Windows Server 2003

Konfiguration als Domänencontroller & weitere Möglichkeiten



Inhaltsverzeichnis

- **<u>Teil 1</u>** Grundwissen und ein bisschen Theorie
- Teil 2 Einrichten des Active Directory
- <u>Teil 3</u> Konfiguration von DNS-/WINS- und DHCP-Serverdienst Einstellungen auf den Clients + Hineinheben der Clients in die Domäne
- <u>Teil 4</u> Erstellen der benötigten Freigaben, Anlegen von Usern Zuweisen Basis- und Profilordner Einführung Gruppenrichtlinien
- <u>Teil 5</u> Erstellen und Verknüpfen eines Login-Skripts, setzen von lokalen Berechtigungen, DHCP-Reservierungen für die Clients
- <u>Teil 6</u> Installation und Konfiguration der Software Update Services (SUS)
- <u>Teil 7</u> SUS-Server Dateien bei Neuinstallation sichern
- **<u>Teil 8</u>** 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 <u>Glossar von AT-Mix</u> 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 <u>LAN</u> 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 <u>Windows 2000</u> als Active Directory bekannt - ist es im Grunde, <u>Rechner</u> 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 "<u>Active Directory</u>" (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 <u>Active Directory</u> ein, d.h. wir stufen den Server zum Domänencontroller hoch.

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

Servername: IP-Adresse: DNS-Domain: NETBIOS-Domain: MYDOMAIN

TESTSERVER 192.168.10.254/24 mydomain.local

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

gemein Authenklisierung Enweitert /etbindung herstellen über: Intel 21140-basierter PCI-Fast Ethemet/ Nerse Verbindung verwendet folgende Elemen Clerif für Microsoft-Netzwerke Clerif für Microsoft-Netzwerke Datei- und Druckertreigabe für Microsoft	Adapter (Standard Kgnligurieren te:
Yetbindung herstellen über. ■ Intel 21140-basierter PCI-Fast Ethemetv Nese Verbindung verwendet folgende Elemen ■ Elem für Microsoft-Netzwerke ■ Netzwerklastensouglisch ■ Jate- und Druckertreigabe für Micros	Adapter (Standard Kgntigutieten te:
Intel 21140-basenter PD-Fast Ethemet Verbindung verwendet folgende Elemen Of Clent für Microsoft-Netzwerke Netzwerklastenausgleich Date- und Druckertreigabe für Micros	Adapter (Standard Kontigurieren te: coft-Netzwerk e
Viese Verbindung verwendet folgende Elemen Ø Elemi für Microsoft-Netzwerke Ø Netzwerklantensungleich Ø Latei- und Druckertreigabe für Micro	Kontgurieren te: colt-Netzwerke
Nese Verbindung verwendet lolgende Elemen Die Gent für Microsoft-Netzwerke Die Netzwerklaritenausgleich Datei- und Druckertreigabe für Micro	ie: :oft-Netzwerke
Elent für Microsoft-Netzwerke Ketzwerklastenausgleich Elent für Understreigabe für Microsoft	alt-Netzwerke
	Firemashaltan
M T Internetprotokol [TCP/IP]	
Installeren Derstalleren	Eigenschaften
Beschreibung TCP/P das Standardsrotokoli 5.a WAN-Ne	towelke dat den
Datenaustausch über verschiedene, miteine Netzwerke ermöglicht.	ander verbundene
- Sumbal bai Mathing on in Infohmulich ann	
Zines as reasoning in modelet in an	-Weite
0	K Abbreche

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

igens	chaften von Internetproto	skoll (TCP/IP)
Allger	mein	
IP-E Net bez	Einstellungen können automatis zwerk diese Punktion unterstüt Netzwerkadministrator, um di alben. "E-Adresse automatisch bezi	ich zugewiesen werden, wenn di ich. Wenden Sie sich andernfalls a geeigneten IP-Einstellungen zu ehen
-0	Folgende IP-Adresse verwer	ndens
1	P-Adresse:	192 . 168 . 10 . 254
-	Sybnetzmaske:	255 . 255 . 255 . 0
	itandardgateway:	192 . 168 . 10 . 100
0	• DIS-Serveradresse a korral	ach bezañan
6	Folgende DNS-Serveradress	en verwenden:
	evorzugter DNS-Server:	4 4 4
4	Alternativer DNS-Server:	
		Erwote
		ACC

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:

Wählen Sie eine Funktion aus. Sie können i Intfernen, Offnen Sie Software, wenn die	noch nicht hinzugeň gewünschte Funiti	ügte Funktioner on nicht aufgef	hinzufügen und Fu Ihrt ist.	sktioner
Serverfunktion Dakteerver Drudsserver Anwendungsserver (IIS, ASP NET) Malkerver (NDP3, SMTP) Terminalserver RAS(VPN-Server Distance of treatment Distance of the Server Distance of the Server DHCP-Server Streaming Media-Server WINS-Server	Konfiguriert Nein Nein Nein Nein Nein Nein Nein Nein	on nicht aufgeruhrt ist. Domänencontroller (Active Directory) Domänencontroller speichern Verzeichnisdeten und verwalten Berutzersmelideprozesse und Verzeichnissuchen. Weitere Informationen über Domänencontroller.		
	< Zurück	Weiter >	Abbrechen	H

"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.



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 <u>Windows Server</u> 2003-CD im Laufwerk eingelegt sein, da der DNS-Server nun nachinstalliert wird. Entsprechend trefft ihr folgende Auswahl: "Nein, DNS auf diesem Computer installieren und konfigurieren" und klickt dann auf "Weiter".



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.

In PDF konvertiert von Lukas Läderach

				1
ie den vollständige suptaltz beispiel mit	en DNS-Namer Hosoft.com]	der neuen Dom	ine ein	
diger DNS-Name fr	ir die neue Dor	liäne:		
ain local				-
		a the street	hide here is	Abbreaks
5 a K	Sie den volktändig auptritz beitpiel mit diger DNS Mane fr an local	Sie den volitiöndigen DNS-Namen auptatz.beispel microsoft.com) diger DNS-Name für die neue Dor an local	Sie den vollständigen DNS-Namen der neuen Domi auptritz beitpiel microsoft com) diger DNS-Name für die neue Domäne: ain local	Sie den volktändigen DNS Namen der neuen Domäne ein auptatz beispiel microsoft com) diger DNS Name für die neue Domäne: an local

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.

NetBIOS-Domänenname Geben Sie einen NetBIDS-F	Namen für die neue Domäne an	S
Dieser Name wird von Benu neue Domäne zu identifizier zu übernehmen, oder geber	utzem von früheren Windows-Versionen verwendet, ur en Klicken Sie auf "Weiter", um den angezeigten Na 1 Sie einen neuen Namen ein.	n die men
<u>N</u> etBIDS-Domänenname:	XYCOMAIN	

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 trefft im Dialog "Berechtigungen" die Auswahl "Nur

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



Hiermit legt ihr fest, dass weiter DCs bzw. Domänen mindestens auf Windows 2000 bzw. <u>Server 2003</u> 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 Benutzername 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 <u>http://windowsupdate.microsoft.com</u> 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 (<u>Windows</u> 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.

Netzwerkdienste	×
Klicken Sie auf die Kontrollkästchen der Komponenten, die hinzugefügt bzw. entfer werden sollen. Grau gefüllte Kästchen kennzeichnen Komponenten, die nur zum Te installiert werden. Klicken Sie auf "Details", um die Unterkomponenten anzuzeigen.	nt eil
Unter <u>k</u> omponenten von "Netzwerkdienste":	
🗹 💂 DHCP-Protokoll (Dynamic Host Configuration Protocol) 0,0 MI	
🗹 🛃 DNS-Server (Domain Name System) 1,7 Mi	3
🗆 📃 Einfache TCP/IP-Dienste 0,0 MI	3
🗌 🗔 📮 Internetauthentifizierungsdienst 0,0 MI	3
🗆 📮 RPC-über-HTTP-Proxy 0,0 Mi	3
🗹 🚚 WINS (Windows Internet Name Service) 0,9 MI	3
	-
Beschreibung: Installiert einen DHCP-Server, der temporäre IP-Adressen Clientcomputern im gleichen Netzwerk zuweist.	
Erforderlicher Speicherplatz: 37 MB	
Verfügbarer Speicherplatz: 14446.5 MB	5
	hen
DHCP und WINS installieren	

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.

zugewiesen werden, wenn das Wenden Sie sich andernfalls an æigneten IP-Einstellungen zu	
n N	2
	7
192 . 168 . 10 . 254	
255 . 255 . 255 . 0	
192.168.10.100	
beziehen gerwenden: 192 , 168 , 10 , 254	
Erweitert 	
	zugewiesen werden, wenn das Wenden Sie sich andernfalls an reigneten IP-Einstellungen zu 192 . 168 . 10 . 254 255 . 255 . 255 . 0 192 . 168 . 10 . 100 beziehen gerwenden: 192 . 168 . 10 . 254 <u>Erweitert</u>

Dann bitte auf "Erweitert" klicken, auf der Registerkarte WINS ebenfalls die IP-

		•	0		
Adresse des Servers	eintragen und	"NetBIOS	über TCP/IP	aktivieren"	anschalten.

Erweiterte TCP/IP-Einstellungen
IP-Einstellungen DNS WIN
<u>₩</u> INS-Adressen in Verwendungsreihenfolge:
192.168.10.254 t
Hinzufügen Bearbeiten Entfernen
Wenn die LMHOSTS-Abfrage aktiviert ist, gilt sie für alle Verbindungen, für die TCP/IP aktiviert ist.
LMHOSTS-Abfrage aktivieren
NetBIOS-Einstellung Standard: NetBIOS-Einstellung des DHCP-Servers verwenden. Falls die statische IP-Adresse verwendet wird oder der DHCP-Server keine NetBIOS-Einstellung anbietet, wird NetBIOS über TCP/IP aktiviert. NetBIOS über TCP/IP aktivieren
NetBIOS über TCP/IP deaktivieren
Ullatotai
OK Abbrechen
Anpassen der TCP/IP-Einstellungen am Server - WINS

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:

å dismymt - [DNS\/TESTSERVER\/Re	verse-Lookupzonen]	미치
🤱 Dabei Aktion Ansicht Benater	1	8 🖂
🗢 🔶 🖪 💽 😭 🛢 🛙	3	
Cons Proved Lookyporen Proved Lookyporen Construction of the second o	Reversie Lookupzonen	
	I	
Reverse-Looku	Ipzone einrichten	

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.

iscent	
Activ	e Directory-Zonenreplikationsbereich
Si	e können festlegen, wie DNS-Daten im Netzwerk repliziert werden.
w	ie sollen Zonendaten repliziert werden?
0	Auf allen DNS-Servern in der Active Directory-Gesamtstruktur "mydomain.local"
C	Auf allen DNS-Servern in der Active Directory-Domäne "mydomain.local"
_	
	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local"
	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf
,	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen.
Ċ	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen. Auf allen Domänencontroller, die im Bereich der folgenden Anwendungsverzeichnispartition angegeben werden:
Ċ	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen. Auf allen Dgmänencontroller, die im Bereich der folgenden Anwendungsverzeichnispartition angegeben werden:
c	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen. Auf allen Dgmänencontroller, die im Bereich der folgenden Anwendungsverzeichnispartition angegeben werden:
C	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen. Auf allen Domänencontroller, die im Bereich der Folgenden Anwendungsverzeichnispartition angegeben werden:
	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen. Auf allen Dgmänencontroller, die im Bereich der folgenden Anwendungsverzeichnispartition angegeben werden: Image: State Sta
	Auf allen Domänencontrollern in der Active Directory-Domäne "mydomain.local" Wählen Sie diese Option, falls die Zone von Windows 2000-DNS-Servern, die auf Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen.) Auf allen Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen.) Auf allen Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen.) Auf allen Domänencontrollern in derselben Domäne ausgeführt werden, geladen werden sollen. Anwendungsverzeichnispartition angegeben werden: ())

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

Assistent zum Erstellen neuer Zonen
Zonentyp Der DNS-Server unterstützt verschiedene Zonen- und Speicherungstypen.
Wählen Sie den Zonentyp aus, den Sie erstellen möchten:
 Primäre Zone Erstellt eine Kopie einer Zone, die direkt auf diesem Server aktualisiert werden kann.
Sekundäre Zone Erstellt eine Kopie einer Zone, die auf einem anderen Server existiert. Mit dieser Option wird die Verarbeitungsmenge von primären Servern ausgeglichen und die Fehlertoleranz gewährleistet.
Stubzone Erstellt eine Kopie einer Zone, die nur Namenserver- (NS), Autoritätsursprungs- (SOA) und "Glue Host"- (A) Einträge enthält. Ein Server mit einer Stubzone ist für diese Zone nicht autorisierend.
Die Zone in <u>Active Directory speichern</u> (nur wenn der DNS-Server als Domänencontroller eingerichtet ist)
<u>المارة عام</u> < <u>Z</u> urück <u>W</u> eiter Abbrechen Hilfe Hilfe
DNS-Zone hinzufügen

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 Netzwerkkennung oder den Namen der Reverse-Lookupzone an. Netzwerkkennung: 192 .168 .10
Die Netzwerkkennung ist der Teil der IP-Adresse, der dieser Zone angehört. Geben Sie die Netzwerkkennung in ihrer normalen Reihenfolge (nicht umgekehrt) ein. Wenn Sie eine Null in der Netzwerkkennung verwenden, wird diese im Zonennamen angezeigt. Beispiel: Netzwerkkennung 10 erstellt Zone 10.in-addr.arpa und Netzwerkkennung 10.0 erstellt Zone 0.10.in-addr.arpa.
Name der <u>R</u> everse-Lookupzone: 10.168.192.in-addr.arpa
Klicken Sie auf "Hilfe", um weitere Informationen über das Erstellen einer Reverse-Lookupzone erhalten.
∠
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 (f ür Active Directory empfohlen) Diese Option ist nur f ür Active Directory-integrierte Zonen verf ügbar.
 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.
Ulla failai < Zurück
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:
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.
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.

In PDF konvertiert von Lukas Läderach

genschaften von TE	STSERVER		? ×
Debugprotokollierung Schnittstellen	Ereignisprotokol Weiterleitungen	lierung Überw Erweitert	achen Sicherheit Stammhinweise
Weiterleitungen helfe diesem Server nicht I folgenden DNS-Dom	n bei der Auflösung beantwortet werder änen weiterleiten.	g von DNS-Abfra n. Abfragen von N	gen, die von Namen in
<u>D</u> NS-Domäne:			
Alle anderen DNS-D	omänen		<u>N</u> eu
			Entfernen
Weiterleitungs-I <u>P</u> -Adr	essliste der gewähl	ten Domänen: n	
194.25.0.60	Entferner	_	
	Nach <u>o</u> be	n	
	Nach <u>u</u> nte	n	
<u>S</u> ek, bis zur Zeitüber Keine <u>R</u> ekursion	schreitung der Wei für diese Domäne s	erleitungsabfrage verwenden	en: 5 Whitetai
	ОК	Abbrech	en Ü <u>b</u> ernehmen
arver für die We	iterleituna va	on DNS-Anf	ragen einrichte

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".

gravino Generostatus Genero	Herungen Huru Registrienungen Huru Registrienungen Annen Sie die Computer- und Gruppeneinträge der a schlienen Kölen Sie auf "Aktion" und denn auf "Enträge inträge anzungen. Im Dalagfald "Dinträge anzeigen" inträge folgendermäßen filtern: die Registriente "Enträgeszerdnung", um nach Bestaer zu en der Begisterkante "Enträgesbestaer", um nach Bestaer zu Huru Bestaer bestaerbesten Gennagfunge Enträgesbestaer Bestaerbesten oder von Brein herzugsfüge Enträgesbestaer
---	--

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 <u>N</u> amensmuster 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
Suche starten Abbrechen
WINS testen

Das Ergebnis sollte so aussehen:

In PDF konvertiert von Lukas Läderach



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.

In PDF konvertiert von Lukas Läderach

Subsit Aligon Arrischt 2 Set Image: Set	Itestserver nydomán kozii [192.168.10.254] Image: Servich bizunfügen Ein Bareich bizunfügen Ein Bareich bizunfügen P-Adressen zugeriesen werden körnen. Kichen Sie im Merch "Adressen einen Bereich erstellen und konfiguieren, bevor dynamische P-Adressen zugeriesen werden körnen. Kichen Sie im Merch "Adressen inder Bereich", um einen neuen Bereich hirzunfügen. Weitere Enformationen zum Einstehten eines DHCP-Servern finden Sie in der Ordinahäfe. IJ/In To Kall
DHCP anpassen	

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.

P DHCP		
Dabai Aktion Anaicht	2	
🗢 -> 🗈 🔟 🗙 🖆	2 🖸 🛃 🖵	
P OHCP	testserv	er. nydonain. local [192.168.10.254]
E- testserver. mydone	Statistik angeigen	
a sa ra domaina	Neuer Bureich	Bereich hinsufügen
	Schern Wiederherstellen	In ist ein Sterich von IP-Admusen, die Computern, die dynamische IP-Admusen erfordern, en sind. Sei müssen einen Bereich erstellen und konfigurieren, bevor dynamische ein zugewiesen werden können.
	Alle Bereiche abstimmen Autorisierung gufheben	e in Menü "Aktion" auf "Neuer Beneich", um einen neuen Beneich himzuzfügen. nformationen zum Einrichten eines DHCP-Servers finden Sie in der Onlinehäfe.
	genutzerklassen definieren HerstellerNassen definieren Vordefinierte Ogsionen einstellen	misossi
	Alle Laska	• <i>Solutoral</i>
Erstellt einen neuen Bereich	Bruicht	•
DHCP anp	assen	

Ich habe in meiner Testumgebung nur zehn Adressen gewählt.

Bereichserstellungs-Assistent
IP-Adressbereich Sie können den Adressbereich für den Bereich bestimmen, indem Sie einen ganzen Satz von aufeinander folgenden IP-Adressen identifizieren.
Geben Sie den Adressbereich an, den der Bereich verteilt. §tart-IP-Adresse: 192.168.10.110 End-IP-Adresse: 192.168.10.119 Eine Subnetzmaske legt fest, wie viele Bits einer IP-Adresse für die Netzwerk- bzw. Subnetzkennung verwendet werden sollen und wie viele für die Hostkennung. Sie können die Subnetzmaske nach der Länge oder als IP-Adresse angeben. Länge: 24 Subnetzmaske: 255.255.255.0
001∩70३७) < Zurück <u>We</u> r्र> Abbrechen
IPs des DHCP angeben

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.

Bereichserstellungs-Assistent		
Ausschlüsse hinzufügen Ausschlüsse sind Adressen oder ein Adressbereich, die nicht vom Server verteilt werden.		
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.		
Start-IP-Adresse: End-IP-Adresse:		
Ausgeschlossener Adressbereich:		
E <u>n</u> tfernen		
Ulla Ta≷a) < Zurück Weiter > Abbrechen		
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 Lesedauer für die vom DHCP-Server vergebenen Einstellungen. Diese steht in der Standardeinstellung auf 8 Tage und kann für unsere Zwecke durchaus so belassen werden.

Bereichserstellungs-Assistent
Leasedauer Die Leasedauer bestimmt, für wie lange ein Client eine Adresse aus diesem Bereich verwenden kann.
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 DFÜ-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.
Begrenzt auf:
Iage: Stunden:
Ulta Tasai
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 b 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		
ß		
्याück <u>W</u> eiter > Abbrechen		
DHCP-Optionen festlegen		

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

Router (Standardgatew Sie können die Router verteilt werden sollen.	ay) oder Standardgateways angeben, die von diesem Bereich
Geben Steleine IP-Adre verwendet wird, hinzuzu IP-Adresse:	sse unten an, um die Adresse für einen Router, der von Ülients ifügen.
	Hinzyfligen
192.168.10.100	Entfernen Nach <u>o</u> ben Nach unten

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.

reichserstellungs-Assistent					
Domänenname und DNS-Server Das DNS (Domain Name System) ordnet Domänennamen zu und übersetzt die von Clients im Netzwerk verwendeten Domänennamen.					
Sie können die übergeordnete Domäne festle DNS-Namensauflösung verwenden sollen.	egen, die die Clientcomputer im Netzwerk für die				
Obergeordnete Domäne:					
Geben Sie die IP-Adresse für die Server an, u DNS-Servern im Netzwerk zu konfigurieren.	um Bereichsclients zur Verwendung von				
<u>S</u> ervername:	I <u>P</u> -Adresse:				
testserver.mydomain.local	Hinzufügen				
Auflösen	192.168.10.254 Entfernen				
	Nach <u>o</u> ben				
	Nach <u>u</u> nten				
	णीतांठका				
	< <u>Z</u> urück <u>W</u> eiter > Abbrechen				
mäne 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 ermöglic Broadcasts zur Registrierung und Auflösung v	ht Windows Clients, WINS abzufragen, bevor von NetBIOS-Namen verwendet werden.					
<u>S</u> ervername:	I <u>P</u> -Adresse:					
TESTSERVER	Hinz Nigen					
Auflösen	192.168.10.254 Entfernen					
	Nach <u>o</u> ben					
	<u>N</u> ach unten					
Ändern Sie die Option 046, Knotentyp WINS/ Verhalten für Windows DHCP-Clients zu ände	/NBT, in den Bereichsoptionen, um dieses ern.					
	णातंठस्त					
	< <u>Z</u> urück <u>W</u> eiter > Abbrechen					
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.

Le DHCP						
Datei Aktion Ansicht 2						
← → 🗈 🔟 📝 🐺 🧬						
P DHCP - testserver. nydomain. local [192, 168, 10, 254]	Bereichsoptionen					
	Optionsname	Hersteller	Wert	klasse		
E- Berech (192,168,10,0) PhotoMath	and Rouber	Standard	192, 168, 10, 100	Ceiter		
- Adversiences	2006 DNS-Server	Standard	192,168,10,254	Keine		
E 🚰 Reservierungen	044 WINS/NENS-Server	Standard	192.168.10.254	Caine .		
Bereichsoptionen	Ore with S/NB1-Knotentyp	Standard	008	kene		
Serveroptionen						
			R			
			- 11)),	อาร์อโอโ		
	1		5,511			
1						
1)			
DHCP kontrollieren						

Nun können wir den ersten Client in die Domäne heben. Ich gehe hier von XP-Clients aus, Win2000 funktioniert aber beinah 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. Diecm 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:

🖼 C:\WINDOWS\System32\cmd.exe
Hostname
Uerbindungsspezifisches DNS-Suffix: Beschreibung. Intel 21140-basierter PCI-Fast Ether netadapter (Standard) Physikalische Adresse 00-03-FF-DF-10-E7 DHCP aktiviert. Ja Autokonfiguration aktiviert Ja IP-Adresse. 192.168.10.110 Subnetzmaske. 192.168.10.100 DHCP-Server 192.168.10.254 DNS-Server. 192.168.10.254 Primärer WINS-Server. 192.168.10.254 Lease erhalten. Freitag. 10. Dezember 2004 20:25:43 Lease läuft ab. Samstag. 18. Dezember 2004 20:25:43
CMD

Wenn die Einstellungen stimmen, geht am Client wie folgt vor: Start => Systemsteuerung => System => Registerkarte "Computername" => 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
C Arbeitsgruppe:
ARBEITSGRUPPE
U/m/3861
Client in die Domäne setzen

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

Computernamen är	ndern ?×
	G
Geben Sie Namen ur Berechtigung dieser	nd Kennwort eines Kontos mit der Domäne beizutreten ein.
Benutzername:	🕵 MYDOMAIN\Administrator 💌 🔤
Kennwort:	•••••
	OK Abbrechen
Client in die Dor	näne 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).

Copyright © 1985- Microsoft Corporati	2001 Professional Microsoft
Benutzername:	Administrator
Kennwort:	•••••
Anmelden an:	MYDOMAIN
DE	Über das DFÜ-Netzwerk anmelden OK Abbrechen Herunterfahren) Optionen <<

Damit ist dieser Client nun Mitglied eurer Domäne, was ihr natürlich auch kontrollieren könnt: Startet am Server das MMC-SnapIn "Active Directory Benutzerund 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.

🐗 Active Directory-Benutzer und -	Computer				
🥥 Dabel Aktion Analchit Benaber	ĩ				_ _ _×
← → [1] [2] [3] [6] [× ≦	' 🖸 🗟 👩 🦉 🖉	🎽 🗸 🍕 📜			
Adve Directory-Benutzer und -Comp	Conputers 1. Objekte				
Gespeicherte Abfragen	Nanie	Typ	Beschreibung		
E- up reconantica	ESTPC .	Computer			
Conputers					
E Donain Controllers E E ExelanSecurityPrincipals					
Users					
	1 16				
				1111575351	
				5911119811	
<u> </u>	1				
	_			1	
Prüfuna, ob	Clients	im AD) sind		
	0		G		

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.

🛓 disrigint - [DNS\/TESTSERVER\/Fo	rward-Lookupzonen',mydomain.	local]	alo X
🤱 Dabei Aktion Ansicht Bensber	2		_0×
🗢 🔶 🗈 🐹 🗙 🔂 🗔	12 8 9 34		
La CNS	nydomain Jocal 11 Einträge		
 TESTSERVER 	Hare Jacks Johnstones Torestonationes Torestonationes Torestonationes Torestonationes Torestonationes Distriction net übergeordneteen Districtisch net übergeordneteen Districtisch net übergeordneteen Districtisch net übergeordneteen Districtisch net übergeordneteen	Typ AutorRiksunsprung (SOA) Namenserver (NS) Host (A) Host (A) Host (A)	[29], besteerver nydonuin local., hostnaste testierver.nydonain local. 192:168-10.254 192:168.10.10 192:168.10.254
			เปิดชององ
	•		•
Prüfung des D	NS		

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 Freigabenames.

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.



Gebt nun die benötigten Daten ein.

Ordnerfreigabe-Assi Name, Beschreit Legen Sie fest, verwenden kör	stent 🗵				
Geben Sie Informati Offlineverwendungs	ionen über die Freigabe für Benutzer an. Klicken Sie auf "Ändern", um die einstellungen von Inhalten für Benutzer zu ändern.				
<u>F</u> reigabename:	Profile\$				
Freigabepfad:	\\TESTSERVER\Profile\$				
B <u>e</u> schreibung:	Pfad f. servergesp. Profile				
<u>O</u> fflineeinstellung:	Ausgewählte Dateien und Programme sind offline verfü				
	Ŗ				
	/////∂/∂}∂/ <zurück weiter=""> Abbrechen</zurück>				
Neue Freigal	be				

Dann setzen wir die Berechtigungen für diese Freigabe.

Ordnerfreigabe-Assistent						
Berechtigungen Geben Sie Berechtigungen für die Freigabe an.						
Verwenden Sie eine der folgenden Standardfreigabeberechtigungen, oder erstellen Sie benutzerdefinierte Freigabe- und Ordnerberechtigungen.						
Alle Benutzer haben schreibgeschützten Zugriff						
Administratoren haben Vollzugriff, andere Benutzer haben schreibgeschützten Zugriff						
 Administratoren haben Vollzugriff, andere Benutzer haben schreibgeschützten Zugriff und Schreibzugriff 						
Benutzerdefinierte Freigabe- und Ordnerberechtigungen verwenden						
Da Berechtigungen, die Sie auf dieser Seite festlegen, nur den Zugriff auf die Freigabe steuern, sollten Sie Berechtigungen für einzelne Dateien und Ordner ebenfalls festlegen. Weitere Informationen über Berechtigungen finden Sie in der <u>Hilfe</u> .						
Klicken Sie auf "Fertig stellen", um die Freigabe zu erstellen.						
< <u>Zurück</u> Fertig stellen Abbrechen						
Peresetigung für die Freigebe						

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

Berechtigungen anpassen		<u>? ×</u>
Freigabeberechtigungen Sicherh	neit	,
<u>G</u> ruppen- oder Benutzernamen:		
🕼 Domänen-Admins (MYDOM	AIN\Domänen-Ad	mins)
🗾 👧 Domänen-Benutzer (MYDO	MAIN\Domänen-B	enutzer)
	Hinzufijgen	Entfernen
Berechtigungen für Domänen-Be	enutzer Zulassen	Verweigern
Vollzugriff		
		H
		บปลาร์จิต
	OK	Abbrechen

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 <u>Active Directory</u> 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.

Active Directo	ry-Benutzer und -Co	mouter				
Dates Argon	Anacht genetar	1. [7][9][4] 3m 207 4.	TT /3 14			1012
Adive Directory	-Benutzer und -Compi	LEI 1999 L 3' 112 1124 mai Users 21 Objekte	भ ब्यु हा			
El 🤤 Gespeichero	e Abhragen	Nanie	Typ	Bestvelbung		
E ge redorment en	es es Socurt) Principals Socurt) Principals de Tosks este socurt societ de Tosks Societ Societ de Tosks Societ Soci Societ Societ Soci Societ Societ Societ Societ Societ	Administrator De409-Administrator De409-A	Bendure Scherheitsgrup Scherheitsgrup Scherheitsgrup Scherheitsgrup Scherheitsgrup Bendure Scherheitsgrup der Scherheitsgrup Bendure Scherheitsgrup	Vardahnarban Konto Fir Pilogladar, da Administra Pilogladar, da mar Lamazu Gruppe TMS-Administrat CHSI-Charth, da elyamin Administratore der Donn Alle Stestationen und Alle Stestationen und Alle Giste derer Donsler Vardahnarban Konto Fir Gruppe für dis Hiffe und Server in desser Gruppe E Nitglieder desser Gruppe Nitglieder desser Gruppe		
					切れわるれ	
Instalk ein neues Ob	jest.					l.
1	D					
veuen	Benutz	er anleger	ו			

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

Neues Objekt - Benutz	er	×
Erstellen in	n: mydomain.local/Users	
⊻orname:	Test <u>I</u> nitialen:	
<u>N</u> achname:	User	
Vollständiger Name:	Test User	
Ben <u>u</u> tzeranmeldenam TestUser	e: @mydomain.local	
B <u>e</u> nutzeranmeldenam	e (Prä-Windows 2000):	
MYDOMAIN\	TestUser	
	Ulatosai	_
	< <u>Zurück</u> <u>W</u> eiter > Abbrecher	
leuer 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/Us	ers
Kennwort:	
Kennwort <u>b</u> estätigen:	
🔲 Benutzer <u>m</u> uss Kennwort bei der nächste	en Anmeldung ändern
🔲 B <u>e</u> nutzer kann Kennwort nicht ändern	
🗖 Kennwort Jäuft nie ab	
Konto ist <u>d</u> eaktiviert	
	णानकेन
< <u>Z</u> ur	ück 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.

Mitglied von Einwählen Umgebung Sitzungen Remoteüberwachung Terminaldienstprofile COM+ Allgemein Adresse Konto Profil Rufnummern Organisation Benutzerprofil	enschaften von Tes	st User			?
Remote uberwachung Terminaldienstpronie CUM+ Allgemein Adresse Konto Profil Rufnummern Organisation Benutzerprofil Profilpfad: \\\TESTSERVER\PROFILE\$\\%USERNAME% Anmeldeskript: I Basisordner I © Lokaler Pfad: mit: RVER\USER\$\%USERNAME% ØVin röttil I ØK Abbrechen Ubernehme	Mitglied von	Einwählen	Ι U	mgebung	Sitzungen
Benutzerprofil Profilpfad: \\TESTSERVER\PROFILE\$\%USERNAME% Anmeldeskript: I Basisordner Lokaler Pfad: Verbinden von: U: mit: RVER\USER\$\%USERNAME%	Allgemein Adresse	ng Konto	Profil	Rufnummern	Organisation
Benutzerpron Profilpfad: \\TESTSERVER\PROFILE\$\\%USERNAME% Anmeldeskript: I Basisordner I © Lokaler Pfad: I @ Verbinden von: U: mit: RVER\USER\$\%USERNAME% U//// 78/61 U//// 78/61 I OK Abbrechen Ubernehme	- D		1		
Profilpfad:	Benutzerproni	UTFOTOF			
Anmeldeskript:	Profilpfad:	INTESTSE	RVERNPH	IUFILE\$\%USEF	INAME %
Basisordher Lokaler Pfad: Verbinden von: U: mit: RVER\USER\$\%USERNAME% UIntotat OK Abbrechen Ubernehme	Anmelde <u>s</u> kript:		Ι		
Basisordner Lokaler Pfad: Verbinden von: U: mit: RVER\USER\$\%USERNAME% UInTotal OK Abbrechen Ubernehme					
○ Lokaler Pfad: ● Verbinden von: U: ● Mill: milt: RVER\USER\$\%USERNAME% Ut/milletail OK Abbrechen Ubernehme	Basisordner				
Verbinden von: U: ■ mit: RVER\USER\$\%USERNAME%	O Lokaler Pfad:				
Ulla foto de la companya de la compa	Verbinden von:		nit: BVE	B\USEB\$\%US	FBNAME성
णात्रस्त OK Abbrechen <u>Ob</u> ernehme			nie linie		
णातरुखा OK Abbrechen <u>Ob</u> ernehme					
Ultriotal OK Abbrechen <u>Ob</u> ernehme					
Ulin foitai OK Abbrechen <u>Ob</u> ernehme					
Ulla fotol OK Abbrechen <u>Ob</u> ernehme					
WhiteRat OK Abbrechen Obernehme					
Ultriotal OK Abbrechen Obernehme					
Ulfatetat OK Abbrechen Obernehme					
OK Abbrechen Übernehme				ų.	ଆର୍ଶଚଞ୍ଚା
		(эк	Abbrechen	0 <u>b</u> ernehme
	afilmfa al una d Du				

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 xbeliebigen 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: <u>http://WinTotal.de/softw/index.php?id=2545</u>

Installiert diese bitte direkt auf dem <u>Server</u>. 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.

Gesantstruktur nydonain Jocal Gela Conaren	Velkna	mydomain.local Vetinigite Snapenichtinenderkte Gruppenichtinenventrung Delegerung						
Portuit Domain Rolloy Portuit Domai	01 4 5 10 01	Vetniplagoreherikige - T	Gisppenichtinerobjekt Statut Doman Policy	Erzeungen	Unit	Status des Grupperrichtile Aktivient		

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:

Neues Gruppenrichtlinienobjekt	×
Name: Ordnerumleitung	
	OK Abbrechen
Neues GPO	

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

In PDF konvertiert von Lukas Läderach

					included a
Gruppenrichtlinienobje Inheit Delegenorg Name - Stelast Doman Roky Stelast Doman Roky Stelast Doman Roky Stelast Doman Roky Schemung - Schemung - Schemung - Beglitt seehen Eigeren Lieben	kte in mydomein local	WHI-Falo Knine Koine Knine	Gesindert 27.11.2004 11: 21.11.2004 11: 00.07.2005 14:	Besitzer Dominenr-Ad. Dominenr-Ad.	
Undersonnen Aktualsonen			Whato	807	
2			3 Gruppervichtlinie	nobriekt/	

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.

🚡 Gruppenrichtlinienobjekt-Editor			
+ → IE B G G			
Computerioring Insciences motional local lists Computerioringunation Softwareshallungen Windows-Enstellungen Windows-Enstellungen	Ordnerumkeitung [testserver Markeren Sie ein Siement, um demen Beschreibung anzuzeigen.	mydomain.local] Richtlinie Name Computeriorfiguration Benutzeriorfiguration	
in û Wedows-Enstellungen in û Administrative Yorlagen	•		
4 ×	Ervedard / Standard /	เป็นสอริส	
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:

when mishing Decisioner, purchasin, local Birth	Nume	Turn	T
Consultationality (Indexentionality of the analysis) Consultation (Indexention of the analysis) Software exists it was a set of the analysis of t	L.	in deser Ansicht werde	n keine Elemente angezeigt.
			Ula fosal

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

Eigenschaften von Eigene Dateien
Ziel Einstellungen
Sie können den Pfad des Ordners "Eigene Dateien" angeben.
Einstellung: Standard - Leitet alle Ordner auf den gleichen Pfad um. 💌
Dieser Ordner wird auf den angegebenen Pfad umgeleitet.
Zielordner In das Basisverzeichnis des Benutzers kopieren ▼
5
P%
Hinweis: Diese Einstellung ignoriert den Wert der Option "Benutzer exklusiven Zugriff auf Eigene Dateien erteilen" auf der Einstellungsseite.
เป็นสอริสา
OK Abbrechen Ü <u>b</u> ernehmen
GPO bearbeiten

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

Eigenschaften von Eigene Dateien	<u>?</u> ×
Ziel Einstellungen	1
Wählen Sie die Umleitungseinstellungen für Eigene Dateien.	
Dem Benutzer exklusive Zugriffsrechte für Eigene Dateien erteiler	
🔽 Den Inhalt von Eigene Dateien an den neuen Ort verschieben	
Entfernen der Richtlinie	
Ordner nach Entfernen der Richtlinie am neuen Ort belassen	
 Ordner nach Entfernen der Richtlinie zurück an den Ort des lokale Benutzerprofils umleiten 	en
Einstellungen für den Ordner "Eigene Bilder"	
💿 Ordner "Eigene Bilder" dem Ordner "Eigene Dateien" unterordner	n
C Keine administrative Richtlinie für den Ordner "Eigene Bilder"	
UIATORA	/
OK Abbrechen Ü <u>b</u> erne	ehmen
GPO bearbeiten	

Nun schließt ihr den Gruppenrichtlinienobjekte-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 "Delegierung" an.

E Group Policy Management	Ordnerumleitung				
G Gesantsouturi mydonian Jocal	Bereich Details Einstellungen Delegierung				
E 🖓 nydonain local	Folgende Gruppen und Benutzer haben die angegebe	me Benechtigung für dieses Gruppensichtliniensbeikt			
St Default Domain Policy	Bappen und Benutzer				
Concernint/diservable/te	Name -	Zuläczge Berechtgungen	Geett		
C Default Domain Controllers Policy	Authentificiente Benutzer	Lesen (durch Sicherheitslitterung)	Nein		
Default Domain Policy	Dominen-Admins (MYDOMAIN/Dominen-Ad.	Einstellungen bearbeiten / Löschen / Sicherheit verändern	Nein		
Croherunietung	ZDOMANENCONTROLLER DER ORGANISAT	Lesen	Nem		
Radiate	SVSTEM	Einstellungen bearbeiten / Loschen / Sicherheit verandern Einstellungen bearbeiten / Lischen / Sicherheit verändern	Neit		
	and the second	Ula tosal			
	Englemin	Egeneration E	Investor 15		
	1.	11	1		

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

Sicherheitseinstellungen für Ordneru	mleitung	×
Sicherheit		
<u>G</u> ruppen- oder Benutzernamen:		
Authentifizierte Benutzer		
🗾 🕵 Domänen-Admins (MYDOMAIN\D	omänen-Adr	nins)
DOMÄNENCONTROLLER DER (ORGANISAT	
ERSTELLER-BESITZER		_1
■ Organisations-Admine (MYDOMAII	MAraanieati	one-Admine)
<u>H</u> inz	ufügen	<u>E</u> ntfernen
Berechtigungen für Authentifizierte Benutzer	Zulassen	Verweigern
Vollzugriff		
Lesen		
Schreiben		
Alle untergeordneten Objekte erstelle	n 📙	
Alle untergeordneten Ubjekte losche	n 🔟	
Klicken Sie auf "Erweitert", um spezielle Berechtigungen oder erweiterte Einstelli anzuzeigen.	e ungen _	Er <u>w</u> eitert Whatatan
ОК	Abbrechen	<u>Ob</u> ernehmen
GPO übernehmen		

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

therheitseinstellungen für Oro	Inerumleitung	>
Sicherheit		
<u>G</u> ruppen- oder Benutzernamen:		
🕵 Authentifizierte Benutzer		_
👧 Domänen-Admins (MYDOM/	AIN\Domänen-Ad	mins)
🕼 DOMÄNENCONTRAJLLER I	DER ORGANISA	гіом 🔄
🕵 ERSTELLER-BESITZER		
Contractions-Admine (MVD)	OMAIN\Organicat	ione.Admine
	<u>H</u> inzufügen	<u>E</u> ntfernen
Berechtigungen für Domänen-Adr	_{mins} Zulassen	Verweigern
Vollzugriff		
Lesen	\checkmark	
Schreiben	\checkmark	
Alle untergeordneten Objekte e	erstellen 🗹	
Alle untergeordneten Objekte li	öschen 🗹	
Gruppenrichtlinie übernehmen		
Klicken Sie auf "Erweitert", um sp Berechtigungen oder erweiterte E anzuzeigen.	ezielle instellungen	Er <u>w</u> eitert เปฏิภาจะอา
OK	Abbrechen	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.

EGroup Policy Management 15 Datas Altion Anacht Benatur 2			21a 81a
Group Policy Hanagament Gesentstruktur mydowan Jocal Gosentstruktur mydowan Jocal Gosentstruktur nydowan Jocal Gosent Policy Gosent Policy Gosent Policy Gosent Controllers Gosent Controllers Gosent Controllers	Ordnerumleitung Besteh Detals Einstekungen Delege Verknäptungen Für dense Verzechnis anzeigen: ander Die fogenden Standote, Demänen und D	sung nan. Ioc al ganisationweinheiten sind wit dem Objek	(verknight
Default Domain Controllers Policy	Ptad =	Etzwungen Verknüphung :	Rivert Plad
in Gay wett reach?	Sichesheitsfilterung Die Einstellungen dieses Grappenschliese Brapen, Bendzer und Coepute: Name -	objekts gellen na fut die folgenden	
	Endufferetrizente Benutzen Hinzufligen	Egentratie	
	WHI-Filterung Dieses Gruppenrichtlinienstijelit ist mit tolg Keino	enden WM Fåer vesknipft	Ulintəsəl I
	1		

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.

Ordnerfreigabe-Assi	istent X
Name, Beschreil Legen Sie fest, verwenden kör	bung und Einstellungen , wie Benutzer diese Freigabe im Netzwerk anzeigen und nnen.
Geben Sie Informati Offlineverwendungs	ionen über die Freigabe für Benutzer an. Klicken Sie auf "Ändern", um die seinstellungen von Inhalten für Benutzer zu ändern.
<u>F</u> reigabename:	Data
Freigabepfad:	\\TESTSERVER\Data
B <u>e</u> schreibung:	Freigabe für allg. Benutzerdaten
Offlineeinstellung:	Ausgewählte Dateien und Programme sind offline verfü Ängern
	marazai
	< <u>∠urück</u> <u>W</u> eiter > Abbrechen
Neuen Ordne	er 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:

🗁 C:\Profile\$				×
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>F</u> a	voriten E <u>x</u> tras	2		7
🔇 Zurück 👻 🕤 👻 🏂 Suc	hen 防 Ordner	😰 🌶 🗙 🍤 🖪		
Adresse 🛅 C:\Profile\$			💌 🔁 Wechseln z	:u
Name 🔺	Größe	Тур	Geändert am	
TestUser		Dateiordner	07.01.2005 11:24	
•			Illarosoi .	F
1 Objekt(e) ausgewählt		🚽 😽 Arbeitsplatz		*
Profilordner				

🗁 C:\User\$			
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>F</u> a	voriten E <u>x</u> tras	2	A.
🌀 Zurück 👻 🕤 👻 🏂 Suc	hen 🌔 Ordner	🖻 🕑 🗙 🍤 [
Adresse 🛅 C:\User\$			💌 🔁 Wechseln zu
Name 👻	Größe	Тур	Geändert am
TestUser		Dateiordner	07.01.2005 11:24
•			Ullarokai 🕨
1 Objekt(e)	0 Byte	😪 Arbeitsplatz	
User-Ordner			

Eigenschaften von Eigene Dateien	?×
Ziel Allgemein Sicherheit	
Der Ordner Eigene Dateien ist eine Verknüpfun unten angegebenen Zielordner.	g zum
Zielordner Ziel: <u>INTESTSERVERNUser\$NTestUser</u>	
Ullai	5247
OK Abbrechen Übe	rnehmen
Eigene Dateien	

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 <u>www.gruppenrichtlinien.de</u> 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 <u>Server</u> verbindet.

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



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 denjenigen, 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.

	st User _?
Mitglied von Remoteüberwacht Allgemein Adresse	Einwählen Umgebung Sitzungen Ing Terminaldienstprofile COM+ Konto Profil Rufnummern Organisatic
Benutzerprofil <u>P</u> rofilpfad: Anmelde <u>s</u> kript:	\\TESTSERVER\Profile\$\TestUser
Basisordner C Lokaler Pfad: C Verbinden von:	U: mit: \\TESTSERVER\User\$\TestUs
	Watera

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.

Group Patry Planetaria A Geographics Planetaria Group Patry Planetaria Geographics Geographi	Gruppenrichtliniesobjek	ite in mydomain.local				
Conservation	Rem - 3 Delas Donais Costoles. 3 Delas Donais Poloy 3 Logistat 3 Octowerketing	Stan und Texposit fini datain	VMPR	U//// ///	Finitop Donineen Ad Donineen Ad Donineen Ad	
	<u></u>			4 Gruppervichtlinier	ebailti .	_

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

Script über Gruppenrichtlinie zuweisen	Gruppenerschiltmisenskijskit-Editor		
Creater understanden Constant information Constant informa	Dies tellen Belga I		
Script über Gruppenrichtlinie zuweisen	◆ → ¹		
Script über Gruppenrichtlinie zuweisen	Longerskipt, Destansver mydonain.bical Ficktifnia Congerskipt, Destansver mydonain.bical Ficktifnia Softwersentetkingen Middee-Gintallungen Middee-Gintal	tere Demoiden ⊇Atmoiden	
Script über Gruppenrichtlinie zuweisen		L;	
Script über Gruppenrichtlinie zuweisen		Country's Second	Ularotar
Script über Gruppenrichtlinie zuweisen		(many, saved)	
Script über Gruppenrichtlinie zuweisen			•
	Script über Grup	penrichtlinie zuv	veisen

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

Eigenschaften von Anmelden	<u>?</u> ×
Skripts	
Skripts zum Anmelden für Loginskript	
Name Parameter	
	Nach <u>o</u> ben
	Nach <u>u</u> nten
	Hinzufügen
	Bearbeiten
	Entrement
Gruppenrichtlinienobjekt anzuzeigen.	sem
Dateien anzeigen	
	Ullatotal
OK Abbreche	n <u>Ob</u> ernehmen
Script über Gruppenrichtlinie zuweisen	

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).

Durchsuchen						<u>?×</u>
<u>S</u> uchen in	: 🤤 NETLOGON a	an Testserver	-	- 😗 🛛	• 😁 🔰 🌶	
Zuletzt verwendete D	login.bat					
Desktop						
🤌 Eigene Dateien						
State Arbeitsplatz						
S						
Netzwerkumge	Datei <u>n</u> ame:	login.bat			Black	<u>}∂ÿf</u> fnen
Dung	Dateityp:	Alle Dateien			•	Abbrechen
Script über G	ruppenrichtlini	e zuweisen				

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).

Jiggen Alge geath feedw 1 ⇒ → C 10 10 17 12					_ID : _IØ ::
Group Policy Planapanent G. A Generativitizet systematical Group Contents	Gruppensichtiniesobjekte in mydomain.local Irinit Deisjawag				
Comparison Construction Con	Tyme - 2 Dena Bonen Gotode 3 Dena Ponen Poloy 3 Dena Ponen Poloy 3 Dehevenheteng	Status de Statgemichten dativen dativen dativen dativen dativen dativen dativen	Vell/Fage Exists Faite Faite Faite Faite	Bandoff 21111200411 21111200412 21111200412 21111200412 2111200812 0611200814	tentor Doniree-Md Doniree-Md Doniree-Md Doniree-Ad Doniree-Ad
				เปิโก (อา	a)
Drag an Drop auf	lokale Do	omäne			

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

Setzen lokalen Kommen wir nun zum von 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.

Computer auswählen	×
Wählen Sie den Computer aus, den dieses Snap-In verwalten soll.	
Dieses Snap-In verwaltet:	
C Lokalen Computer (Computer, auf dem diese Konsole ausgeführt wird)	
<u>Anderen Computer:</u> <u>testpd</u> <u>Durchsuchen</u>	
OK 19/1/ (Abblechen	
Computerverwaltung, anderer Computer	

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

In PDF konvertiert von Luk	as Läderach
----------------------------	-------------

📮 Computerverwaltung					
📃 Datei Aktion Ansicht Eenster	? _ _ _ ×				
Computerverwaltung (TESTPC)	Name System Datenspeicher Dienste und Anwendungen				
	เปิกสอริลโ				
Computerverwaltung, and	lerer Computer				

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

Eigenschaften von Administratoren	? ×
Allgemein	
Administratoren	
Bes <u>c</u> hreibung: Fänkten Vollzugriff auf den Computer bzw. die Domä r <u>M</u> itglieder:	e.
Administrator MYDOMAIN\Domänen-Admins	
Hinzufügen	,
OK Abbrechen Überne	hmen
Gruppe Administratoren	

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

Benutzer, Computer oder Gruppen wählen	<u>? ×</u>	
Objekttyp:		
Benutzer oder Gruppen	<u>O</u> bjekttypen	
Suchpfad:		
mydomain.local	<u>P</u> fade	
<u>G</u> eben Sie die zu verwendenden Objektnamen ein (<u>Beispiele</u>):		
Test User (TestUser@mydomain.local)	Namen überprü <u>f</u> en	
Erweitert	UIIABBrechen	
Gruppe Administratoren, hinzufügen		

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".

<u>Ф</u> рнср						
Datei Aktion Ansicht ?						
Ф рнср	Adressleases					
🖻 🔂 testserver.mydomain.local [192.	IP-Adresse des Clients	Name	Leaseablaufdatum			
Bereich [192.168.10.0] MYD Adresspool Adressleases Bereichsoptionen Serveroptionen	92.168.10.110	testpc.mydomain.local	31.01.2005 12:41:10			
6						
			เปิกสอริลโ			
	•			•		
<u> </u>						
DHCP						

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.

🖎 Eingabeaufforderung	<u>_ ×</u>
Microsoft Windows [Version 5.2.3790] (C) Copyright 1985-2003 Microsoft Corp.	-
C:\Dokumente und Einstellungen\Administrator>ping testpc	
Ping wird ausgeführt für testpc.mydomain.local [192.168.10.110] mit 32 Bytes en:	Dat
Antwort von 192.168.10.110: Bytes=32 Zeit<1ms TTL=128 Antwort von 192.168.10.110: Bytes=32 Zeit<1ms TTL=128 Antwort von 192.168.10.110: Bytes=32 Zeit<1ms TTL=128 Antwort von 192.168.10.110: Bytes=32 Zeit<1ms TTL=128	
Ping-Statistik für 192.168.10.110: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca. Zeitangaben in Millisek.: Minimum = Oms, Maximum = Oms, Mittelwert = Oms	
C:\Dokumente und Einstellungen\Administrator>_	
世界ものでいた	_
Ping zur IP	

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

🛤 Eingabeaufforderung				
C:\Dokumente und Einstellungen\Administrator>arp -a				
Schnittstelle: 192.168.10.254 0x10003 Internetadresse Physikal. Adresse Typ 192.168.10.110 00-03-ff-df-10-e7 dynamisch				
C:\Dokumente und Einstellungen\Administrator>				
		UUBGoVEREST		
			-	
MAC-Adresse über arn -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.

Neue Reservierung	<u>? ×</u>			
Geben Sie Informationer	n für einen reservierten Client an.			
Reservierungs <u>n</u> ame:	TestPC			
IP-Adresse:	192.168.10.80			
MAC-Adresse:	00-03-ff-df-10-e7			
B <u>e</u> schreibung:	Erster PC im LAN			
Unterstützte Typen — O Bei <u>d</u> e				
⊙ Nur DH <u>C</u> P ○ Nur BOOT <u>P</u>				
	Hinzufügen			
Reservierung über MAC-Adresse				

Nach Klicken von OK sollte das in etwa so aussehen:

LO DHCP			_O×			
Datei Aktion Ansicht ?						
	<i>\$</i>					
😰 DHCP	[192.168.10.80] TestPC					
📋 🗟 testserver.mydomain.local [192.168.10.2	Optionsname	Hersteller	Wert			
Bereich [192.168.10.0] MYDOMAIN	💞 003 Router	Standard	192.168.10.100			
Adressleases	💞 006 DNS-Server	Standard	192.168.10.254			
	@044 WINS/NBNS-Server	Standard	192.168.10.254			
	1046 WINS/NBT-Knotentyp	Standard	0x8			
Bereichsoptionen						
Serveroptionen						
		ma	25251			
	•		• • • • •			
)			

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.

CHICP						
Qabei Kilgon ğınadıt j						
2 0HO	Adresoleases					
B - B tector ver. nydanain. kcal [192.168.	(P-Adresse des Clents	Hana	Leoseablas/risk.m	7/2	Endeutige Kenneng	De
- Advergool	and 197.168.18.80	16SUPC	Reserverung (maktiv)	Keste	constit/d/sowr	- 61
Advestigates	A 192, 169, 18, 19, 19	tadąc.nydanah.local	31.01.2005 12:41:10	DHIDP	000207473067	
🗄 🎑 Reservierungen						
- 20 Terrichsoniares						
- Serversptieren		R				
						- 1
						- 1
						- 1
						- 1
						- 1
						- 1
				- <u>U</u> h	10101	- 1
1	4					1
	A 1		A 1			
Noch wird eine	Adresse	aus dem	1 Adress	pool	verwen	det

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



Lösen der IP



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



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 <u>Skript GetMac</u> 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 Gruppenrichtlinien. Aber der Verteiluna erfolgt via 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 SUSSP1: 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 (It. 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.

Anwendungsserver	×
Klicken Sie auf die Kontrollkästchen der Komponenten, die hinzugef werden sollen. Grau gefüllte Kästchen kennzeichnen Komponenten, installiert werden. Klicken Sie auf "Details", um die Unterkomponent	ügt bzw. entfernt , die nur zum Teil en anzuzeigen.
Unter <u>k</u> omponenten von "Anwendungsserver":	
🗆 🚡 Anwendungsserverkonsole	0,0 MB 🔺
🗆 🍓 ASP.NET	0,0 MB
🗹 👰 COM+-Netzwerkzugriff aktivieren	0,0 MB
🗆 🗊 DTC-Netzwerkzugriff aktivieren	0,0 MB
🗹 🎀 Internetinformationsdienste (IIS)	18,1 MB
🗌 🚅 Message Queuing	6,5 MB
Beschreibung: IIS enthält Web-, FTP-, SMTP und NNTP-Unterstüt Unterstützung für FrontPage und Active Server Pag	zung sowie jes (ASP).
Erforderlicher Speicherplatz: 14,2 MB	Details
Verfügbarer Speicherplatz: 14392,3 MB OK	<u>し</u> <i>UIMTのその1</i> Abbrechen
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:

Date: Rearbotton Janairit Recordses Future 7	
Cause - C - A - C - Salar Artesta Reador - C - C - C	_
Here The Scholar Scholar	Y Stehen a Lite
The second second	
Software Update Services	
Subware tighter Services Set options	
Set, your Software Lipitate Services options, and then dish Apply.	
Synchronize server Select a perger enrice configuration:	
Approve updates P De not use a prove server to access the Internet.	
C Use a procy perver to access the Internet	
Other Options # Adamatically detect procy server settings	
The te tokenopping dever to access the intervent:	
Verv approvality Address. Noti get	
Sec options	
Marker server Unit: Piperiord eseases	
E allo-date autostratos shen canactag to programme	
200 Alter and Markan Markan Andreas	
La wood of tweet operation to a second	
Difference in the second	
In Internet Security P your clerks cannot receive a RedBIOS name (computername) you should change the to a CRE name (computername do	nairvane) or use the server's IP address.
Select which server to wynchronize centers! Trees:	
C: Synchronize from a local Software Update Services servers	
Type-the name of the sarver. Example: CopVUs.	
Synchronical list of approved barne updated from this location (values mode)	
Select hew you want to handle new versions of previously approved updates:	
C: Do not automatically approve new versions of approved updates. I will manually approve these updates later.	
Select where you want to store updates:	
C. Haintain the updates on a Picrosoft Windows Update server	nnsessa -
1.6° Saves the undates to a local follow	94449644 -
	HEDY
need mananet companies are specificationed. <u>Territ of site</u>	Lakales Talaani
i në ng	1 1 1 2 manual surgery
dmincharflächa das CLIC Comusia	

Data Barbeton gradat Services File	nsoft Internet Balarier 10 - 1		3	#×
🔾 žalick + 🕐 - 💽 👔 🐔 🔎 Suzben	👷 Favorten 🔮 Heden 🕑 🔝 - 😓 🗔		T Vietneb re	Links 24
Software Updat	te Services		levin 1.	3630,7557
Selfware Update Services	Set options Set root Software Update Services splices, and then disk Apply.			
Synchrwisse server	Synchronics list of approved issue updated from this location ()	replace mode)		*
Other Options	Select here you want to handle new versions of providently ap 6 Automaticaly approve new versions of provided approved update C. Denot automatically approve new versions of approved updates. 3	pproved apdates: es 1 wil manually approve these updates later.		
Herrisprondiky Set option Marker server	Scient where you want to stare updates: C Maintain the updates on a Pikrosoft Windows Update corver C for the updates on a Pikrosoft Windows Update corver			
The star	(e) save the updated to a local today lightforman installation packages only for these locales:		Select All Cear Al	
Abeut Software Update Services	E Andric	🗖 Dalar		
Recent Windows Lipidae	Andric enabled Conversional	D Japanese		
Merceaft Security	Chinese Sangared	 Japanese MEC Ensure 		
Contraction of the second seco	E Gash	Nerwegien		
	E Darish	E Poluh		
	E Datch	Portuguese (Brazilian)		
	E English	Portuguese (Skandard)		
	E Firmin	E Rumlan		
	E Frinds	C Souk		
	E Guel	E Sovenen		
	C Greek 1891	E Secto		
	E History	The ended		
	Hebrew enabled	E Turkih		
	E Hargarian		コロップっとっこ	1.1
				P4
@ 2002 Missarett Corporation, All rights ren	rood. Terrar of ann. Amerididite.			
2			Lukales Intranet	
Adminoberfläc	he des SUS-Servers	3		

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":

Microsoft Software Update Services - M	ensel Islenet Bykein
tai Bearboiton graicht Bavariton Ba	
anax • () - 💽 🙎 😭 J. Suite	Privaten @ Peden @ [] - 13 []
elle El atr/locacitational	S S Assessed in
Software Linds	te Services
Software opus	Ite Oct YICeS
Software Update Services	Synchronize server
D.u.	tair eicheantair (mai)
	two constructions (particle) is characterized and construction with the following tradition features consist, or manually exceptions was assure at an time.
	Sara for water Name Sara for the water Name Sara Sara Sara Sara Sara Sara Sara Sar
	All the many states and states an
Other Options	
 Yes synchronization log 	
Vev approvaling	
Set options	
Maritar server	
See Also	
About Software Update Services	
Monosoft Windows Lipidate	
Merceoft Security	
🖸 Microsoft Support Encodedge Base	
	A
	111525551
	112701112511
000 Mixeraft Corporation. All rights re	terret Jerre d'une Ameridiste.
etig	Lakako Intsonet
مريحة والمعالم	
aminobert	lache 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".

Schedule Synchronization	Webseitendia	log 🔀
 Do not synchronize on a set Synchronize using this sch At this time: 03:00 - 	chedule edule:	
On the following day(s):		
C Daily		
Weekly		
🔘 Sunday	🔿 Monday	🔿 Tuesday
🖲 [Wednesday]	🔘 Thursday	🔿 Friday
🔿 Saturday		
Number of synchronization	n retries to attempt	on a scheduled synchronized
	C	K (U)//Ganbaly
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.

Dennis Schwere Haddle Services H	kennel bidenet fojkerer
Adregee (1) http://localhost/liusiAdway/	🗴 🖉 Petersen i 🖉 Vectorien sa Linka *
Software Upda	tte Services
Software Syndotic Services Software Syndote Services Software source Approve updates Other Options	Synchronizo server Med ophimization Mitteeld, SK. Issues 7885 832668 Tracin down to at activities you error to annually ophimize with the Schwarzipdes Service on eacually ophimize you error at any time. Strategies have: Schwarzipdes Service
Yeev synchronizatien leg Hev approvaling Set options Meriter server	Bernholm quotate from the Photosoft Walance Update server Borelanding pandage P of 2016 (1,4-10), NHL complete Canadian Scarry (Labolan to Scarro Labolance G. Ser (Labolance G) Canadian Scarry (Labolance To Scarro Labolance G)
See Also About Software Update Services Microsoft Windows Update Microsoft Security Microsoft Security	Tela Pognes (PK cospile)
6. 2003 Micourth Americana Mildolm	切ねつきみ
e Perto	Lakelo Internet
Synchroni	sieren 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):

In PDF konvertiert von Lukas Läderach



	com_microsoft.9867801_IE501_SP3,10:00:00:2005-01-23T16:32:03
	com nicrosoft. 0867801 [E301_314,16:06:06:05-01-23116:32:03
	com_microsoft.9867801_IE6_SP1.10/00/00/2005-01-23T16:32:03
	com_microsoft.Q889293_IE6_SP1_updateexe,10 00 10 2005-02-13T10:52:06
	com_nicrosoft.Q900036_US_NET_ES_5520,10:00:00:2005-01-23T16:32:03
	com_nicrosoft.Q900036_VS_NET_ES_SDK_5521,10\00\00\2005-01-23T16:32:03
	com_nicrosoft.Sasser_A_B_Cln,10:00:00:2005-01-23T16:32:03
	com_nicrosoft.SB\$2003_KB832880_40598,10:00:2005-01-23I16:32:03
	com_nicrosoft.SB\$2003_KB872769_40850,1010012005-01-23T16:32:03
	com_nicrosoft.W2kSKP_Full_Corp_S189,10:00:00:00:2005-01-23116:32:03
	com_nicrosoft.Windows 2000 Service Pack 4 Network Install for II Professionals,1
	EIDEIDE(2003-01-23110-32-03)
	c_{00} (1) c_{20} (1) $c_{$
	c_{00} nicrosoft vn sn 2 Hongkong 101301001201521632183
	com nicrosoft XP SP1 5446 10 100 100 12005-01-23116:32:03
	13.02.2005 11:57:36: File updated
	C:\SUSAutoApprove\autoapproveupdates.vbs(195, 3) CDO.Message.1: Der "SendUsing"-
	Konfigurationswert ist ungültig.
	WHITTER STORE ST
1	
	G-NS0SHILLON J070067
ſ	Approve über ein Script
4	

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:

Eigenschaften von Automatische Updates konfigurieren 🔋 🔀
Einstellung Erklärung
Automatische Updates konfigurieren
Nicht <u>k</u> onfiguriert Aktiviert
© Deaktiviert
Automatische Updates konfigurieren:
4 - Autom. Downloaden und laut Zeitplan 💌
Folgende Einstellungen sind nur erforderlich und gelten nur, wenn 4 gewählt wird.
Geplanter Installationstag: 0 - Täglich
Geplante Installationszeit: 12:00
I I
Unterstützt auf: Windows Server 2003-Produktfamilie, XP SP1, 2000 S
<u>V</u> orherige Einstellung <u>Nächste Einstellung</u> <i>∭hifotai</i>
OK Abbrechen Übernehmen
Einstellungen der Gruppenrichtlinie

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.

In PDF konvertiert von Lukas Läderach

Eigenschaften von Internen Pfad für den Microsoft Updatedien?
Einstellung Erklärung
😭 Internen Pfad für den Microsoft Updatedienst angeben
Nicht <u>k</u> onfiguriert
<u>Aktiviert</u>
C <u>D</u> eaktiviert
Interner Updatedienst zum Ermitteln von Updates:
http://testserver
Intranetserver für die Statistiken:
http://testserver
(Beispiel: http://IntranetUpd01)
J Unterstützt auf: Windows Server 2003-Produktfamilie, XP SP1, 2000 S
Vorherige Einstellung Nächste Einstellung ∭hir∂tai
OK Abbrechen Obernehmen
Einstellungen der Gruppenrichtlinie

Der nächste Konfigurations-Dialog sieht dann so aus:

Eigenschaften von Geplante Installationen automatischer Up 🔶 🗙
Einstellung Erklärung
Geplante Installationen automatischer Updates erneut planen
Nicht <u>k</u> onfiguriert Aktiviert
O Deaktiviert
Nach dem Systemstart warten (Minuten).
Unterstützt auf: Windows Server 2003-Produktfamilie, XP SP1, 2000 S
Vorherige Einstellung Nächste Einstellung ∭hirfoRei
OK Abbrechen Obernehmen
Einstellungen der Gruppenrichtlinie

Und der vierte und letzte dann so:

Eigenschaften von Kein automatischer Neustart für geplante I 🎴 🗙
Einstellung Erklärung
🛱 Kein automatischer Neustart für geplante Installationen automatischer
 ○ Nicht <u>k</u>onfiguriert ○ <u>Aktiviert</u> ○ <u>D</u>eaktiviert
Unterstützt auf: Windows Server 2003-Produktfamilie, XP SP1, 2000 S
Vorherige Einstellung Nächste Einstellung
OK Abbrechen Obernehmen
Einstellungen der Gruppenrichtlinie

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:

S Group Policy Management					
3월 Datei Aktjon Ansicht Beneter 2			그리지		
← → 🗈 🗉 🖦 🖻 🗙 🕄 😫					
Group Policy Management	SUSUpdates				
E-B Donanen	Bereich Details Einstellungen Delegierung				
🗄 🤯 nydonain local	Folgende Gruppen und Benutzer haben die angegebene Berechtigung für dieses Gruppenrichtlinienobjekt				
Default Donain Policy	Bruppen und Benutzer:				
- M Ordnerunleitung	Name -	Zulässige Berechtigungen	Beebt		
B Domain Controllers	Authentifizierte Benutzer	Lesen (durch Sicherheitslitterung)	Nein		
🗄 🤤 Gruppervichtlinienabjekte	Domanen-Admint MYDDMAIN/Domanen-Ad	Einstellungen bearbeiten / Loschen / Sicherheit verändern	Nein		
Default Domain Controllers Policy	COMAKENLON TRULLER DER UNBANISAT.	Einstellungen bescheiten / Löschen / Sicherheit verändern	Nen		
- St Loginskript	C SYSTEM	Einstellungen bearbeiten / Löschen / Sicherheit verändern	Nein		
Conteruntetung Conteruntetung Software Software Software Software Conteruntetung Software Software					
		ปปกาอโอโ			
	Hinzufügen. Entfernen	Eisenscheiter Ei	weitert.		
GPO für Domänen-Ad	lmins übernehmen				

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".

cherheitseinstellungen für SUSUpdates 🛛 🔀						
Sicherheit						
Gruppen- oder Benutzernamen:						
🕵 Authentifizierte Benutzer						
Domänen-Admins (MYDOMAIN\Domänen-Admins)						
OMÄNENCONTROLLER DER ORGANISATION						
I ERSTELLER-BESITZER						
Crasniestions.Admine_IMYDOMAIN\Drasniestions.Admine}						
<u>H</u> inzufügen <u>E</u> ntfernen						
Berechtigungen für Domänen-Admins Zulassen Verweigern						
Vollzugriff 🛛 🗖 📥						
Lesen 🗹 🗖						
Schreiben						
Alle untergeordneten Objekte erstellen 🗹 🔲						
Alle untergeordneten Ubjekte loschen 🗹 🔲 🔤						
Klicken Sie auf "Erweitert", um spezielle Berechtigungen oder erweiterte Einstellungen Erweitert						
anzuzeigen.						
OK Abbrechen Übernehmen						
PO 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 <u>http://www.susserver.com</u> 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 <u>Patches</u> 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 Diensteverwaltung 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\ HKEY_LOCAL_MACHINE\ SOFTWARE\ WindowsUpdate sowie 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://)

In PDF konvertiert von l	Lukas	Läderach
--------------------------	-------	----------

💰 Registrierungs-Editor						
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>F</u> avoriten <u>?</u>						
🕀 💼 SystemCertificates	•	Name	Тур	Wert		
🖻 💼 Windows		(Standard)	REG_SZ	(Wert nicht gesetzt)		
📄 Installer		MUServer 🛃	REG_SZ	http://MITTELERDE		
⊡ IPSec		(WUStatusServer	REG_SZ	http://MITTELERDE		
🕀 🛄 NetCache						
terne windows NT						
WindowsFirewall WindowsFirewall Program Croups						
Program Groups						
	_					
	τl.		1.1.14	J		
	_	•	Uup	i Jessei 🕨 🕨		
Arbeitsplatz\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate						

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

```
"NoAutoRebootWithLoggedOnUsers"=1
"NoAutoUpdate"=0
"AUOptions"=4
"ScheduledInstallDay"=0
"ScheduledInstallTime"=b
"RescheduleWaitTime"=5
"UseWUServer"=1
```

In PDF konvertiert von Lukas Läderach

💰 Registrierungs-Editor						
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>F</u> avoriten <u>?</u>						
Generation	Name (Standard) NAUOptions NoAutoRebootWi NoAutoUpdate CheduleWaitT ScheduledInstall	Typ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Wert (Wert nicht gesetzt) 0x00000004 (4) 0x00000001 (1) 0x00000000 (0) 0x00000005 (5) 0x00000000 (0) 0x00000000 (0) 0x00000000 (0)			
			0x00000001 (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 <u>Susserver.com</u> und bei Microsoft im SUS Deployment Guide

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