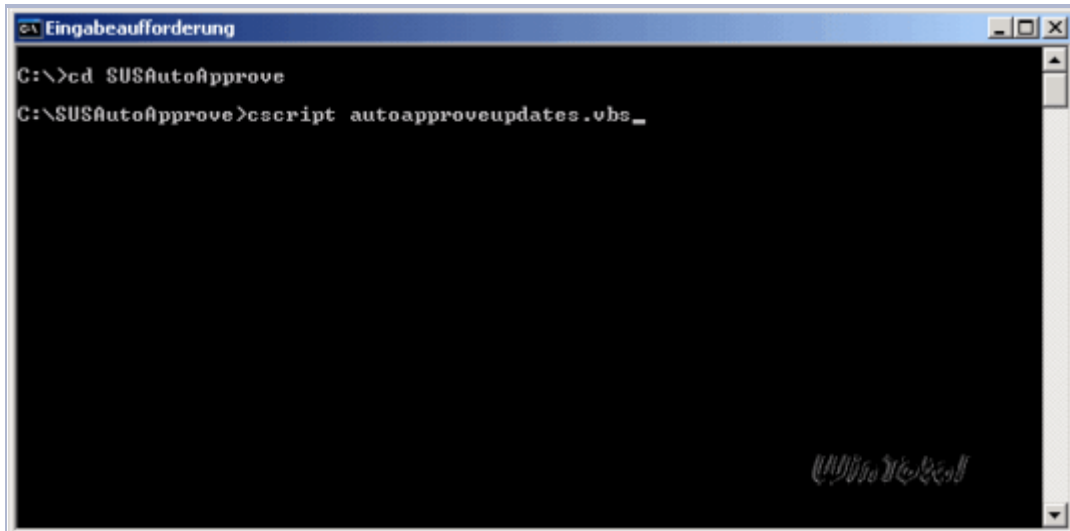
Nach einem Klick auf OK gelangen wir auf die "Approve Updates"-Seite; hier können wir nun entscheiden, welche Updates für die Installation freigegeben (approved) werden.



In unserem Fall sollten wir erstmal alle vorhandenen Updates markieren, angesichts der Masse an Updates, die nach dem ersten Synchronisieren zur Verfügung steht, wäre es müßig, alle Updates einzeln anzuklicken, wir behelfen uns also daher mit einem kleinen Tool: Autoapproveupdates.vbs - Download:

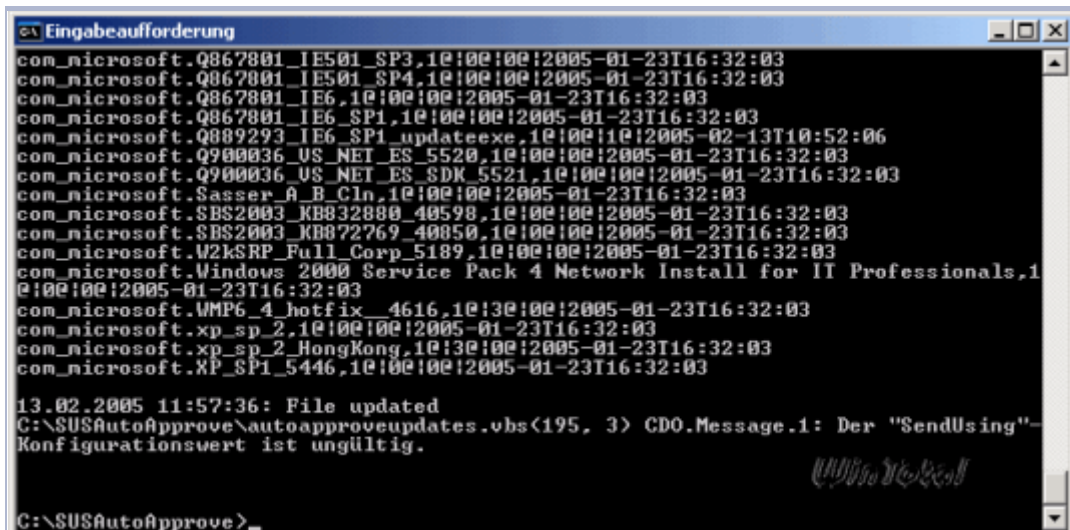
<http://www.WinTotal.de/softw/?id=2627>

Die Konfiguration des Skripts ist selbsterklärend, der Aufruf des Skripts erfolgt über die Kommandozeile (ich habe das Skript im Verzeichnis C:\SUSAutoApprove abgelegt):



```
Eingabeaufforderung
C:\>cd SUSAutoApprove
C:\SUSAutoApprove>cscript autoapproveupdates.vbs_
```

Approve über ein Script



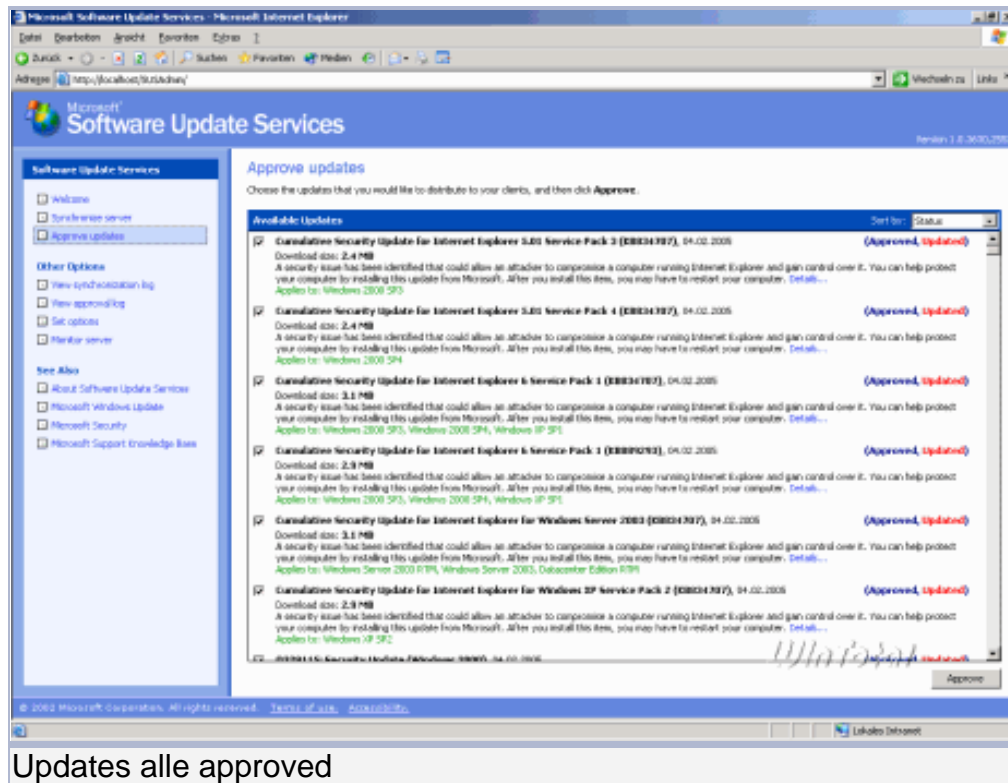
```
Eingabeaufforderung
com_microsoft.Q867801_IE501_SP3,10:00:00:2005-01-23T16:32:03
com_microsoft.Q867801_IE501_SP4,10:00:00:2005-01-23T16:32:03
com_microsoft.Q867801_IE6,10:00:00:2005-01-23T16:32:03
com_microsoft.Q867801_IE6_SP1,10:00:00:2005-01-23T16:32:03
com_microsoft.Q889293_IE6_SP1_update.exe,10:00:00:2005-02-13T10:52:06
com_microsoft.Q900036_VS.NET_ES_5520,10:00:00:2005-01-23T16:32:03
com_microsoft.Q900036_VS.NET_ES_SDK_5521,10:00:00:2005-01-23T16:32:03
com_microsoft.Sasser_A_B_Cln,10:00:00:2005-01-23T16:32:03
com_microsoft.SBS2003_KB832880_40598,10:00:00:2005-01-23T16:32:03
com_microsoft.SBS2003_KB872769_40050,10:00:00:2005-01-23T16:32:03
com_microsoft.W2kSRP_Full_Corp_5189,10:00:00:2005-01-23T16:32:03
com_microsoft.Windows_2000_Service_Pack_4_Network_Install_for_IT_Professionals,10:00:00:2005-01-23T16:32:03
com_microsoft.WMP6_4_hotfix_4616,10:30:00:2005-01-23T16:32:03
com_microsoft.xp_sp_2,10:00:00:2005-01-23T16:32:03
com_microsoft.xp_sp_2_HongKong,10:30:00:2005-01-23T16:32:03
com_microsoft.XP_SP1_5446,10:00:00:2005-01-23T16:32:03

13.02.2005 11:57:36: File updated
C:\SUSAutoApprove\autoapproveupdates.vbs(195, 3) CD0.Message.1: Der "SendUsing"-Konfigurationswert ist ungültig.

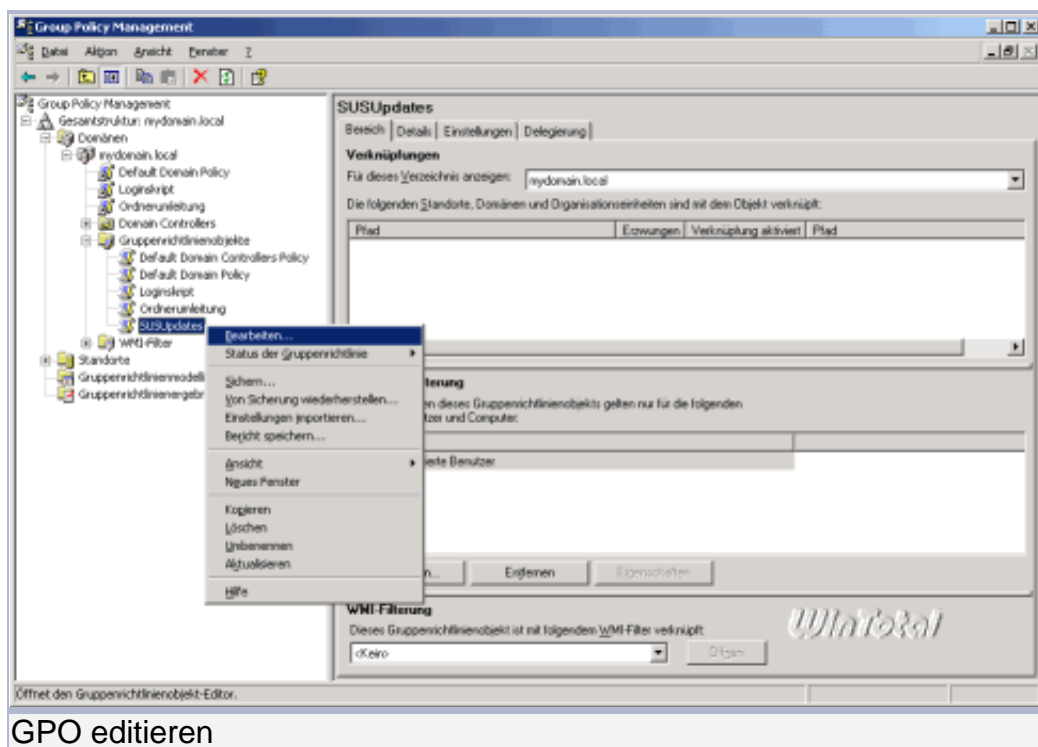
C:\SUSAutoApprove>
```

Approve über ein Script

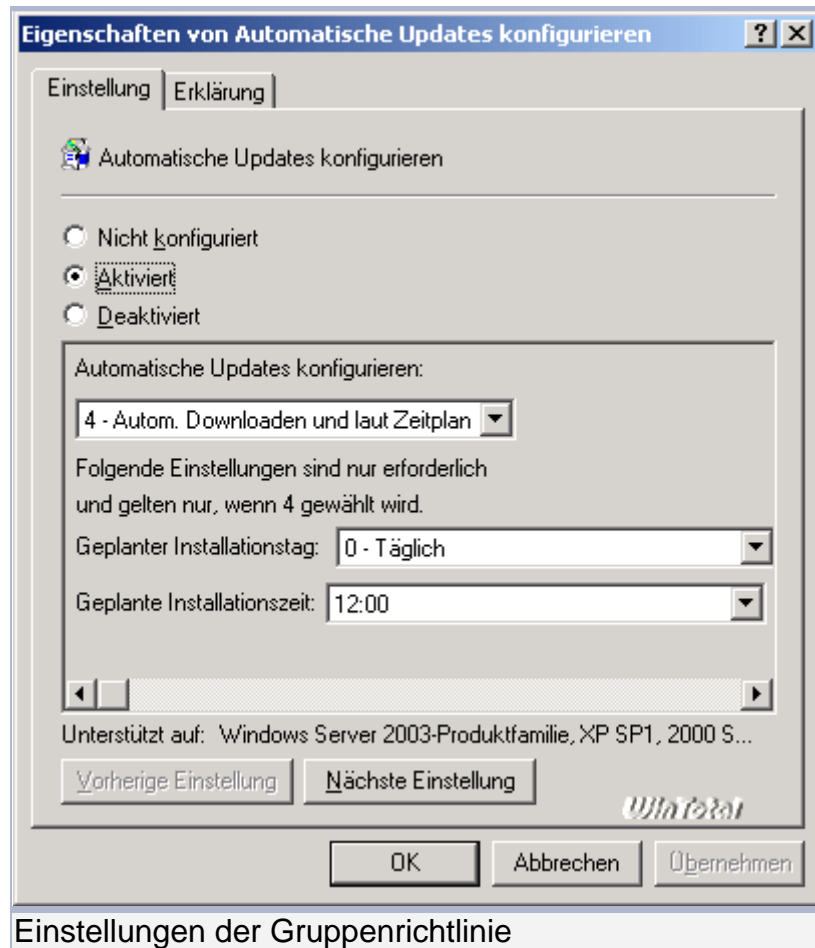
Nach dem Ausführen des Skripts sieht die "Approve Updates"-Seite unseres SUS-Servers dann in etwa so aus:



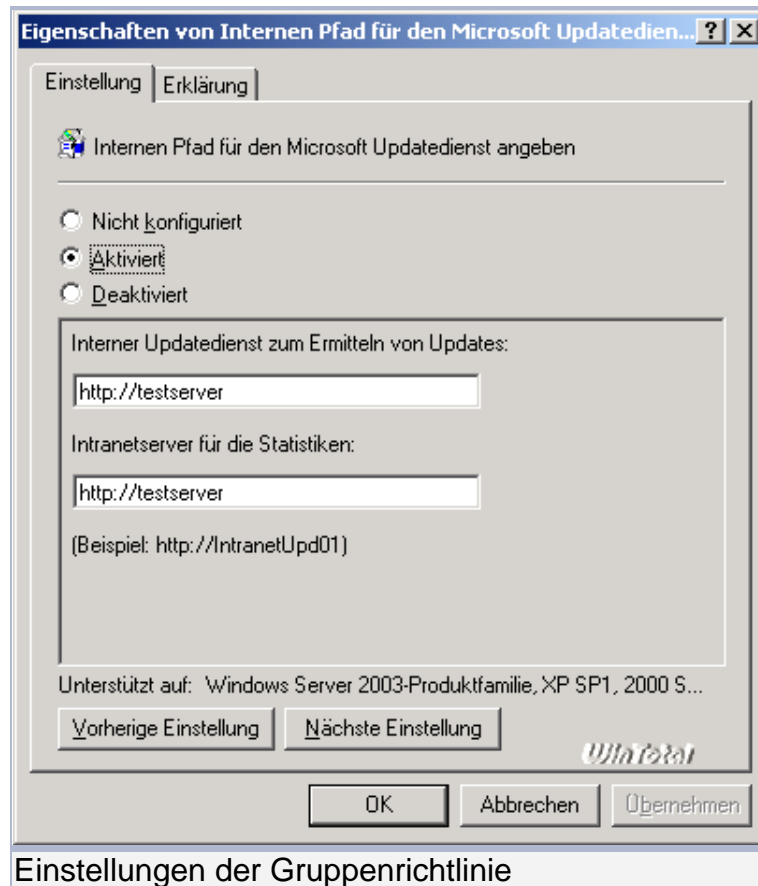
Alle Updates sind somit freigegeben, nun kümmern wir uns darum, dass die Clients im Netz diese Updates auch von unserem SUS-Server herunterladen. Dazu nutzen wir die Gruppenrichtlinien-Funktionalität, die uns in Form der Vorlage wuau.adm zur Verfügung steht. Dazu öffnen wir die GPMC und erstellen uns ein neues GPO mit dem Namen SUSUpdates, welches wir mittels Rechtsklick => Bearbeiten in den GPO-Editor laden.



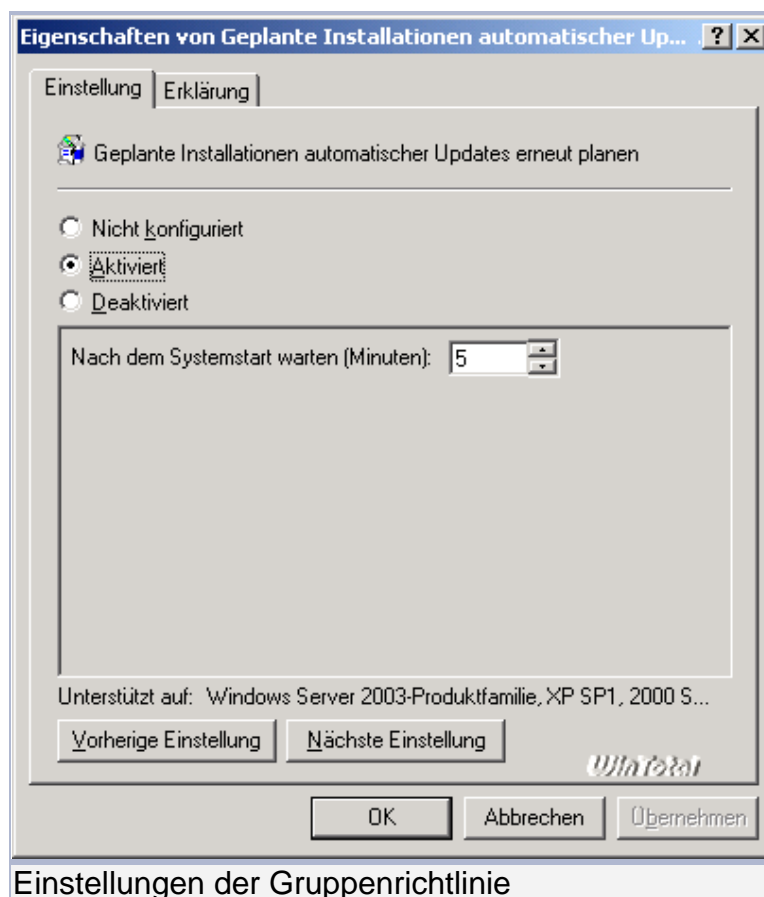
Wir navigieren nun im linken Baum zu Computerkonfiguration => Administrative Vorlagen => Windows Komponenten => Windows Update und doppelklicken den obersten Eintrag "Automatische Updates konfigurieren". Die Konfigurationsmöglichkeiten sind im Reiter "Erklärung" erläutert, daher spare ich mir das an dieser Stelle. Meine bevorzugte Einstellung ist auf dem Screenshot zu sehen:



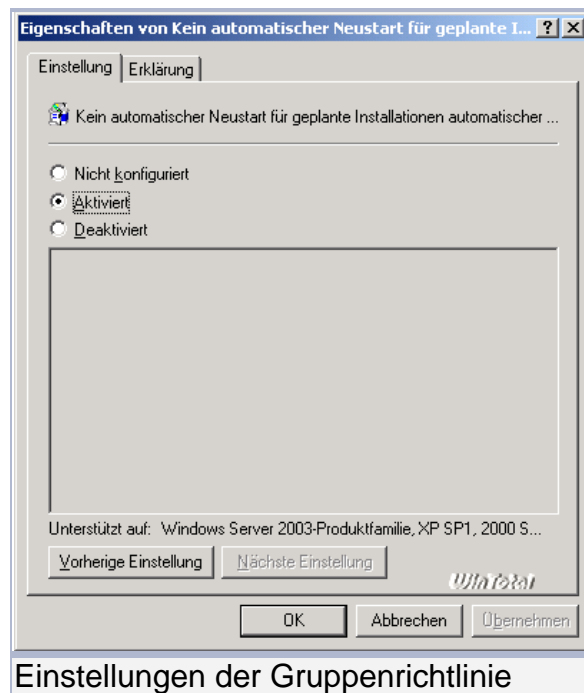
Nach Klick auf "Übernehmen" und "Nächste Einstellung" gelangen wir zum nächsten Konfigurationspunkt, hier wird der Name des zu verwendenden SUS-Servers festgelegt. Beachtet bitte, das SUS entweder mit dem NetBIOS-Namen oder mit der IP-Adresse funktioniert, nicht aber mit einem FQDN.



Der nächste Konfigurations-Dialog sieht dann so aus:

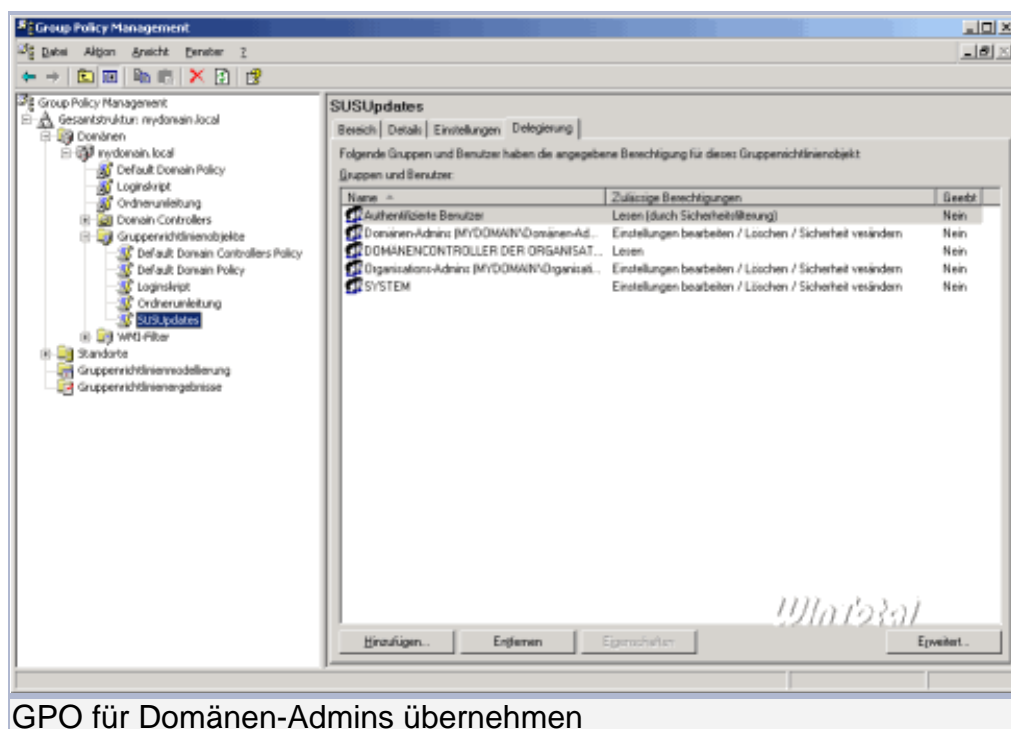


Und der vierte und letzte dann so:

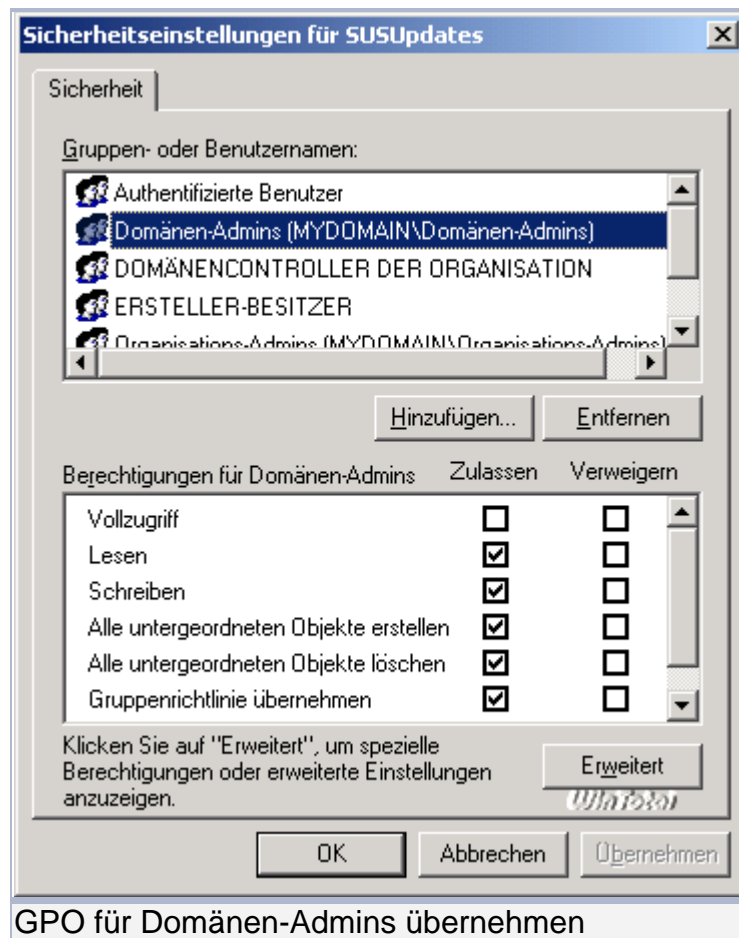


Bei diesem hier ist wichtig zu wissen, dass das Deaktivieren zu Datenverlusten führen kann, da ein User, der nur über "Benutzer-Rechte an einem Rechner verfügt, den automatischen Neustart NICHT aufhalten kann.

Wir beenden die Konfiguration mit Klick auf OK und schließen den GPO-Editor. Da momentan die Standard-Delegierung für dieses GPO gilt, würden nur die Benutzer, nicht aber die Domänen-Admins diese Richtlinie übernehmen, was zur Folge hat, dass der Server selbst nicht geupdatet wird. Um dies zu ändern, rufen wir uns den Delegierungs-Dialog in der GPMC auf:



Ein Klick auf "Erweitert" liefert uns die Einstellungen, wer dieses GPO übernimmt und wer nicht, hier setzen wir bei der Gruppe "Domänen-Admins" den Haken bei "Gruppenrichtlinie übernehmen".



GPO für Domänen-Admins übernehmen

Damit ist die Konfiguration für das automatische Installieren von Updates abgeschlossen, sowohl die Clients als auch der Server sollten nun nach einem Neustart diese neuen Einstellungen laden und dann die Updates installieren.

Die Website <http://www.susserver.com> bietet einige nette Tools zur Verwaltung und Überwachung eines SUS-Servers an, u.a. lässt sich mit deren Tools nachvollziehen, welcher Client wann welches Update vom SUS-Server geladen und installiert hat usw.

Da hier die Systemvoraussetzungen so unterschiedlich sind wie die Wünsche der Benutzer, was denn nun überwacht werden soll, verzichte ich an dieser Stelle darauf, die Tools alle vorzustellen - das würde auch den Rahmen des Artikels deutlich sprengen.

Teil 7

SUS-Server Dateien bei Neuinstallation sichern

Läuft der SUS-Server erstmal eine Zeit, hat er einiges an Updates heruntergeladen. Wer nun den Server neu installieren muss und die ganzen Patches nicht nochmals herunterladen möchte, muss die folgenden Dateien sichern und auf dem neu eingerichteten SUS-Server wieder zurückspielen:

- Den ganzen Ordner `\SUS\content\cabs`, dessen Ziel bei der Installation des SUS angegeben wurde.
- Alle Dateien von `c:\inetpub\wwwroot\dictionaries\`
- Aus dem Ordner `c:\inetpub\wwwroot\` die Dateien **ApprovedItems.txt**, **aucatalog1.cab** und **aurtf1.cab**
- Aus dem Ordner `c:\inetpub\wwwroot\autoupdate\dictionaries` die Dateien **ApprovedItems.txt**, **providerslots.txt**, **settings.txt**

Damit der neue SUS-Server die Konfiguration und Dateien übernimmt, muss der Systemdienst **Software Update Synchronization Service** neu gestartet werden.

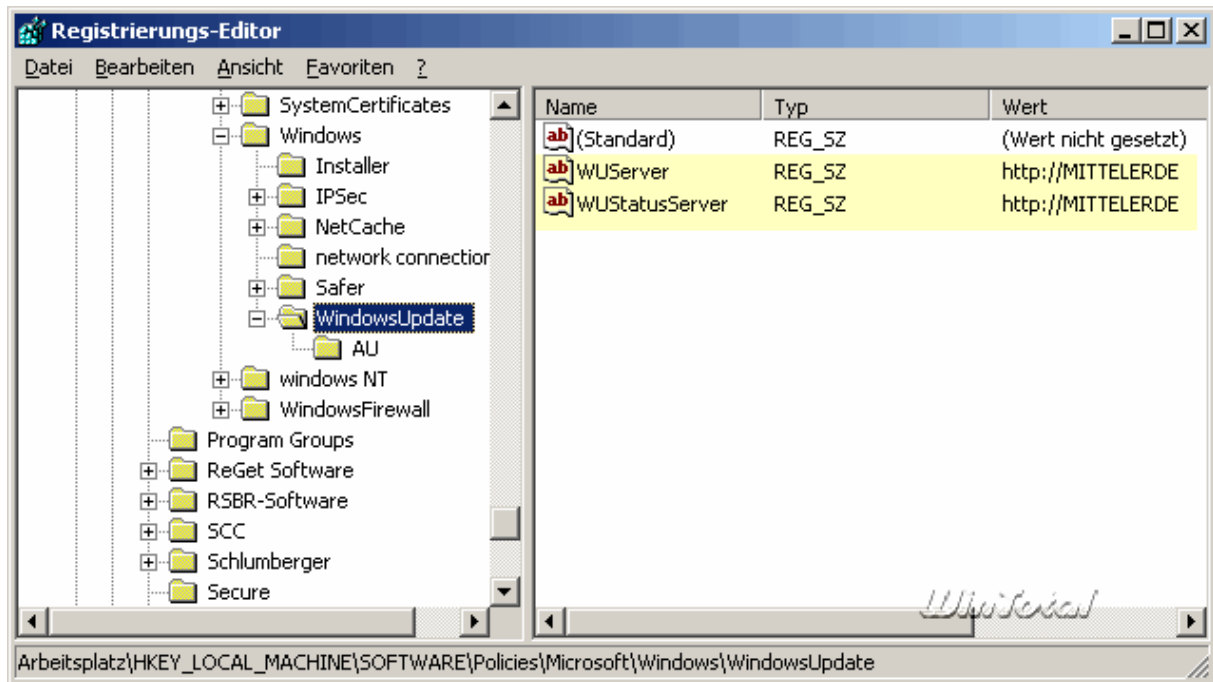
Teil 8

Clients nur kurzfristig an SUS-Server anbinden

Wer einen SUS-Server betreibt (Software Update Services Server von Microsoft), kann auch Clients nur kurzfristig zum „Auffrischen“ der Rechner an den SUS-Server binden (z.B. PC von Bekannten). Dafür muss einzig die Erreichbarkeit des SUS-Servers sowie der AutoUpdate-Modus festgelegt werden.

Für das kurzfristige Einbinden eignet sich hervorragend das kostenlose Tool Software Update Service Utility (<http://wintotal.de/softw/index.php?id=2044>). Das Kommandozeilenprogramm bindet einen Rechner kurzfristig an einen SUS-Server. Man gibt als Parameter die IP oder den Rechnernamen an. Danach stoppt das Programm den Update-Dienst, startet diesen neu. Windows braucht dann bis zu 10 Minuten, um den SUS-Server zu kontaktieren. Nach einem Neustart entfernt sich das Programm wieder selbstständig. Wer die Einstellungen lieber von Hand vornimmt, muss zunächst den Dienst „Automatische Updates“ über **net stop wuauserv** oder über die Dienstverwaltung stoppen.

Die folgenden Änderungen an der Registry müssen später wieder rückgängig gemacht werden. Aus diesem Grund empfiehlt es sich den Zweig unter `HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Microsoft\ Windows\ WindowsUpdate` sowie `HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ WindowsUpdate\ Auto Update` vorher komplett als REG-Datei zu exportieren und später wieder einzulesen. Anschließend werden in der Registry unter `HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Microsoft\ Windows\ WindowsUpdate` die folgenden Zeichenfolgen geändert: **WUServer** mit Wertangabe des Servers (am besten die IP mit `http://`) und **WUStatusServer** mit Wertangabe des Servers (am besten die IP mit `http://`)



Zudem muss man einen Unterschlüssel **AU** mit folgenden REG-DWORD-Einträgen anlegen:

"NoAutoRebootWithLoggedOnUsers"=1

"NoAutoUpdate"=0

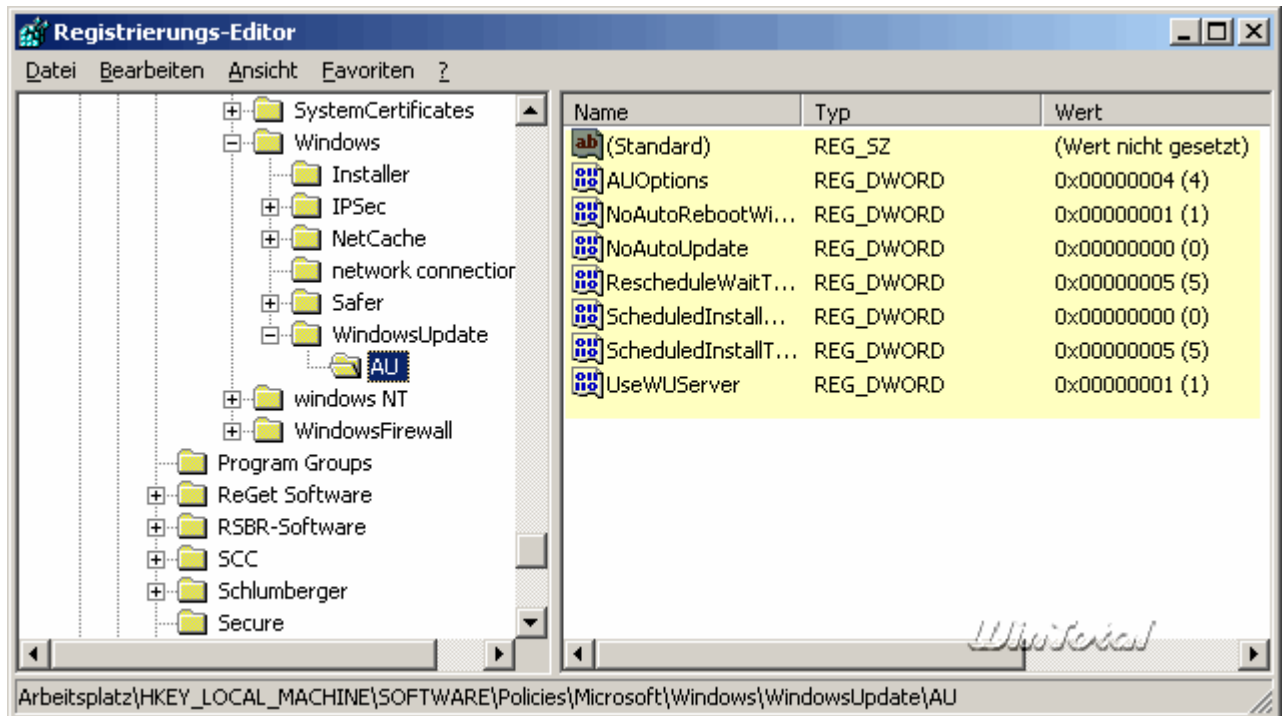
"AUOptions"=4

"ScheduledInstallDay"=0

"ScheduledInstallTime"=b

"RescheduleWaitTime"=5

"UseWU Server"=1



Durch die Angabe "AUOptions"= 4 werden alle nötigen Updates ohne Nachfrage vom Server geladen und auch installiert. Nur bei einem Neustart wird der Anwender gefragt. Wer gezielt noch Updates ablehnen möchte, muss dagegen AUOptions = 3 verwenden (bei beiden Einträgen) und sich als Administrator in dieser Zeit angemeldet haben.

Anschließend löscht man in der Registry unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update* die Werte bei **LastWaitTimeout**, **DetectionStartTime**, **NextDetectionTime** (sofern vorhanden) und ändert den Wert des Eintrags **AUState** auf „2“. Danach startet man den Dienst „Automatische Updates“ (z.B. über die CMD **net start wuauserv**) wieder und wartet, bis eine Verbindung zum SUS-Server aufgebaut wird (kann bis zu 15 Minuten dauern). Sind alle Updates geladen und der Rechner ist neu gestartet, muss man die Veränderungen an der Registry wieder rückgängig machen.

Weitere Informationen finden sich auch auf Susserver.com und bei Microsoft im SUS Deployment Guide

<http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx>