Dr. Suppan International Institute

# Der Netzwerk Insider

März 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

# Windows (.NET-)Server 2003 warten oder starten?

**von Markus Holländer**

**Für viele Unternehmen stellt sich die Frage, ob sie zu Windows Server 2003, dies ist die neueste Namenskreation aus dem Hause Microsoft, oder auch zu dem besser bekannten Windows .NET-Server 2003 migrieren sollen bzw. müssen.**

Aktuell zeichnet sich eine sehr leichte Erholung am IT-Markt-Horizont ab, zumindest sollen die IT-Budgets langsam wieder aufgestockt werden. Ob dies auch Auswirkungen auf das bereits laufende Jahr hat, bleibt abzuwarten.

Bei den Recherchen zu diesem Artikel fiel mir ein neuer Begriff ins Auge, der die aktuelle Lage gut skizziert: PONI = Price Of Non Investment. In der heutigen Zeit ist also der Preis für eine Nichtinvestition interessanter als der ROI = Return of Investment? Dies kann man im Allgemeinen sicher nicht sagen, doch werden Investitionen zumindest so manches Mal hinausgezögert. Vielleicht liegt es aber auch an den ROI-Beispielberechnungen, die Microsoft zum Thema Windows XP und Office XP zur Verfügung stellt.


Investment oder Non Investment – das ist hier die Frage

Ein gutes Beispiel für ein PONI-Konzept war die Wall Street. Diese hatte nicht in ein Archivierungssystem für Emails investiert und muss jetzt neben der Investition dafür auch noch 8,25 Mio $ Strafe zahlen*. Immerhin sind so namhafte Unternehmen wie die Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney und Piper Jaffrey betroffen.

Genau diese Thematik betrifft auch die Windows Server Welt.

Dieser Artikel beschäftigt sich zum einen mit der Thematik, welche Neuerungen und Veränderungen bei den elementaren Diensten im IP-Umfeld und insbesondere im Active Directory mit Windows Server 2003 auf die Administratoren zukommen und zum anderen werden auf Basis dieser Informationen Anhaltspunkte geliefert, wer migrieren sollte – immer unter dem Gesichtspunkt ob derzeit NT oder W2K eingesetzt wird.

Für Windows NT 4.0 (Enterprise) Server endet die letzte Supportphase, der von Microsoft genannte "Extended Support", am 31.12.2004 (dieser Zeitpunkt wurde während der Artikelerstellung von Microsoft um 1 Jahr nach hinten verschoben), für Windows 2000 (Advanced) Server endet diese Phase am 31.03.2007*.

weiter Seite 6

* Quelle: Time to PONI up von Frank Hayes in der Computerworld, 09.12.02, http://www.computerworld.com/managementtopics/roi/story/0,10801,76504,00.html

** siehe: http://support.microsoft.com/default.aspx?scid=fh;en-us;lifewin

ComConsult feiert das Jubiläum der Ausbildung zum ComConsult Certified Network Engineer

# CCNE wird 5 Jahre alt!

**Seit Beginn der Ausbildung und Zertifizierung zum CCNE haben mehrere Tausend Teilnehmer die zugehörigen Kurse durchlaufen. Das Zertifikat des ComConsult Certified Network Engineers ist damit die in Deutschland dominierende herstellerneutrale Zertifizierung. Die Liste der Unternehmen, die ihre Mitarbeiter/Innen zertifizieren lassen, belegt eindrucksvoll den Grad der Akzeptanz in der Branche.**

Grundsätzlich bietet dabei die Ausbildung und Zertifizierung folgende Vorteile:

- systematische Aus- und Weiterbildung nach dem modernsten Stand der Technik
- strenge und herstellerneutrale Orientierung an der Praxis mit optimaler Verwertbarkeit des Erlernten im Tagesbetrieb
- formaler Nachweis der bestehenden Kenntnisse, besonders wichtig in einem enger werdenden Markt, der zunehmend Qualifikations-Nachweise erfordert

Wir finden, dass dieser Erfolg gefeiert werden muss! Deshalb ist bis zum 30.06.03 ein HP 5450 oder wahlweise ein Sony Clie NX70V Bestandteil des Ausbildungspakets. Diese Geräte erlauben es gleichzeitig durch die potenzielle Integration in Bluetooth und Wireless-Netzwerke sowie die Einbindung in Unternehmensmail und Informationsdienste einen Teil des gelernten praktisch umzusetzen. Mit der von uns für diese Geräte bereitgestellten Schlagwortliste sind sie zudem immer in der Lage, wichtige Begriffe und Abkürzungen der Kommunikationstechnik nachzuschlagen.

Wie in jedem Jahr haben wir auch diesmal die Kurse mit Beginn des Jahren an den neuesten Stand der Technik angepasst.

Feiern Sie mit uns! Werden Sie ComConsult Certified Network Engineer!

Ihr Dr. Jürgen Suppan

Zum Geleit

# Der PDA, das unbekannte Risiko

Nicht ohne Hintergedanken haben wir zwei hochmoderne PDAs zum CCNE-Jubiläum zum Teil des Ausbildungspakets gemacht.

Technik und Leistung der aktuellen PDA-Generation haben sich doch gegenüber den ersten Palms aus der Frühzeit der PDAs deutlich verändert. Dabei spielt es eigentlich kaum eine Rolle, ob wir Pocket-PC oder PalmOS als Basis nehmen.

Eine der wesentlichen Änderungen ist die zunehmende Offenheit der Plattform und die leichte Integration von Applikationen.

Ohne Zweifel ist speziell dieses Feature durch den Eintritt von Microsoft noch gefördert worden. Auch Symbian als Basis für moderne Softphones hat sich in ähnlicher Weise entwickelt. Dort gestattet speziell die Java Microedition das individuelle Nachladen spezieller Applikationen (siehe als Beispiel Nokia 6310, 7650 oder Sony Ericsson P800).

Parallel hat sich das Leistungsvermögen beachtlich entwickelt. Schnelle Prozessoren (XScala als Beispiel), ein immer größerer Speicher (64 MB), ein akzeptables Farbdisplay und flexible Architekturen (siehe speziell das Modulkonzept des Compaq/HP iPAQ 39xx und 54xx) verschaffen dem PDA die Eignung, für beliebigste Anwendungen eingesetzt werden zu können. Der größte Handlungsbedarf besteht ohne Frage im Bereich des integrierten Wechselspeichers, hier sollte der Gigabyte-Bereich im Laufe des Jahres in Form eines handelsüblichen und herstellerunabhängigen (also kein Memory-Stick) Mediums hoffentlich fallen.

Wer sich einen Überblick über den Stand der Entwicklung verschaffen will, der sehe sich die Applikationsliste auf dem Microsoft-Server (www.pocketpc.com) an, die neben den üblichen Spielereien auch finanzwirtschaftliche Programme oder spezielle Applikationen wie den MindManager umfasst (als Fotoamateur gefällt mir auch ACDsee in der Mobile-Version).

Der eigentliche Sprung, der aus einem PDA ein universelles Endgerät macht, ist aber ohne Zweifel die Integration in die Kommunikationsnetze eines Unternehmens. HP hat es mit dem iPAQ 5450 vorgemacht, der sowohl Bluetooth als auch Wireless LAN nach IEEE 802.11b eingebaut hat. Spätestens mit der nächsten Chipgeneration (siehe Intel Centrino, Auslieferungsbeginn voraussichtlich April) wird die Netzwerkintegration Standard für die PDAs werden. Damit nicht genug. Der moderne PDA beinhaltet einen VPN-Clienten, einen Windows-ICA-Terminal-Agenten sowie einen Windows XP Terminal-Clienten.

So weit so gut. Wer aber einmal versucht hat, ein Backup von einem PDA zu ziehen (speziell unter PocketPC, Aufwand ewig) oder wer einmal mit der Netzwerk-Integration zu kämpfen hatte (warum darf man beim 5450 die IP-Adresse des Mail-Servers nicht angeben sondern nur den Namen??), dem wird deutlich werden, dass in der zu befürchtenden Ausbreitung der PDAs ein ernstzunehmender Betriebsaufwand liegt.

Die Integration der diversen Terminal-Clienten sowie die zunehmende Verfügbarkeit von Analyse-Software (siehe Sniffer Wireless) unterstreichen auch, dass hier ein zu beachtendes Sicherheitsthema liegt.

Noch ist unklar, welche Applikationen in Zukunft alles auf der universellen Plattform PDA angeboten werden. Ebenso ist unklar, ob diese Applikationen einen Mehrwert beinhalten. Erste Untersuchungen haben aber gezeigt, dass sich das Kommunikationsverhalten von Personen in Kombination mit einem netzwerktechnisch integrierten PDA im positiven Sinne entwickelt hat (siehe Testinformationen unter ZDnet und Heise).

Mein persönliches Fazit ist, dass die weitere PDA-Entwicklung unbedingt sorgfältig beobachtet werden muss. Mit der Bereitstellung von Centrino und der Chipintegration der Funknetze wird es noch einmal einen Schub geben. Der Einstieg in die Betriebskonzepts-Diskussion und das Thema Desktop-Management sollte nicht zu weit in die Zukunft geschoben werden.

Wie man sieht, ist die Einbeziehung moderner PDAs in unser CCNE-Jubiläumspaket nicht nur eine Spielerei, sie hat einen ernsten Hintergedanken.

In diesem Sinne,
Ihr Dr. Jürgen Suppan

## Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos als PDF-Datei
über den eMail- VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

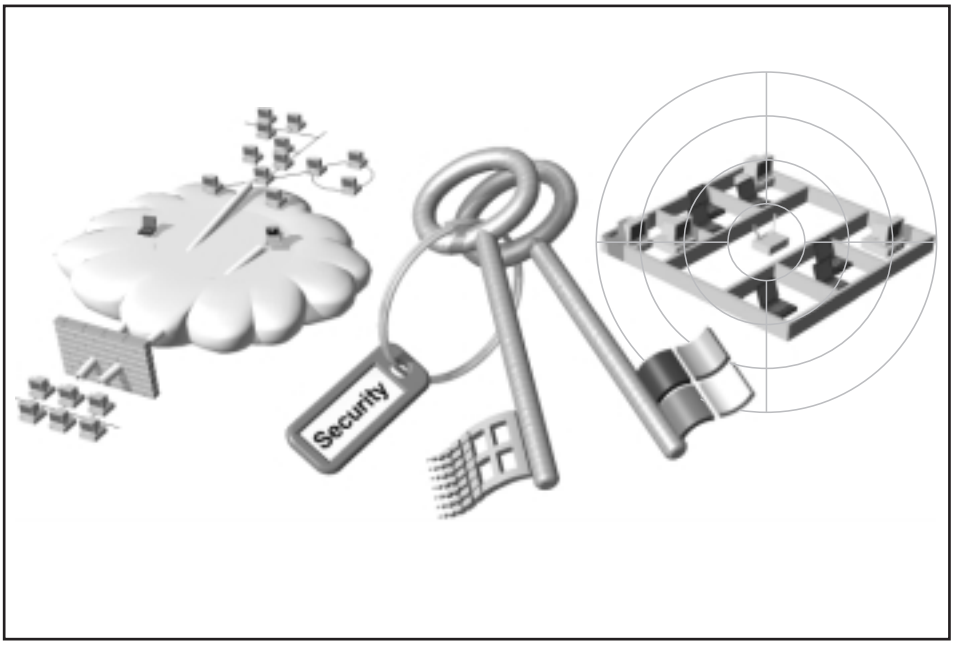
ComConsult Research

# Das Research-Paket: Sonderveranstaltung und Reports Windows Security, Virtual Private Network und Wireless LAN Sicherheit

**ComConsult Research hat eine tiefgehende Untersuchung der Sicherheit in Windows Betriebssystemen durchgeführt. Die Fragestellungen sind:**

- **Welche Sicherheits-Mechanismen sind in Windows NT und Windows 2000 enthalten?**
- **Wie kann eine Windows-Installation gehärtet werden?**
- **Welche Potenziale beinhalten EFS, IPsec und PKI?**
- **Welche Gefahren beinhaltet der Browser-Betrieb und welche Möglichkeiten gibt es, diese zu reduzieren?**

**Aufgrund der hohen Brisanz des Themas präsentiert die ComConsult Akademie die Ergebnisse unter Einbeziehung der Themenbereiche VPN und Wireless Security als Sonderveranstaltung "Windows-Security: Clienten-Sicherheit effizient und erfolgreich realisieren" vom 31. März bis 1. April 2003 im Park Plaza in Köln.**




## Zum Thema

Der Netzwerk-Client, typischerweise ein PC mit Windows-Betriebssystem, entwickelt sich immer mehr einerseits zum Haupt-Sicherheitsrisiko der gesamten IT-Infrastruktur und dementsprechend andererseits zum bevorzugten Angriffsziel.

Nachdem wir heute in der Lage sind, einen direkten Angriff auf Server und Daten von Außen wirkungsvoll und massiv zu erschweren, gehen immer mehr Angriffe den Umweg über die Clienten.

Dies hat zwei dominierende Ursachen:

- Arbeitsplatz-PCs browsen im Internet, führen Skripte aus, laden Daten von Außen nach Innen und bieten somit eine Reihe von nur schwer abzusichernden Angriffflächen.
- Hat ein Angreifer einen PC übernommen, kann er unter Nutzung dessen Rechte sich frei im Unternehmen bewegen und den Angriff auf Server und Daten oder noch schlimmer andere externe Systeme starten.

Die Absicherung der auf Windows 2000 und NT basierenden PCs ist damit die zentrale herausragende Aufgabe jedes aktuellen Sicherheits-Konzeptes. Dabei gestatten sowohl die in Windows vorhandenen Bordmittel als auch die erheblichen Möglichkeiten einer sicherheitssensitiven Konfiguration eine massive Reduzierung der Gefahrenlage.

Dabei muss gerade das Thema Windows Security im direkten und untrennbaren Zusammenhang mit zwei weiteren Themen gesehen werden: der Planung und Umsetzung von VPN-Lösungen und Wireless Security

Das hat folgende Gründe:

- Speziell in der Kommunikation über unsichere Netzwerke hinweg (Internet, Wireless) ist VPN-Technologie momentan die wichtigste Sicherheitstechnik. Auch im lokalen Anwendungsbereich breiten sich die VPN-Lösungen geradezu explosionsartig aus
- Im Bereich Wireless werden speziell Notebooks mit sensiblen Daten oder mit Zugang zu wichtigen Firmendaten immer mehr zentraler Gegenstand einer Sicherheits-Lösung. Hier ist aber bis 2004 mit einer 95%-igen Integration von Funknetzen zu rechnen, die wiederum extrem sicherheitskritisch sind. Auch der gesamte Bereich der Hot-Spot-Technologien muss dabei mit äußerster Vorsicht betrachtet werden, beinhalten Hot-Spots auf Funkbasis doch massive Sicherheits-Probleme für Notebooks und PDAs.

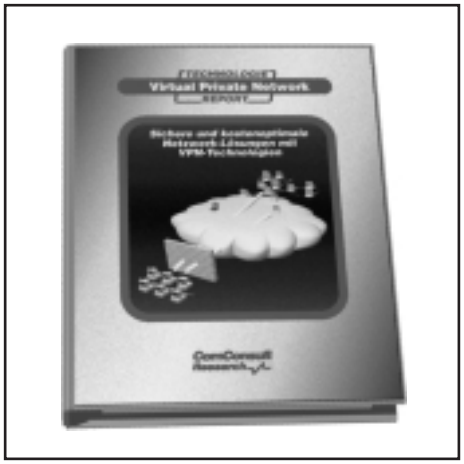
Windows Security, Virtual Private Network und Wireless LAN Sicherheit

**Der neueste Report der Research-Reihe:**

**Windows Security-Report "Sicherheit in Windows-Systemen"**

- Welche Sicherheits-Mechanismen beinhalten Windows NT und Windows 2000?
- Wie können Windows-Clienten-Installationen gehärtet werden?
- Welche Dienste sind kritisch, welche können, welche sollten deaktiviert werden?
- Welche Möglichkeiten bietet der EFS-Dienst zur Verschlüsselung von Dateien und Ordnern, wie kann mit den Einschränkungen dieses Dienstes umgegangen werden?
- Was bieten IPsec, PKI und Zertifikate?
- Wie kann der Windows Explorer gesichert werden?

Einzelpreis 298,--



**Virtual Private Network-Report "Sichere und kostenoptimale Netzwerk-Lösungen mit VPN-Technologien"**

- Wie Sie kostenoptimale Remote-Access-Lösungen aufbauen können
- Wie Sie typische und gravierende Sicherheitsmängel im Betrieb von Notebooks und im Netzzugang von Führungskräften beseitigen können
- Wie Sie durch gezielten Einsatz von VPN-Technologien intern und extern eine hohe Sicherheit für Personendaten, für kritische Anwendungen und im medizinischen Bereich erreichen können
- Wie Sie auch in unsicheren Umgebungen und bei Nutzung des Internets optimale Sicherheit erreichen
- Wie Sie Lösungen aufbauen, die nicht nur technisch gut sind, sondern auch wirtschaftlich und betriebs-optimal

Einzelpreis 349,--

**Wireless LAN Sicherheits-Report "Sicherheit in Wireless LANs"**

- Was bedeutet eigentlich Session-Hijacking?
- Mit welchem Aufwand können verschlüsselte WLANs abgehört werden?
- Soll WEP-Verschlüsselung eigentlich eingesetzt werden oder besser nicht?
- Was verstehen Hersteller unter "Closed System"?
- Welche weiteren Lösungsansätze stehen zur Verfügung?
- Wie werden sich Funknetze in der Zukunft weiterentwickeln?
- Welche grundlegenden Design-Entscheidungen müssen Sie bereits heute berücksichtigen, um auf die neue WLAN-Generation umsteigen zu können? Worauf sollten Sie bei kurzfristigen Investitionsentscheidungen achten?

Einzelpreis 298,--

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung Sonderveranstaltung

Ich buche die Sonderveranstaltung
**Windows-Security: Clienten-Sicherheit effizient und erfolgreich realisieren**

☐ als Paket mit den drei Reports
**Windows-Security**
**Virtual Private Network**
**Wireless LAN Sicherheit**
zum Preis von € 2.248,-- zzgl. MwSt.

☐ mit dem Report **Windows-Security**
zum Preis von € 1.980,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Hotelzimmer

Buchen Sie über unsere Website:
**www.comconsult-akademie.de**

Vorname _____ Nachname _____

Firma _____ Abteilung _____

Position _____ PLZ, Ort _____

Straße _____ eMail _____

Telefon, Fax _____ Unterschrift _____

**Fortsetzung von Seite 1**

### DNS für das Active Directory von Windows (.NET-)Server 2003

Auch in der neuen Version des Active Directory (Version 2) des Windows Server 2003 ist DNS die entscheidende Basis hinsichtlich Namesauflösung und Dienstidentifizierung. Es muss weiterhin definiert werden, dass ohne eine DNS-Infrastruktur kein Active Directory implementiert werden kann. Im gleichen Atemzug muss allerdings auch festgestellt werden, dass es wohl im Microsoft-Umfeld noch nicht der Fall ist, dass vollständig auf die NetBIOS-Namensauflösung (z.B. WINS, lmhosts) verzichtet werden kann, insbesondere hinsichtlich Applikationen und auch für Migrationen. Isoliert man die Betrachtung auf das Active Directory, dann wird tatsächlich keine NetBIOS-Namensauflösung benötigt. Dies geht jedoch in den meisten Fällen an der Realität vorbei. Fest steht auch, dass der große Schritt von Windows NT in Richtung Windows 2000 gemacht wurde bzw. wird, oder in Richtung Windows Server 2003 gemacht wird. Ein verhältnismäßig kleiner Schritt im Umfeld der Namensauflösung - insbesondere bei DNS - ist die Migration von Windows 2000 nach Windows Server 2003, da die elementaren Aspekte gleich geblieben sind.

Allerdings ist es auch weiterhin so, dass Designentscheidungen, die am Anfang eines Projektes bzw. auch am Anfang der Implementierung getroffen bzw. umgesetzt werden, nur mit sehr hohem Aufwand, nämlich mit der Neuimplementierung des Active Directory, rückgängig gemacht werden können. Das beste Beispiel dafür ist der dcpromo-Prozess, bei dem die Domänenstruktur im Active Directory festgelegt wird. Eine Betrachtung dieser Thematik erfolgt später in diesem Artikel. Aber bevor es zur Installation des Active Directory kommt, muss, wie bereits gesagt, die DNS-Infrastruktur geschaffen werden.

Ein sehr wichtiger Punkt, der vor jeder Konfiguration gemacht werden muss, ist die Definition des primären DNS-Suffixes des Servers selber. Dies wird sehr häufig vergessen und führt dadurch zu Fehlkonfigurationen. Unter den Eigenschaften des Arbeitsplatzes auf der Karteikarte Computernamen muss man den Button ändern wählen, so dass man den Computernamen definieren kann und mit einem Klick auf dem Button Weitere gelangt man dann in das Fenster zur Konfiguration des primären DNS-Suffixes (siehe auch Bild 1: Primäres DNS-Suffix festlegen).

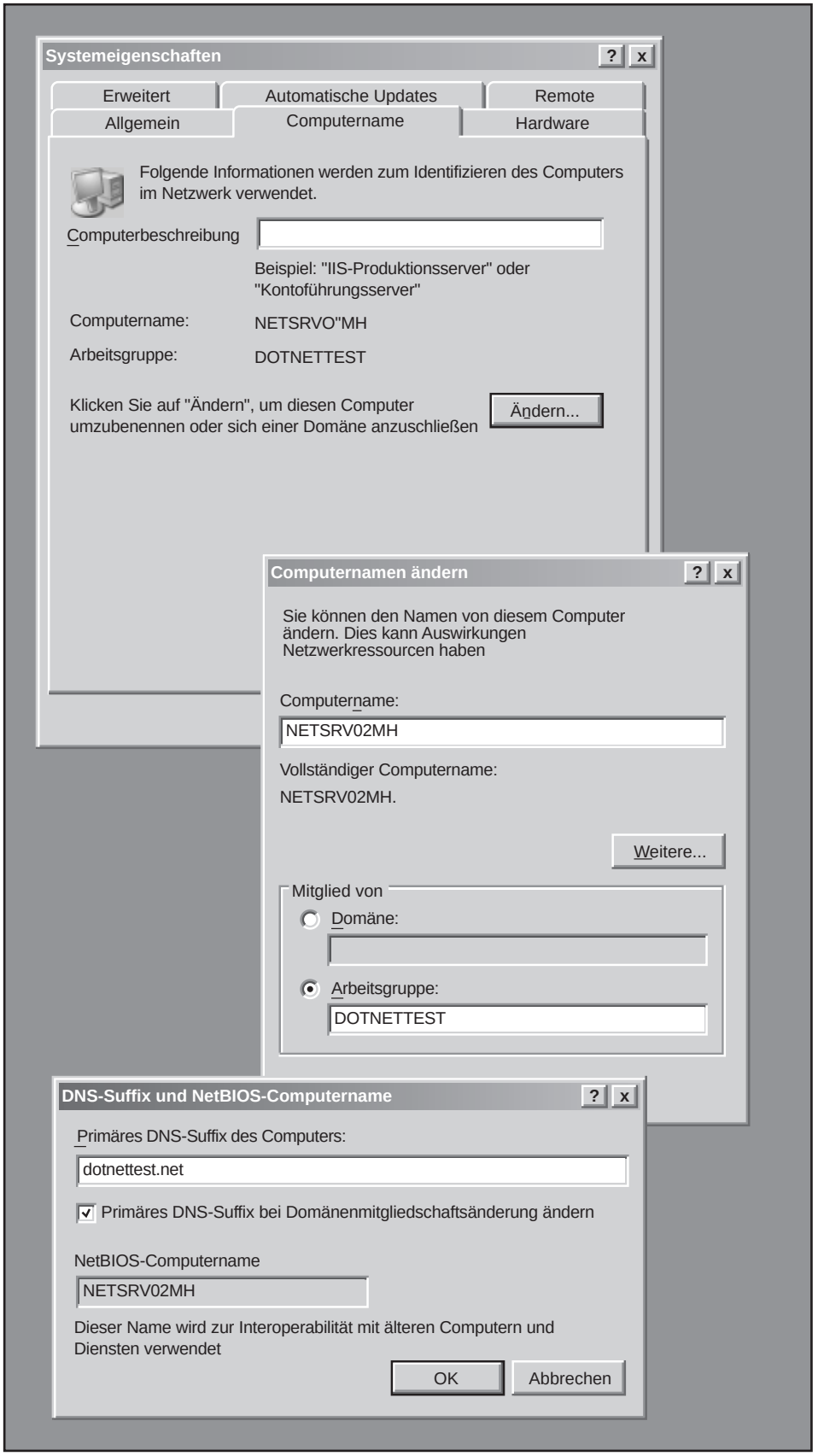
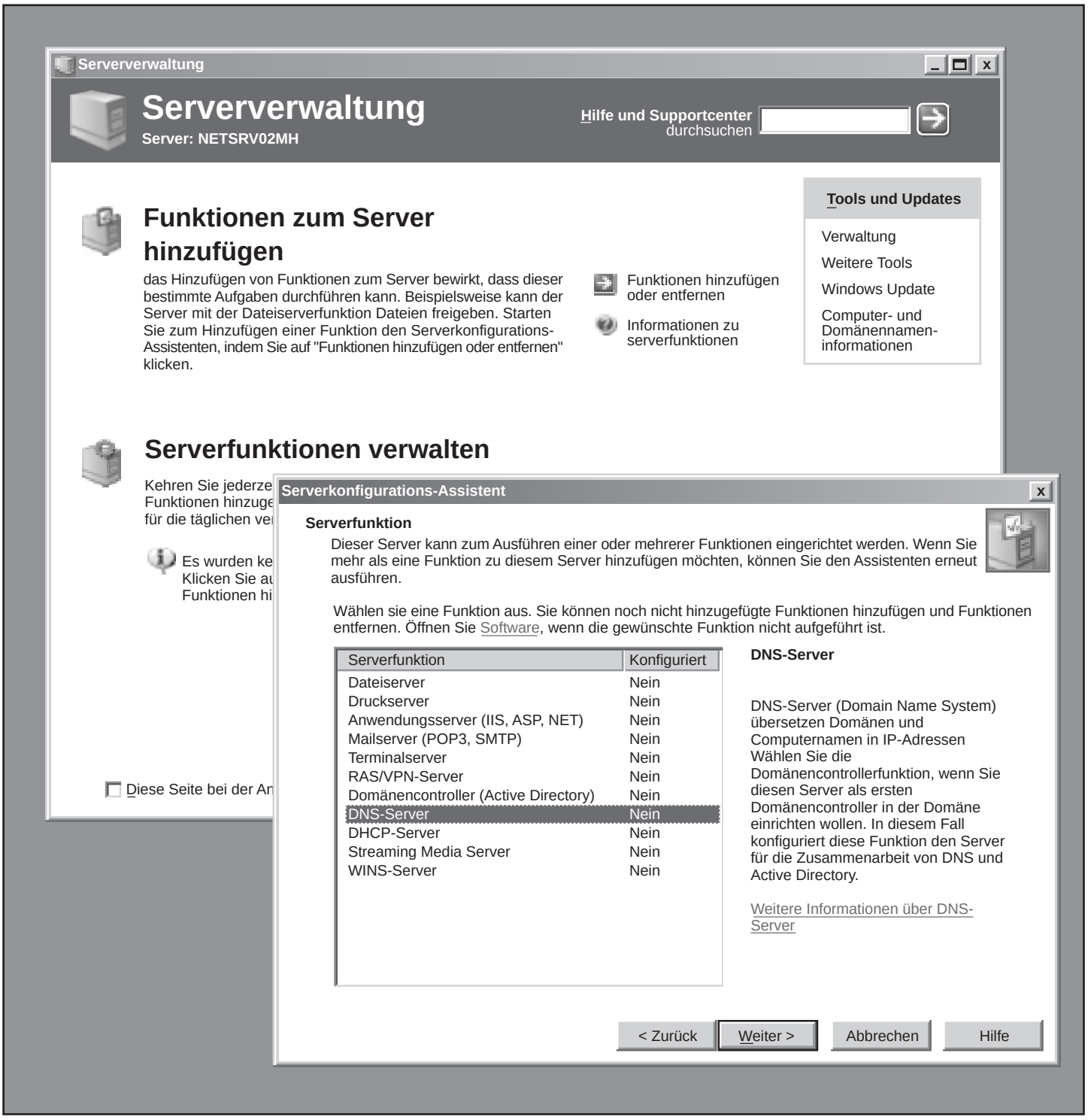



Bild 1 Primäres DNS-Suffix festlegen

Hat man diese grundlegende Konfiguration des DNS-Suffix abgeschlossen und der Server besitzt auch eine entsprechende IP-Konfiguration kann mit der Installation und Konfiguration des DNS-Servers begonnen werden. Hierzu liefert Windows (.NET-)Server 2003 einen Wizard, der es auch unerfahrenen Administratoren erlaubt, den Server zu konfigurieren. Der Wizard zur Serververwaltung, wie ihn Microsoft genannt hat, ermöglicht unter anderem auch die Konfiguration des DNS-Servers. Nach Start des Wizard (Start/Alle Programme/Verwaltung/Serververwaltung) kann man Funktionen hinzufügen oder entfernen, hierzu zählt dann auch DNS. Nach einigen Fenstern gelangt man in das Auswahlfenster wo Serverfunktionen, die konfiguriert werden sollen, ausgewählt werden können (siehe Bild 2: Serververwaltung – Serverkonfigurationsassistent).

Bild 2 Serververwaltung – Serverkonfigurationsassistent



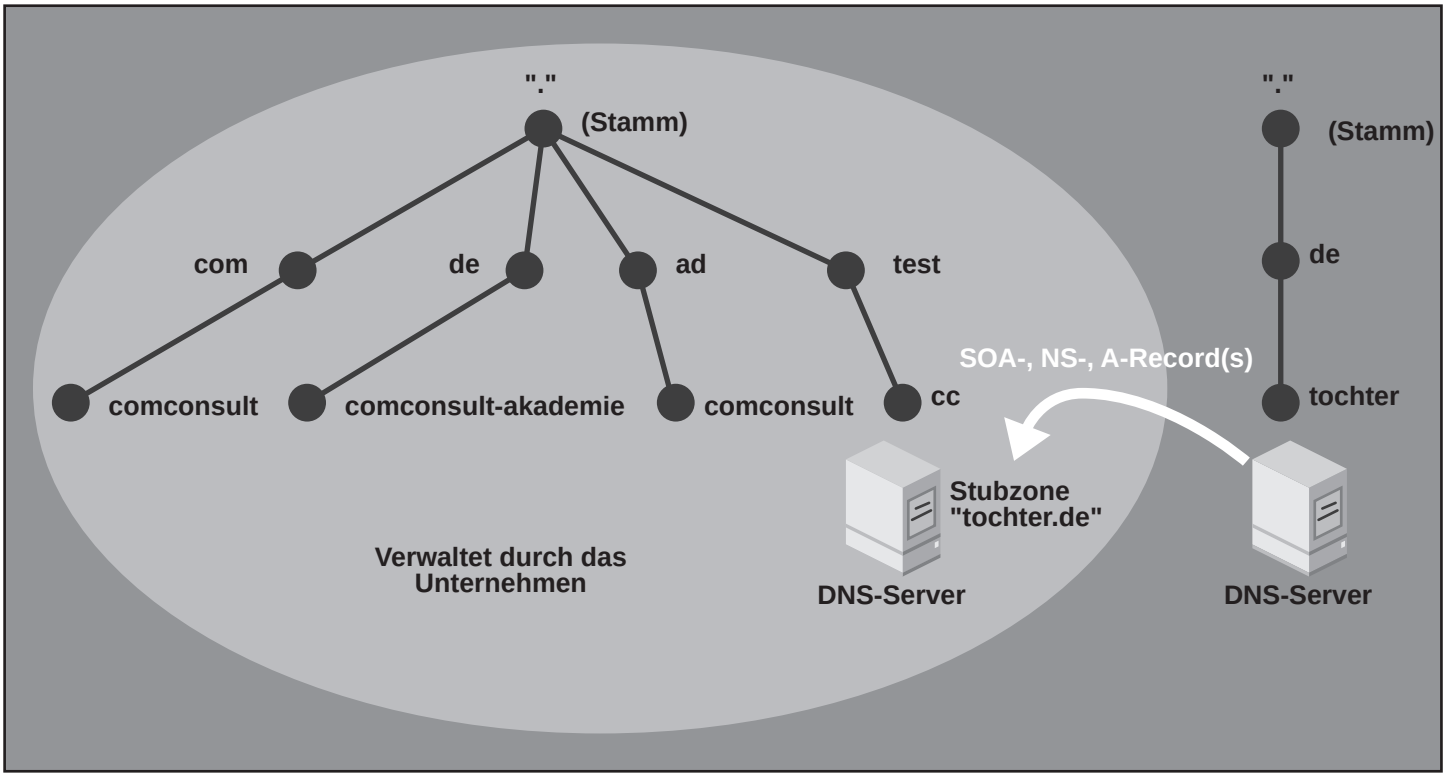
Nach der Auswahl des DNS-Servers wird der eigentliche Wizard zur DNS-Installation und -Konfiguration gestartet.

Im Rahmen dieses Artikels wird nicht auf den gesamten Installationsprozess eingegangen, sondern es werden die wichtigsten Punkte herausgenommen. Grundsätzlich erlaubt der Assistent die Konfiguration von Forward-Lookup-Zonen, Reverse-Lookup-Zonen oder nur von Stammhinweisen. Entscheidet man sich für die Konfiguration von Zonen, dann wird im nächsten Schritt der Zonentyp abgefragt. Bei der ersten Installation - es ist kein Active Directory vorhanden - stehen die klassischen textdateibasierten Zonentypen (primär und sekundär) zur Auswahl und ein neuer Zonetyp, der mit Windows (.NET-) Server 2003 eingeführt wird, die so genannte Stubzone.

Bei einer Stubzone handelt es sich um eine Zone, die lediglich die Ressourceneinträge beinhaltet, um die autorisierten DNS-Server einer Zone zu finden. Diese Ressourceneinträge sind der SOA(start of authority)-resource record, die NS(Name Server) resource records und die erforderlichen A-resource records. Somit handelt es sich nicht um eine sekundäre Zone, die ja alle Ressourceneinträge beinhaltet und repliziert, und auch nicht um einen Hinweis auf einen Stammserver, da direkt eine bestimmte (untergeordnete) Zone angesprochen wird. Der Vorteil liegt darin, dass somit direkt Clientanfragen an die entsprechenden DNS-Server gelangen, wobei die Namensauflösung folgendermaßen erfolgt: Stellt ein DNS-Client eine rekursive Anfrage an einen DNS-Server, die sich auf eine von ihm gehostete Stubzone bezieht, dann sendet dieser Server direkt eine iterative Anfrage an den DNS-Server dieser Zone. Dies geschieht analog zu dem Vorgehen, wie bei der Nutzung eines Nameserver-Records im Cache. Sollte die Namensauflösung mittels der Stubzone nicht funktionieren, dann versucht der DNS-Server, der die Stubzone bereithält, mittels des Standardwegs über die Stammserver eine iterative Anfrage.

Grundsätzlich wird aber durch die Nutzung von Stubzonen die Anzahl der iterativen Anfragen im Vergleich zum Modell via Stammserver minimiert. Ein weiterer Vorteil der Stubzone ist, dass auch zusätzlich autorisierte Server automatisch repliziert werden, ohne dass diese manuell nachgepflegt werden müssen. Für die Praxis haben die Stubzonen aber auch einen wichtigen Designaspekt. Bei vielen Konzipierungen erfolgt die Verwendung eines internen DNS-Stammes. Diese Verwendung bedeutet ja, dass der DNS-Stamm (der Punkt ".") im Unternehmensnetz verwaltet wird und dass eine strikte Abkoppelung von den Stammservern im Internet erfolgt (siehe auch Artikel "Active Directory und DNS eine Welt?" aus dem Netzwerk Insider vom August 2001). Somit entsteht ein "privater Namensraum" bei dem sich alle Rechner "sehen" können, ohne dass besondere Delegierungen eingerichtet werden müssen, auch wenn es sich um unterschiedlichste Namensräume handelt, wie beispielsweise comconsult.com, comconsult-akademie.de, comconsult.ad oder cc.test. Wurde oder wird ein solches Modell etabliert und man hat trotzdem die Anforderung, dass auch Informationen anderer Domänen (z.B. Tochtergesellschaften) außerhalb des eigenen "privaten" Namensraums zur Verfügung gestellt werden müssen, dann ist es noch unter Windows 2000 so, dass sekundäre Zonen dafür eingerichtet werden müssen. Dies hat aber den Nachteil, dass die gesamten Zonen repliziert werden. Mit den Stubzonen ist es jetzt möglich, nur zielgerichtete Verweise auf die relevanten Zonen zu definieren und den Replikationsverkehr auf ein Minimum zu reduzieren. Das Bild 3: Interne DNS-Root und Stubzone stellt dieses Szenario nochmals dar. Anfragen, die sich auf die Domäne tochter.de beziehen, werden mit Hilfe der Stubzone direkt aufgelöst.

Bild 3 Interne DNS-Root und Stubzone



Aber zurück zur Konfiguration des DNS-Servers.

Im Normalfall entscheidet man sich für eine neue primäre Zone. Neben den Namen für die Zone wird man unter Windows Server 2003 nun auch gefragt, ob man die dynamische Aktualisierung zulassen möchte, dies muss unter Windows 2000 im Nachlauf zur ersten Konfiguration gemacht werden. Ebenfalls kann man eine Reverse-Lookup-Zone einrichten.

Nach dieser Konfiguration wird man dann gefragt, ob man Weiterleitungen einrichten möchte. Hier besteht dann die Möglichkeit, gezielt Server anzugeben, auf die Namensanfragen weitergeleitet werden sollen, die der Server selber nicht beantworten kann.

Wählt man an dieser Stelle "nein", dann versucht der Wizard als erstes automatisch Hinweise auf Stammserver zu suchen. Nach der Meldung, dass er keine Stammserver finden kann, wird die Installation abgeschlossen. Es werden die Standard-Stammserver auf dem Server eingetragen.

Möchte man allerdings eine interne DNS-Root verwenden, muss man als nächsten Schritt den Punkt "." als weitere primäre Zone einrichten. Anschließend werden automatisch die erstellten Hinweise auf die Stammserver wieder gelöscht und die entsprechenden Delegierungen für die im ersten Schritt erstellte Domäne erzeugt (siehe auch Bild 4: DNS-MMC nach erster Installation).

Wie ebenfalls aus Bild 4 zu ersehen ist, stellt sich die MMC (Microsoft Management Console) für DNS fast so dar, wie unter Windows 2000. Lediglich die Ereignisanzeige für DNS und direkte Links (Hinweise auf das Stammverzeichnis, Weiterleitungen) wurden zusätzlich implementiert. Dies ist für den Administrator sicherlich im Betrieb hilfreich.

Bis auf die Stubzonen wurden bis jetzt keine nennenswerten neuen Aspekte vorgestellt, wobei gleich darauf zu verweisen ist, dass innerhalb des DNS die wichtigen Neuerungen im Zusammenspiel mit dem Active Directory hinzukommen.

Aus diesem Grund erfolgt jetzt die erste Betrachtung des Active Directory, ebenfalls unter Zuhilfenahme des Wizard zur Serververwaltung.

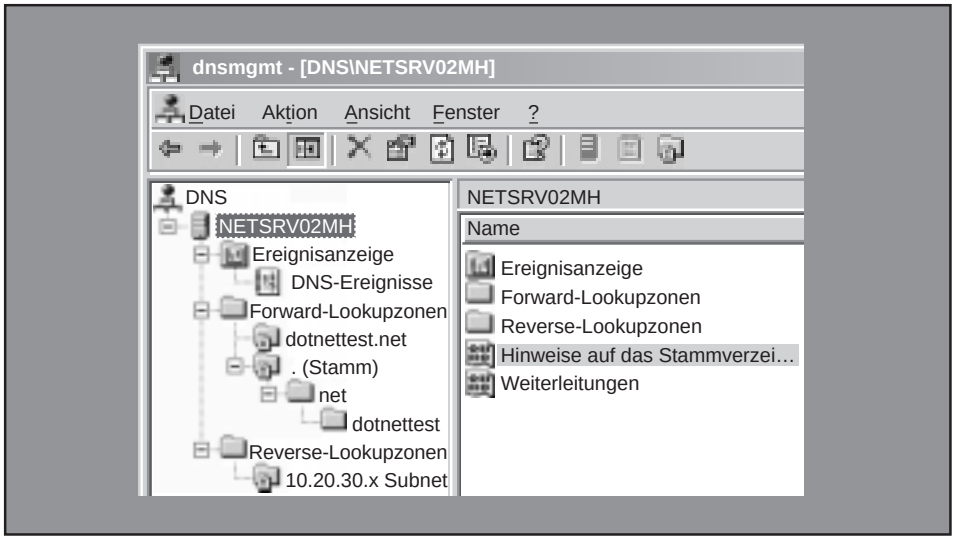


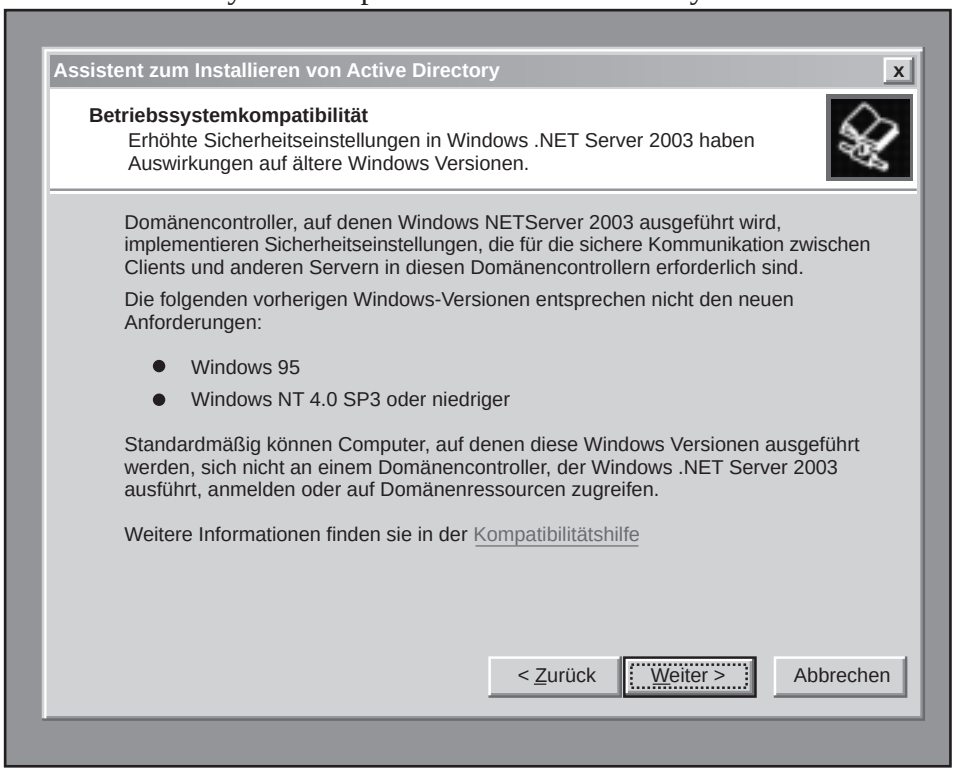

Bild 4 DNS-MMC nach erster Installation

**Implementierung des Active Directory**

Mit dem Wizard oder auch durch das Ausführen von dcpromo.exe wird der Assistent zur Installation des Active Directory gestartet.

Der erste elementare Hinweis folgt direkt, denn mit dem Active Directory von Windows 2003 Server können sich standardmäßig Windows 95- und Windows NT 4.0 SP3- (oder niedriger) Computer nicht mehr an das Active Directory anmelden oder Domänenressourcen nutzen (siehe Bild 5).

Bild 5 Betriebssystemkompatibilität Active Directory Windows Server



In den nächsten beiden Schritten werden sehr entscheidende Konfigurationen für das Active Directory durchgeführt. Wie unter Windows 2000 Active Directory wird mit diesen Angaben definiert, um welchen Domänenkontroller es sich handelt.

Zum ersten für eine neue Domäne oder um einen weiteren Domänenkontroller für eine bestehende Domäne und zum zweiten, sofern es sich um einen neuen Domänenkontroller handelt, ob dieser eine neue Gesamtstruktur (Forest) – also eine neue Active Directory Rootdomäne (nicht zu verwechseln mit einer DNS-Root) –, eine neue untergeordnete Domäne (subdomain) in einer bestehenden Gesamtstruktur oder eine neue Domänenstruktur innerhalb einer Gesamtstruktur (peer domain) bereitstellt. Wichtig ist, wie auch schon unter Windows 2000, dass nur an dieser Stelle die impliziten transitiven Vertrauensstellungen implementiert werden.

Die verschiedenen Modelle, die sich im Vergleich zu Windows 2000 nicht geändert haben, sind ausführlich im bereits benannten Artikel des Netzwerk Insiders vom August 2001 beschrieben.

Mit Windows Server 2003 ist lediglich die Anzahl der Eingabefenster minimiert worden, da dies jetzt nicht in zwei sondern in einem Fenster geschieht (siehe Bild 6).

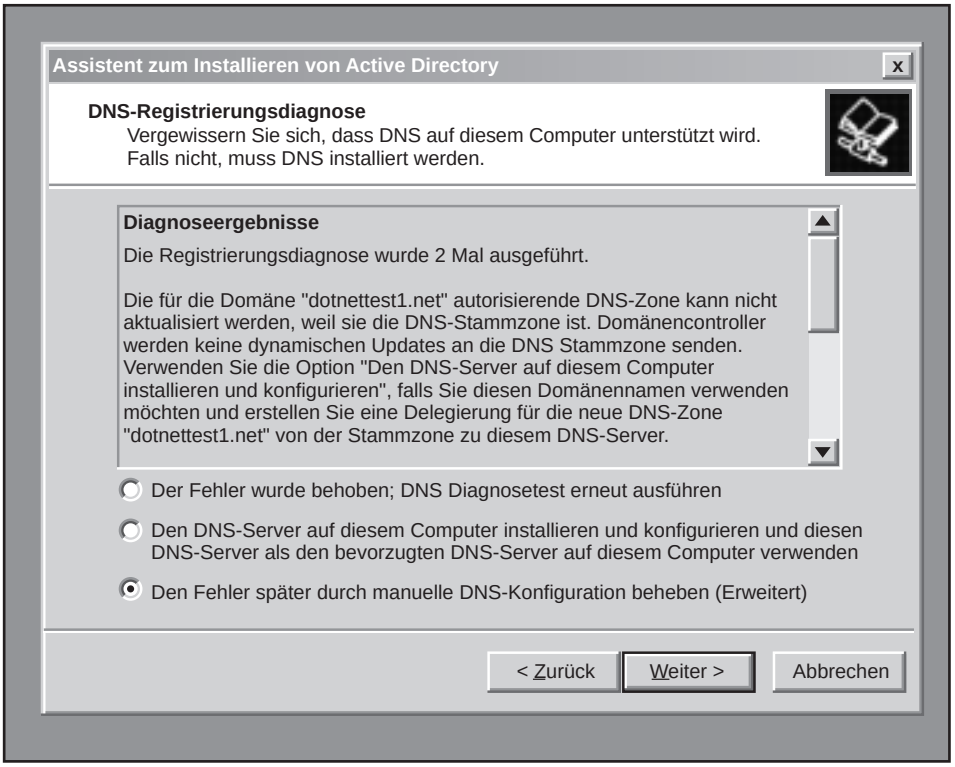
Ebenfalls verbessert wurde die im weiteren Verlauf stattfindende DNS-Diagnose, um sicherzustellen, dass die entsprechende DNS-Infrastruktur vorhanden ist. Ist das Ergebnis negativ, dann kann man unter folgenden Optionen auswählen (siehe Bild 7: Negative DNS-Diagnose bei der Installation des Active Directory):

Man behebt den Fehler im DNS eigenständig und führt die Diagnose erneut aus, man hat kein DNS konfiguriert und lässt den Assistenten ebenfalls DNS installieren und konfigurieren (dies ist in kleineren Umgebungen ggf. zu empfehlen) oder man behebt den Fehler zu einem späteren Zeitpunkt. Die letzte Variante ist natürlich nicht zu empfehlen, da dann von vorneherein eine Fehlkonfiguration vorgenommen wird, die später nur mit erhöhten Aufwand nachgezogen werden kann. Zu empfehlen ist natürlich, entsprechend den aufgezeigten Ablauf innerhalb des Artikels, die vorherige Konfiguration des DNS.

Nach Konfiguration dieser und einiger weiterer Schritte erfolgt die eigentliche Installation des Active Directory. Anschließend ist wiederum ein Neustart des Servers erforderlich.


Bild 6 Wahl der Domänenstruktur unter Windows Server 2003

Bild 7 Negative DNS-Diagnose bei der Installation des Active Directory 2003



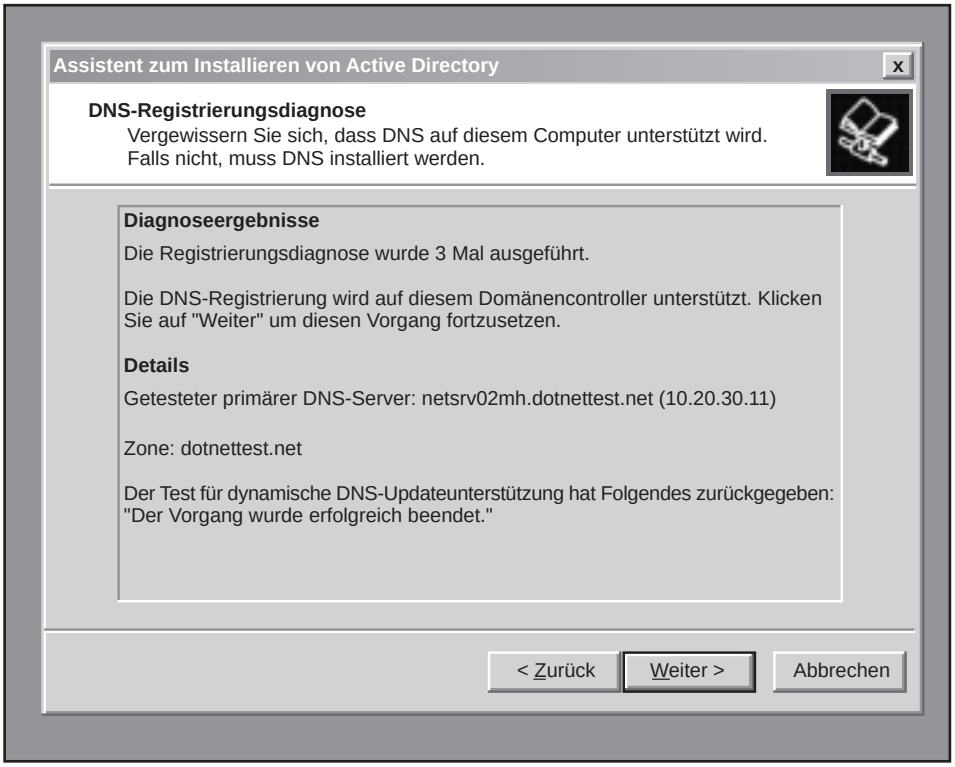
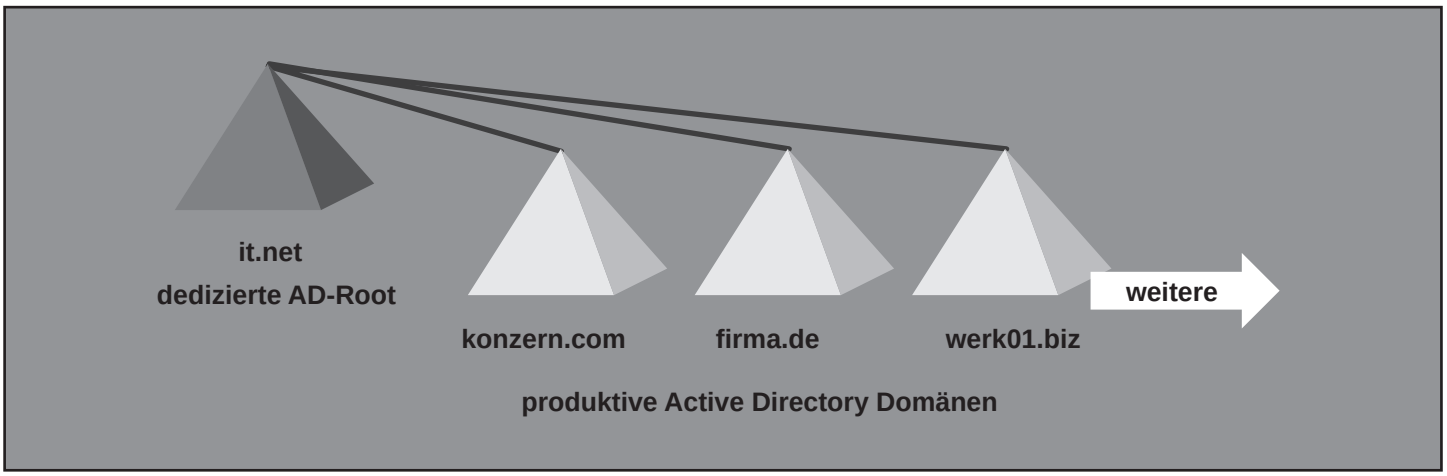



Bild 8 Positive DNS-Diagnose bei der Installation des Active Directory 2003

Mit Windows Server 2003 gibt es aber noch eine zusätzliche Neuerung im dcpromo-Prozess zur Installation des Active Directory. Man kann das dcpromo mit dem Parameter /adv (advanced) ausführen. Wird dies so ausgeführt, dann kann die Erstreplikation von einer Sicherung des Active Directory erfolgen. Dies ist insbesondere für die Implementierung des ersten Domänenkontrollers an Standorten interessant, die über eine nicht so performante WAN-Verbindung verfügen. Nachdem die Erstreplikation von der Sicherung gelaufen ist, werden nur die Änderungen, die sich nach dem Sicherungszeitpunkt ergeben haben, über die standardmäßige Replikation aktualisiert. Für die Planung einer flächendeckenden Implementierung bringt dies somit erhebliche Vorteile.

Wie bereits schon mehrfach im Artikel erwähnt, sind die Entscheidungen, die mit dem dcpromo umgesetzt werden, so elementar wie für das Active Directory bei Windows 2000. Dieser Umstand lässt weiterhin das Thema "dedizierte Active Directory Stammdomäne" im Mittelpunkt der ersten Planungen zum Active Directory stehen. Aufgrund der Projekt- und Seminarerfahrung kann die Implementierung dieser besonderen Domäne fast grundsätzlich empfohlen werden. Insbesondere hinsichtlich der Flexibilität wird mit dieser Art der Implementierung das Bestmögliche erreicht. Natürlich spielen bei der Implementierung einer dedizierten Active Directory Rootdomäne auch sicherheitstechnische Aspekte eine Rolle – also besonderer Schutz für Enterprise-(Organisations-)Admins, Schema-Admins und Domänenadministratoren der Rootdomäne, die sich eigenständig zu Mitgliedern der vorgenannten Gruppen machen können; im Vordergrund steht aber die Flexibilität in der Strukturierung des Active Directory. Wird eine dedizierte Rootdomäne implementiert (sie enthält "nur" die Standardgruppen), dann kann das abhängige Design sehr variabel angepasst werden. Es können Subdomänen im gleichen Namensraum eingefügt werden oder, und dies ist viel häufiger der Fall, man kann z.B. unter Wahrung der Corporate Identity weitere Domänen im eigenen Namensraum anbinden (Peerdomänen). Diese Flexibilität wird mit der neuen Version des Active Directory unter Windows (.NET-)Server 2003 noch gesteigert, denn ab dieser Version ist es auch möglich, zumindest die Domänennamen zu ändern, "natürlich" nicht die Struktur hinsichtlich der Active Directory Root Domäne (siehe hierzu auch Kasten 2 - 4: Domain Rename Tool)! Betrachtet man die Beispielstruktur aus dem Bild 9, so besitzt jeder Teil des Konzerns seine eigene Domäne. Ergeben sich jetzt z.B. Änderungen in der Benennung der Firma, sei es durch Zukauf, dann kann ab der Version 2003 darauf reagiert werden. Dies ist ein Vorteil für die neue Version, wobei dies als nicht so elementar hinsichtlich des ersten Designs angesehen wird.

Bild 9 Dedizierte AD-Root und produktive Domänen



Ferner sollte auch in Konzepten für Windows 2003 Server Active Directory beachtet werden, zum einen die Anzahl der Gesamtstrukturen (erste Designentscheidung) und zum anderen insbesondere die Anzahl der Domänen innerhalb einer Gesamtstruktur so gering wie möglich zu halten. Denn es ist nach wie vor so, dass eine einzige (produktive) Active Directory Domäne die beste Basis für eine effiziente Administration bildet. Grundsätzlich gibt es technisch bis zu einer gewissen Größe (man kann dabei von mehreren zehntausend Benutzern und hundert[en] Standorten ausgehen) nur einen Aspekt, der die Implementierung mehrer Domänen erforderlich macht. Dies sind die Kontorichtlinien, wie die Kennwortrichtlinien, die Kontosperrungsrichtlinien und Kerberos Richtlinien. Bevor jetzt jedoch auf weitere Neuerungen im Active Directory eingegangen wird, wird noch mal das Thema DNS aufgegriffen, da die Kombination DNS und Active Directory neue Aspekte im Windows (.NET-)Server 2003 bietet.

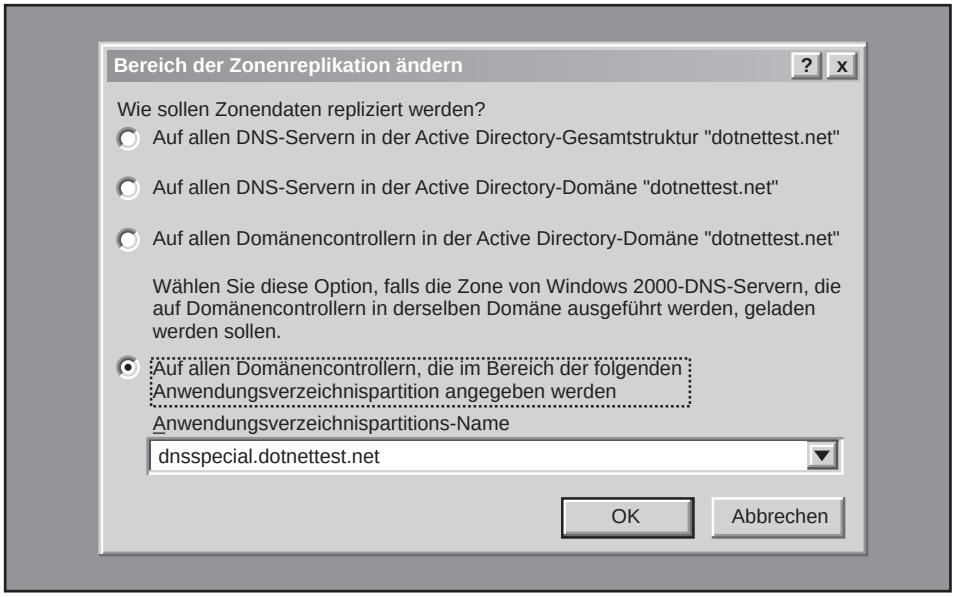



Bild 10 Active Directory integrierte Zonentypen unter Windows Server 2003

### DNS im Zusammenspiel mit Active Directory von Windows (.NET-)Server 2003

Nach der Installation des Active Directory stehen innerhalb des DNS – wie bei Windows 2000 – Active Directory integrierte Zonen zur Verfügung, jedoch gib es hier im Gegensatz zu Windows 2000 eine ganze Reihe verschiedener Typen. War es noch bei Windows 2000 so, dass die integrierten Zonen auf alle Domänenkontroller einer Domäne repliziert werden, besteht bei Windows Server 2003 die Möglichkeit zu differenzieren, siehe Bild 10: Active Directory integrierte Zonentypen unter Windows Server 2003.

Bei den Active Directory integrierten Zonen kann man jetzt wählen, auf welche Server die Informationen zu DNS mittels des Active Directory repliziert werden. Einmal wird unterschieden, dass nur auf Domänenkontrollern repliziert wird, die auch DNS ausführen, oder auf alle Domänenkontrollern. Bei der Replikation auf DNS-Server, die ja auch immer Domänenkontrollern sind, besteht zusätzlich die Möglichkeit zu wählen, ob die Replikation "nur" innerhalb einer Domäne oder in der Gesamtstruktur durchgeführt wird. Erfolgt die Replikation nur auf DNS-Server innerhalb einer Domäne, so wird die Replikationslast verringert, da nur die Maschinen die Informationen erhalten, die den Dienst auch ausführen.

Im Vergleich zu Windows 2000 sollte dies die Standardeinstellung sein, wenn die DNS-Informationen nur in einer Domäne benötigt werden. Allerdings muss auch erwähnt werden, dass bei Implementierungen, die sich auf Active Directory integrierte Zonen stützen, selten der Fall auftritt, dass Domänenkontroller ohne DNS-Server-Dienst implementiert werden.

Viel interessanter ist jedoch die Möglichkeit auf allen DNS-Server in der Gesamtstruktur zu replizieren. Hiermit ist unter Windows 2003 Server eine Möglichkeit geschaffen wurden, Informationen alle relevanten Teilnehmer für das Active Directory zur Verfügung zu stellen. Man muss sich natürlich darüber im Klaren sein, dass dann auf alle Domänenkontroller, die DNS-Server ausführen, die Informationen repliziert werden und somit ein im Projekt zu betrachtendes Replikationsvolumen entsteht.

Bei der Replikation auf alle Domänenkontroller kann man einmal den Windows 2000-Standard wählen, dass die DNS-Informationen auf alle Domänenkontroller der Domäne repliziert werden, oder man kann auswählen, dass auf eine so genannte Anwendungsverzeichnispartition repliziert wird.

Neben den (Standard-) Verzeichnispartitionen oder – wie sie auch genannt werden – Namenskontexten, wie z.B. Domain Naming Context, Configuration Naming Context und Schema Naming Context, können unter Active Directory Windows 2003 Server auch "eigene" Partitionen angelegt werden. Hierbei kann dann explizit definiert werden auf welche Domänenkontroller diese Partition innerhalb der Gesamtstruktur repliziert wird. Entscheidend für DNS ist, dass diese Partitionen auch im DNS-MMC ausgewählt werden können (siehe Bild 10 - dnsspecial.dotnettest.net). Angelegt und verwaltet werden diese Partitionen mit dem Befehlszeilentools dnscmd oder ntdsutil, siehe hierzu auch Kasten 1.

Dieses Feature ist eine hervorragende Neuerung mit Windows Server 2003, welches insbesondere die Flexibilität hinsichtlich des DNS-Designs steigert. Im Umkehrschluss ist jedoch zu berücksichtigen, dass das häufig unter Windows 2000 verwendete Argument "verwende Active Directory integrierte Zonen und man braucht sich nicht mehr um die Replikation zu kümmern, denn dies macht das Active Directory" wegfällt, da dann natürlich entsprechende Planungen erforderlich sind. Grundsätzlich überwiegt jedoch der Vorteil der Flexibilität und der neuen Gestaltungsmöglichkeiten. Betrachtet man das Szenario, welches für die Stubzonen dargestellt wurde (siehe Bild 3: Interne DNS-Root und Stubzone), dann ist diese Stubzone (tochter.de) ein gutes Beispiel für die Speicherung in einer Anwendungspartition. Diese Partition wird dann auf alle Domänenkontroller der produktiven Domänen (comconsult.com, comconsult-akademie.de, comconsult.ad und cc.test) repliziert. Dieses Beispiel wird auch in Bild 10 herangezogen.

## Kasten 1 dnscmd Befehle für Active Directory Anwendungsverzeichnispartitionen

**Anlegen einer Active Directory Anwendungsverzeichnispartition:**

dnscmd <Servername> /createdirectorypartition <fully qualified domain name (FQDN)>
Beispiel: dnscmd server01 /createdirectorypartition dnsspecial.dotnettest.net
(für den lokalen Server kann auch der Punkt "." verwendet werden, ansonsten kann der Hostname oder die IP-Adresse verwendet werden.)
dnscmd . /createdirectorypartition dnsspecial.dotnettest.net
dnscmd 10.10.10.10 /createdirectorypartition dnsspecial.dotnettest.net

**Löschen einer Active Directory Anwendungsverzeichnispartition:**

dnscmd <Servername> /deletedirectorypartition <FQDN>
Beispiel: dnscmd server01 /deletedirectorypartition dnsspecial.dotnettest.net

**Einen Domänenkontroller in die Anwendungsverzeichnispartitionsreplikation aufnehmen:**

dnscmd <Servername> /enlistdirectorypartition <FQDN>
Beispiel: dnscmd server01 /enlistdirectorypartition dnsspecial.dotnettest.net

**Einen Domänenkontroller aus der Anwendungsverzeichnispartitionsreplikation entfernen:**

dnscmd <Servername> /unenlistdirectorypartition <FQDN>
Beispiel: dnscmd server01 /unenlistdirectorypartition dnsspecial.dotnettest.net

**Anzeigen der vorhandenen Anwendungsverzeichnispartitionen:**

dnscmd <Servername> /enumdirectorypartitions
Beispiel: dnscmd server01 /enumdirectorypartitions
Beispielergebnis siehe Bild 11:

```
C:\>dnscmd ./enumdirectorypartitions
Enumerated directory partition list:

        Directory partition count = 3

 dnsspecial.dotnettest.net                  Enlisted
 DomainDnsZones.dotnettest.net              Enlisted  Auto Domain
 ForestDnsZones.dotnettest.net              Enlisted  Auto Forest

Command completed successfully.
```

Bild 11

Hinweis: Die Partitionen "domaindnszones.dotnettest.net" und "forestdnszones.dotnettest.net" entsprechen den im Artikel beschriebenen anderen neuen Zonentypen unter Windows Server 2003 Active Directory DNS.

**Informationen zu einer Anwendungsverzeichnispartition anzeigen lassen**

dnscmd <Servername> /directorypartitioninfo <FQDN>
Beispiel: dnscmd server01 /directorypartitioninfo dnsspecial.dotnettest.net
Beispielergebnis siehe Bild 12:

```
C:\>dnscmd . /directorypartitioninfo dnsspecial.dotnettest.net
Directory partition info:
  DNS root:   dnsspecial.dotnettest.net
  Flags:      0x10 Enlisted
  State:      0
  Zone count: 1
  DP head:    DC=dnsspecial,DC=dotnettest,DC=net
  Crossref:   CN=9b880823-5215-4497-8906-040f438e702d,CN=Partitions,CN=Con...
  Replicas:   2
    CN=NTDS Settings,CN=NETSRV03MH,CN=Servers,CN=Aachen,CN=Sites,CN=Config...
    CN=NTDS Settings,CN=NETSRV02MH,CN=Servers,CN=Aachen,CN=Sites,CN=Config...
Command completed successfully.
```

Bild 12

Das dnscmd ist Bestandteil der Supporttools von Windows (.NET-)Server 2003.

Windows (.NET-)Server 2003 – warten oder starten?

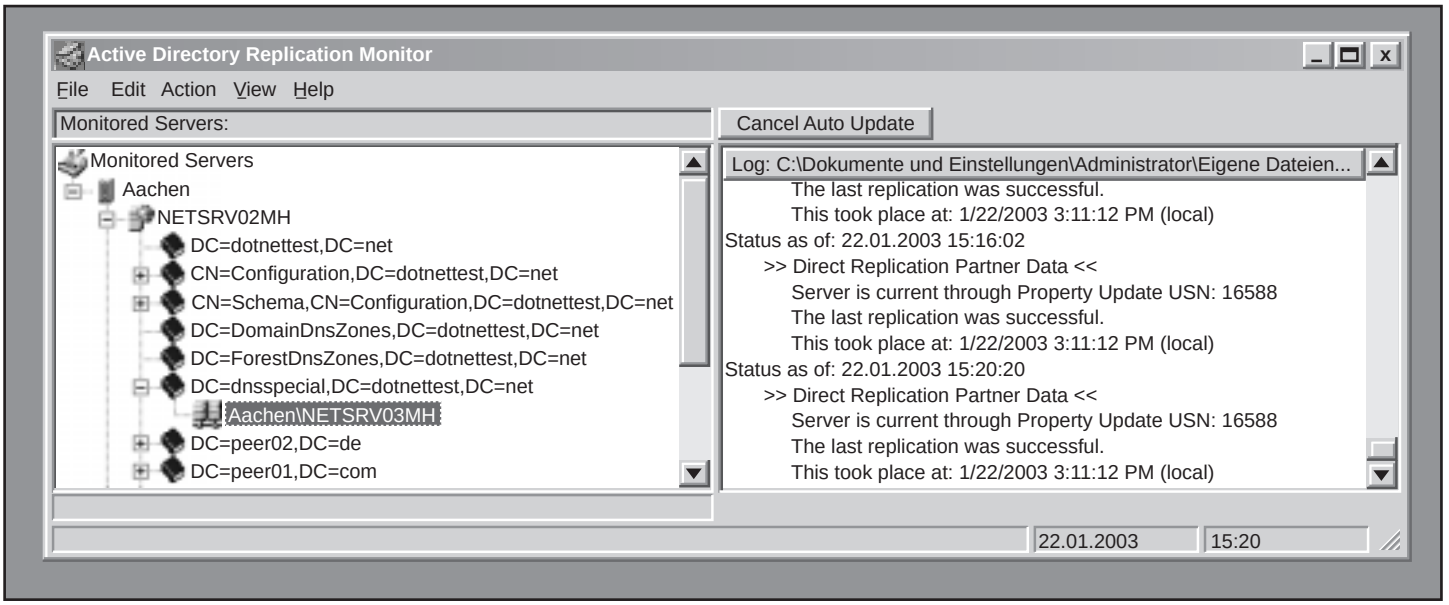
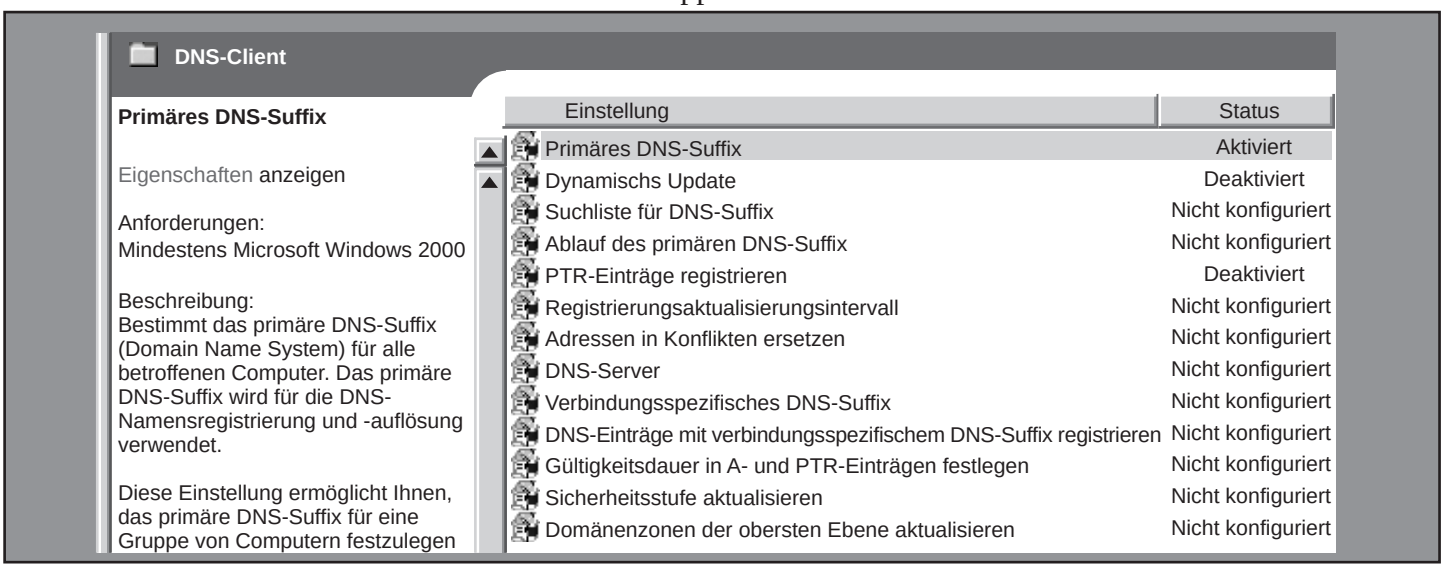



Bild 13 Replikationsmonitor und eine Anwendungsverzeichnispartition

Wie auch die anderen Partitionen des Active Directory, taucht die Anwendungsverzeichnispartition in den entsprechenden Verwaltungstools auf. Bestes Beispiel für ein solches Tool ist der "Replication Monitor" aus den Support Tools, welcher grundsätzlich zu empfehlen ist. Bild 13 zeigt die Darstellung einer Anwendungsverzeichnispartition im Replication Monitor. Zu sehen ist eine Replikationsverbindung zwischen dem angezeigten Domänenkontroller "netsrv02mh.dotnettest.net" und dem Server "netsrv03mh.peer01.com". Die Server liegen innerhalb einer Gesamtstruktur, jedoch in unterschiedlichen Namensräumen. Im Detail wird dokumentiert, dass die letzte Replikation erfolgreich um 15:12 Uhr am 22.01.2003 gelaufen ist und die USN (Update Sequence Number) 16588 lautet. Der Status ist vom 22.01.2003 um 15:20 Uhr.

Eine weitere Bereicherung zum Thema Active Directory und DNS sind die mitgelieferten Gruppenrichtlinien für DNS. War es bis Windows 2000 so, dass man sich bei Bedarf, z.B. zur Definition des primären DNS-Suffixes, selbst erstellter Richtlinien bedienen musste, werden mit Windows Server 2003 eine Reihe von Gruppenrichtlinien geliefert. Allerdings ist hier eine Einschränkung zu beachten, die unter Umständen in so manchen Netzwerken von Nachteil ist: Alle diese Gruppenrichtlinien erfordern auf Clientrechnerseite mindestens Windows XP. Einzige Ausnahme bildet die Richtlinie zur Definition des primären DNS-Suffixes, welche auch von Windows 2000-Clients genutzt wird. In Bild 14 sind die Gruppenrichtlinien dargestellt. Neben dem primären DNS-Suffix sind für viele Implementierungen die Gruppenrichtlinien hinsichtlich dynamischem Update (Dynamisches Update und Sicherheitsstufe aktualisieren) und Suchliste für DNS-Suffix von Bedeutung. Die Thematik Gruppenrichtlinien, die bereits mit Einführung von Windows 2000 explodiert ist, wird im weiteren Verlauf des Artikels nochmals kurz betrachtet, so viel sei aber schon verraten: das Ausmaß der Explosion hat sich vergrößert.

Bild 14 DNS-Gruppenrichtlinien



| Feature | Windows Server 2003 | 2000 | NT 4.0 | BIND 9 | 8.2 | 8.1.2 | 4.9.7 |
|---|---|---|---|---|---|---|---|
| Unterstützung von SRV-Records | • | • | • | • | • | • | • |
| Dynamisches Update | • | • | | • | • | • | |
| Sicheres dynamisches Update basierend auf GSS-TSIG algorithm | • | • | | | | | |
| Inkremmenteller Zonentransfer | • | • | | • | • | | |
| UTF-8 character encoding | • | • | | | | | |
| Dnscmd.exe | • | • | | | | | |
| Active Directory integrierte Zonen | • | • | | | | | |
| Speicherung in Anwendungsverzeichnispartitionen des AD | • | | | | | | |
| Stubzonen | • | | | • | | | |
| EDNS0 | • | | | • | | | |

Tabelle 1 DNS-Feature Vergleich Windows und Bind

Bevor das Thema DNS und Active Directory beendet wird, noch zwei Hinweise: Ein DNS-Server auf Basis von Windows Server 2003 ist mit dem IETF(Internet Engineering Task Force)-Standard DNS Security Extensions-Protokoll gemäß RFC 2535 kompatibel und unterstützt das EDNS0-Protokoll gemäß Definition in RFC 2671, was es ermöglicht, dass der DNS-Server UDP (User Diagramm Protocol) DNS-Nachrichten mit einer Nutzlastgröße von mehr als 512 Oktetten empfängt und sendet. Die Tabelle 1 greift eine kleine Auswahl von DNS-Features auf und vergleicht diese mit älteren Windows Versionen sowie verschiedener BIND-Implementierungen. Hieraus kann man aber bereits ersehen, dass Microsoft natürlich seine eigenen Themen insbesondere in Kombination mit Acitve Directory forciert, aber auch dass einige Neuerungen auch von neuen BIND-Implementierungen unterstützt werden.

Vielleicht ist dies der ideale Zeitpunkt im Artikel um eine kleine persönliche Randnotiz zu vermitteln: Wenn man ein Active Directory aufbaut (und dazu ist auch die DNS-Implementierung zu zählen), dann sollte man dies "gemütlich" angehen, denn zwischen den einzelnen Konfigurationsschritten müssen oft ein paar Minuten liegen und das nicht nur, wenn das System neu bootet. Natürlich können insbesondere Replikationen forciert werden, doch dauert es meist doch noch eine gewisse Zeit bis man fortfahren sollte. Dies an Beispielen darzulegen würde den Artikel sprengen, doch vieles, was mit der Implementierung von Domänen oder Einrichten von Active Directory integrierten Zonen zu tun hat, belegt diese Aussage.

**Active Directory**

Bis zu diesem Punkt wurden im Artikel hauptsächlich Neuerungen vorgestellt, die im engen Zusammenhang mit DNS stehen. Natürlich gibt es noch weitere Neuerungen hinsichtlich des Active Directory, doch bevor diese behandelt werden, sollten die verschiedenen Modi/Levels bekannt sein.

Leider ist es so, dass nicht alle neue Features des Active Directory unter Windows Server 2003 mit der Implementierung des ersten Domänenkontrollers des neuen Betriebssystems zur Verfügung stehen. Vielmehr ist es so, dass viele interessante Features erst genutzt werden können, wenn alle Domänenkontroller unter Windows Server 2003 laufen.

Bestehende Domänenkontroller auf Basis von Windows NT oder Windows 2000 erhalten nicht automatisch die neuen Funktionalitäten, sondern unterliegen vielmehr den gleichen Einschränkungen, die sie auch schon vor der Implementierung von Windows Server 2003 haben.

Einen guten Anhaltspunkt zum Vorgehen bietet hierbei bereits Windows 2000 Active Directory, wo zur Nutzung des einheitlichen Modus (native mode) erst alle Domänenkontroller auf Basis von Windows 2000 laufen müssen und auch zusätzlich die Domäne explizit in diesen Modus gewechselt werden muss. Erst dann wird die Domäne nicht mehr im gemischten Modus (mixed mode) betrieben.

Unter Windows 2003 Server gestaltet sich die Sache noch etwas komplizierter, da sowohl Windows NT 4.0- als auch Windows 2000- und natürlich Windows 2003 Domänenkontroller für das Active Directory vorkommen können. Windows 2003 Server nutzt so genannte "Functionality Levels", um die Verfügbarkeit von (neuen) Funktionalitäten zu klassifizieren. Im Gegensatz zu Windows 2000 wird aber noch zwischen Funktionen auf Domänen- und Gesamtstrukturebene unterschieden.

Kurz gesagt, wenn alle Domänenkontroller in der Gesamtstruktur auf Basis von Windows Server 2003 laufen und alle Domänen in den entsprechenden Modus geschaltet wurden, dann stehen alle neuen Funktionalitäten zur Verfügung.

Folgende Aufstellung gibt einen Überblick über neue Funktionalitäten, die in den verschiedenen Modi zur Verfügung stehen, wobei einige bereits genannt wurden und andere im weiteren Verlauf des Artikels angesprochen werden:

**Domain Functionality Levels**

**Windows 2000 Mixed**

Die "Functionality Levels" auf der Ebene der Domänen orientieren sich an der Art der Domänenkontroller. Werden in der Domäne NT 4.0, Windows 2000 und Windows Server 2003 Domänenkontroller betrieben, dann handelt es sich um den Level "Windows 2000 Mixed". Folgende Features können dann genutzt werden:

- Erstreplikation von Backupmedien, wie bereits im Artikel beschrieben,
- Anwendungsverzeichnispartitionen, wie bereits im Artikel beschrieben,
- "Universal group caching", anmelden ohne Global Catalog,
- Verbesserungen des Benutzer-Interfaces.

Windows (.NET-)Server 2003 – warten oder starten?

### Windows 2000 Native

Sind in der Domäne Windows 2000 und Windows Server 2003 Domänenkontroller vorhanden, dann ist der Functionality Level "Windows 2000 Native" möglich und folgende Features stehen dann zusätzlich zur Verfügung:

- Universelle Gruppen,
- Gruppenverschachtelung,
- Nutzung der SID-Historie.

Für eine Migration von Windows NT 4.0 auf Windows Server 2003 ist der so genannte "Windows .NET interim" (Windows Server 2003 interim) Functionality Level von Interesse, da dabei nur Domänenkontroller auf Basis von Windows NT 4.0 und Windows Server 2003 vorhanden sind. Allerdings stehen hierbei auch nur die Funktionalitäten des "Windows 2000 Mixed" Level zur Verfügung.

### Windows .NET

Sind alle Domänenkontroller auf Basis von Windows Server 2003 implementiert, so kann der "Windows .NET" (Windows Server 2003) Functionality Level aktiviert werden. Zu den bereits beschriebenen Funktionalitäten des "Windows 2000 Native" Levels kommen dann noch folgende Funktionalitäten:

- Umbenennung von Domänen, bereits im Artikel angesprochen.
- Die Fähigkeit den Wert des Attributs "lastlogonTimestamp" von Benutzer- und Computerobjekten zu replizieren. Dies bietet eine bessere Möglichkeit zur Nachverfolgung als das Attribut "lastlogon", welches nicht zwischen Domänenkontrollern repliziert wird.
- Unterstützung der InetOrgPerson-Klasse.

Grundsätzlich ist für das Heraufstufen zu einem neuen Level zu beachten, dass dies nicht mehr rückgängig gemacht werden kann. Ist also einmal der "Windows .NET" Level erreicht, so können keine NT 4.0- und/oder Windows 2000 Domänenkontroller integriert werden. Zu beachten ist ebenfalls, dass das Heraufstufen nur durch Mitglieder der Domänen-Administratoren-Gruppe auf dem so genannten PDC-Emulator erfolgen kann, wobei sich die Verwaltungstools dann automatisch mit diesem verbinden.

### Forest Functionality Levels

Auch auf der Ebene der Gesamtstrukturen (Forests) gibt es Functionality Levels. Vom Verfahren her ist es ähnlich wie bei den Domänen - die Domänenkontroller sind in erster Linie entscheidend - jedoch bezieht es sich jetzt immer auf die Gesamtstruktur.

### Windows 2000

Vom "Windows 2000" Forest Functionality Level redet man, wenn sowohl NT 4.0, Windows 2000 als auch Windows Server 2003 Domänenkontroller vorhanden sind. Hier bei stehen dann genau die gleichen neuen Funktionalitäten wie beim Domain Functionality Level Windows 2000 Mixed zur Verfügung.

### Windows .NET Interim

In einer Gesamtstruktur bei der nur Windows NT 4.0 und Windows Server 2003 Domänenkontroller vorkommen, wird vom "Windows .NET Interim" Forest Functionality Level gesprochen. Im Gegensatz zu den Domain Functionality Levels, bei denen es ja keinen Unterschied zum Level ohne Windows 2000 Domänenkontrollern gibt, stehen in diesem Level zwei neue Funktionen zur Verfügung:

- Verbesserungen bei der Gruppenreplikation, insbes. der universellen Gruppen,
- eine Gruppengrößenbeschränkung besteht nicht,
- Verbesserung des ISTG (Inter-Site Replikation Topologie Generator).

Fairerweise muss man hierbei allerdings erwähnen, dass sich die Vorteile in erster Linie nur auf die Domänenkontroller auf Basis von Windows Server 2003 auswirken, natürlich nicht hinsichtlich der Gruppengröße.

### Windows .NET

Sind alle Domänenkontroller in der Gesamtstruktur Windows Server 2003, dann kann in den "Windows .NET" (Windows Server 2003) Forest Functionality Level geschaltet werden. Somit stehen dann auch alle Neuerungen zur Verfügung, insbesondere auch:

- "Cross forest trusts", Vertrauensstellungen zwischen zwei Gesamtstrukturen können eingerichtet werden.
- Deaktivierung und Neudefinition von Attributen und Objektklassen im Schema.
- Konvertierung einer InetOrgPerson-Objekt-Instanz in eine User-Objekt-Instanz und umgekehrt.

Ähnlich wie bei den Levels auf Domänenebene, sind auch die Heraufstufungen in der Gesamtstruktur nicht mehr rückgängig zu machen, allerdings ist dies noch schwerwiegender! Ein Beispiel könnte sein, dass sich alle Domänen bereits im Windows .NET Functionality Level befinden, die Gesamtstruktur jedoch noch nicht in den Windows .NET Level gehoben wurde. Aus irgendeinem Grund muss jedoch ein NT 4.0 Domänenkontroller zur Verfügung gestellt werden. In dieser Konstellation hätte man dann noch die Möglichkeit eine neue Domäne auf Basis des Windows 2000 Mixed Levels zu implementieren. Ist der Windows .NET Forest Functionality Level aktiviert, dann besteht diese Möglichkeit nicht mehr und man muss nach anderen Lösungen suchen. Natürlich können nur Enterprise-Admins die Gesamtstruktur in den Windows .NET Level heben, wobei eine Besonderheit zu beachten ist, welche die Verantwortung für die Enterprise-Admins nochmals steigert: Ausgangslage für das Heraufstufen können sowohl Domänen im Domain Functionality Level Windows 2000 Native als auch Windows .NET sein, wobei Domänen im Windows 2000 Native Level dann vom Active Directory automatisch in den Windows .NET Level gehoben werden. Dies unterstreicht auch noch mal den Rahmenparameter, dass nur Windows Server 2003 Domänenkontroller in der Gesamtstruktur vorhanden sein dürfen!

Bei der Beschreibung der Domain und Forest Functionality Levels wurden einige Neuerungen kurz angesprochen, welche unter anderem in folgenden Abschnitten näher betrachtet werden.

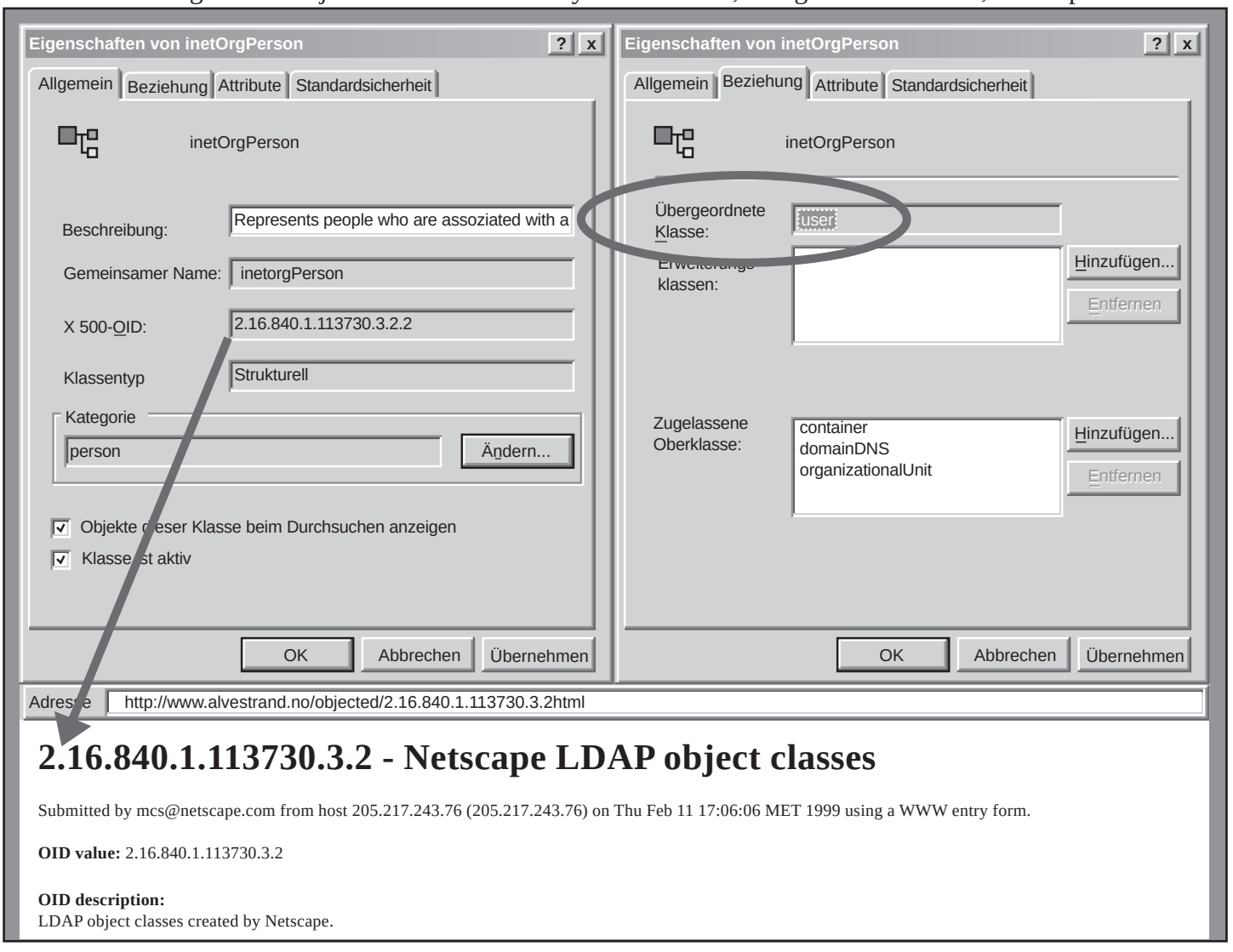
In einer Windows 2000 Active Directory Umgebung gibt es einen Nachteil, der schon so manchen Planer und Administrator enttäuscht hat: Aufgrund der Replikation können Gruppen nicht mehr als 5.000 Mitglieder beinhalten. Diese Beschränkung gibt es unter Windows NT 4.0 so nicht, auch wenn hierbei ganz klar definiert werden muss, dass Microsoft selber die Größe einer Domäne bei ca. 5.000 Benutzern sieht, das Competence Center Backoffice der ComConsult Beratung und Planung GmbH hat diese Grenze meist noch nach unten gesenkt. Unter Windows 2000 bleibt nur die Möglichkeit die Gruppen aufzusplitten, ggf. kann man diese dann jedoch wieder durch das Verschachteln zusammenführen. Mit dem neuen Active Directory fällt diese Größenbeschränkung weg und ist ab dem Forest Functionality Level Windows .NET interim verfügbar. Vervollständigt man diese Überlegungen, so ist dies der primäre Grund, warum eine Windows NT 4.0 Umgebung direkt in eine Windows Server 2003 Active Directory migriert werden sollte.

Im Umfeld der Gruppen bietet die neue Generation des Active Directory noch eine entscheidende Verbesserung gegenüber der Implementierung unter Windows 2000: Bei Änderungen der Gruppenmitgliedschaften an universellen Gruppen werden nur noch die Änderungen zwischen den Global Catalog Servern repliziert, nicht die Liste der gesamten Gruppe. Durch eine weiterentwickelte Version des ISTG kann ein Domänenkontroller die optimale Inter-Site-Replikation berechnen ohne einen Domänenkontroller zu überlasten, so dass die Grenze von ca. 100 Standorten (Sites) zur Nutzung des ISTG bei Windows Server 2003 nicht mehr vorhanden ist. Auch besteht die Möglichkeit, dass Domänenkontroller die universellen Gruppen im Cache vorhalten, so dass die Anzahl der Global Catalog Server verringert werden kann, da somit eine Anmeldung ohne Global Catalog möglich wird. Dies ist insbesondere für kleinere Außenstandorte interessant, da es unter Windows 2000 meist der Fall ist, dass diese auch zum Global Catalog gemacht werden, was aber negative Auswirkungen auf die Replikation hat, weil das Replikationsvolumen steigt. Wird allerdings Exchange 2000 eingesetzt, werden wieder die Global Catalog Server in den Außenstandorten benötigt.

Innerhalb des Schemas des Active Directory wurde eine interessante Neuerung implementiert. Leider ist es immer noch nicht möglich Objektklassen und Attribute zu löschen, jedoch können diese deaktiviert werden. Dies ist noch kein Unterschied zu Windows 2000, doch können die Namen und ObjectID's mit der neuen Version jetzt wieder verwendet werden.

Durch die Unterstützung des InetOrgPerson-Objekts schafft das neue Active Directory eine bessere Interoperabilität zu anderen Verzeichnisdiensten – insbesondere Internetverzeichnissen, da diese oft das InetOrgPerson-Objekt zur Benutzerverwaltung nutzen. Das InetOrgPerson-Objekt ist zwar nicht im X.500-Standard definiert, kann aber als Quasistandard bezeichnet werden, da es von vielen Verzeichnissen genutzt wird. Alle Objekte unterhalb der ObjectID (OID) (2.16.840.1.113730.3.2) wurden von Netscape geschaffen, siehe auch Bild 15. Besonders von Interesse ist dieses Objekt, wenn Unternehmen ein Meta Directory einsetzen (wollen) und eine Integration hinsichtlich der Replikation von Identitätsinformation des Active Directory beabsichtigen. Windows Server 2003 Active Directory beinhaltet die volle Unterstützung für das InetOrgPerson-Objekt, welches von der Benutzer Klasse abgeleitet wird, so dass es als Security Principal genutzt werden kann.

Bild 15 InetOrgPerson-Objekt im Active Directory - X.500-OID, übergeordnete Klasse, Netscape Klasse



### Interoperabilität und Metadirectory

Zum Stichwort Interoperabilität darf ein kleiner Ausblick nicht auf das fehlen, was Microsoft im Bereich seines Metadirectory plant. Im Gegensatz zum Sprung des Active Directory von Windows 2000 nach Windows Server 2003 wird die neue Version des Microsoft Metadirectory Services (MMS) 2003 wohl gravierendere Bedeutung haben. Es ist wohl die erste tatsächliche "Major-Release" seit Microsoft vor über 3 Jahren den Vorgänger von der Zoomit Cooperation übernommen hat. Grundsätzlich sind zwei Versionen des MMS geplant, die ca. 90 Tage nach der Veröffentlichung von Windows Server 2003 verfügbar sein sollen. Zum einen die Standard-Edition, die dann kostenlos zum Download bereit stehen soll, aber mit sehr eingeschränkten Funktionsumfang, und zum anderen die Enterprise-Version, die als der eigentliche Nachfolger im Bereich des Metadirectory zu sehen ist. Die Standardversion wird "nur" Identitätsinformationen zwischen verschiedenen Active Directory Gesamtstrukturen, Exchange 2000 Implementierungen hinsichtlich der globalen Adresslisten und Active Directory Applikationmode Implementierungen synchronisieren. Im Bereich des Active Directory ist dies aber eine sehr gute Erweiterung, da dann in Kombination mit Vertrauensstellungen zwischen Gesamtstrukturen, wie bereits im Artikel beschrieben, auch tatsächlich mehrere Forests in einem Unternehmen nebeneinander existieren können, ohne einen Informationsverlust hinnehmen zu müssen.

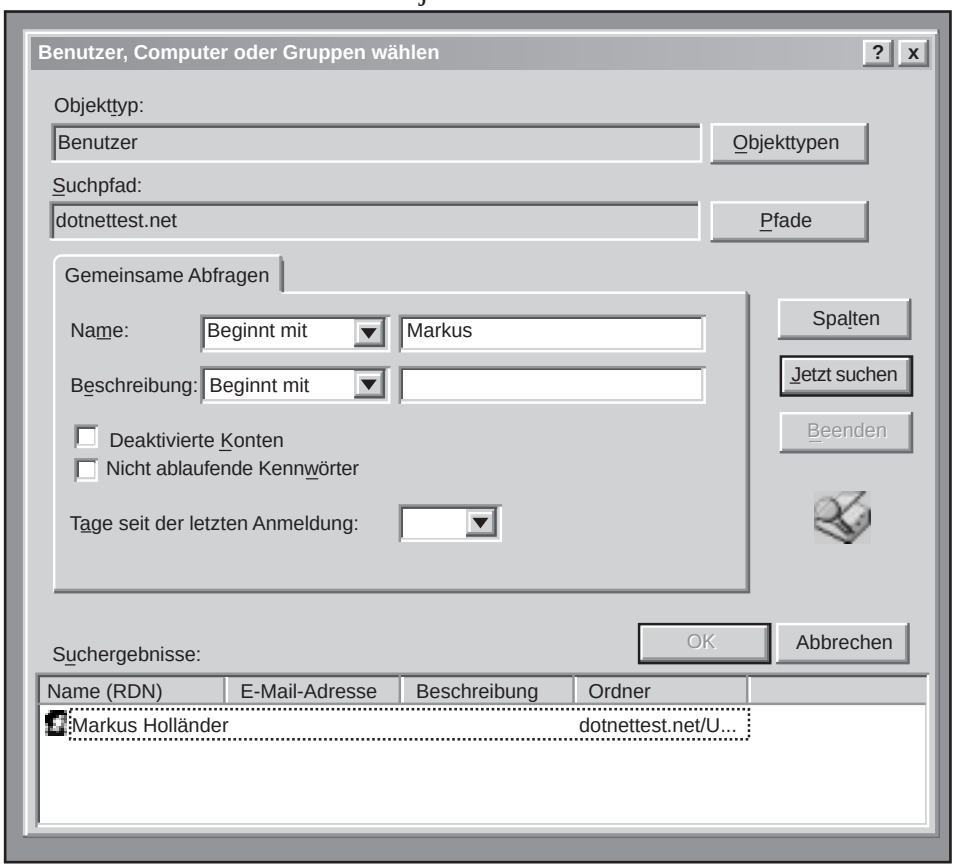
Die Enterprise-Edition bietet aber entscheidende Neuerungen: Die propritäre X.500-basierte Lösung des MMS 2.2 zur Datenspeicherung wird durch den SQL-Server 2000, der strategischen Datenbankplattform von Microsoft abgelöst. Neben den Vorteilen, die durch die Implementierung eines führenden Datenbanksystems gegeben sind und auf der Hand liegen, wie z.B. Stabilität, Sicherheit und Management, wird es natürlich einige andere Effekte geben, die ggf. nicht so gern gesehen werden. Zu diesen Effekten sind insbesondere kein direkter LDAP-Zugriff, ein flacher Namensraum und keine X.500 ähnliche Replikation zu zählen. Dies sollten besonders die Unternehmen im Auge haben, die den MMS bereits nutzen. Andererseits muss erwähnt werden, dass dann der MMS der erste strategische Dienst sein wird, der sich auf den SQL-Server abstützt, wobei dies auch in der nächsten Version des Active Directory nach Windows Server 2003 und hinsichtlich der Dateidienste im Windows XP-Nachfolger (Codename: Longhorn) der Fall sein soll. Die unter MMS 2.2 bestehende Skriptsprache zscript wird nicht weiter unterstützt und durch jede Visual Studio .NET Sprache, wie z.B. Visual Basic und Visual C# .NET, abgelöst. Einige sehr interessante Neuerungen betreffen auch die so genannten Management Agenten (MA) - "Connectoren", die architektonisch überarbeitet werden/wurden. Insbesondere ist die Art bzw. Anzahl der anzubindenden Repositories davon betroffen.Hier kann ich mich persönlich nicht des Eindrucks verwehren, dass Microsoft zu einem weiteren (entscheidenden?) Schlag Richtung Novell ausholt.

Sind noch in der Version 2.2 des MMS Management Agenten für Novell (NDS, Bindery) enthalten, fallen diese wohl zumindest in der ersten Version des MMS 2003 weg. Folgende MA's werden nach letzten Informationen enthalten sein: Sun One/iPlanet Directory 4.x/5.x (inkl. Unterstützung von "changelog"), relationale Datenbanken (insbesondere SQL-Server, Oracle und DB2), Exchange 5.5, Lotus Notes 4.6/5.0 (Lotus C API), Windows NT 4.0, LDIF(LDAP Directory Interchange Format)-Dateien, verschiedene Arten von Textdateien, DSML(Directory Services Markup Language) 2.0, andere XML(Extensible Markup Language) basierte Dateien und die MA's der Standardversion. In diesem Zusammenhang ist auch interessant, dass sich Microsoft entschlossen hat, die Vermarktungsstrategie zu ändern. Kann die Version 2.2 des MMS in erster Linie nur in Verbindung mit Dienstleistungen des Microsoft Consulting Service bezogen werden, so kann die Enterprise Version des MMS 2003 direkt gekauft werden. Hierbei sollte aber nicht verschwiegen werden, dass Microsoft einen Preis ab 24.999,00 $ pro CPU angibt.

### Benutzer-Interfaces

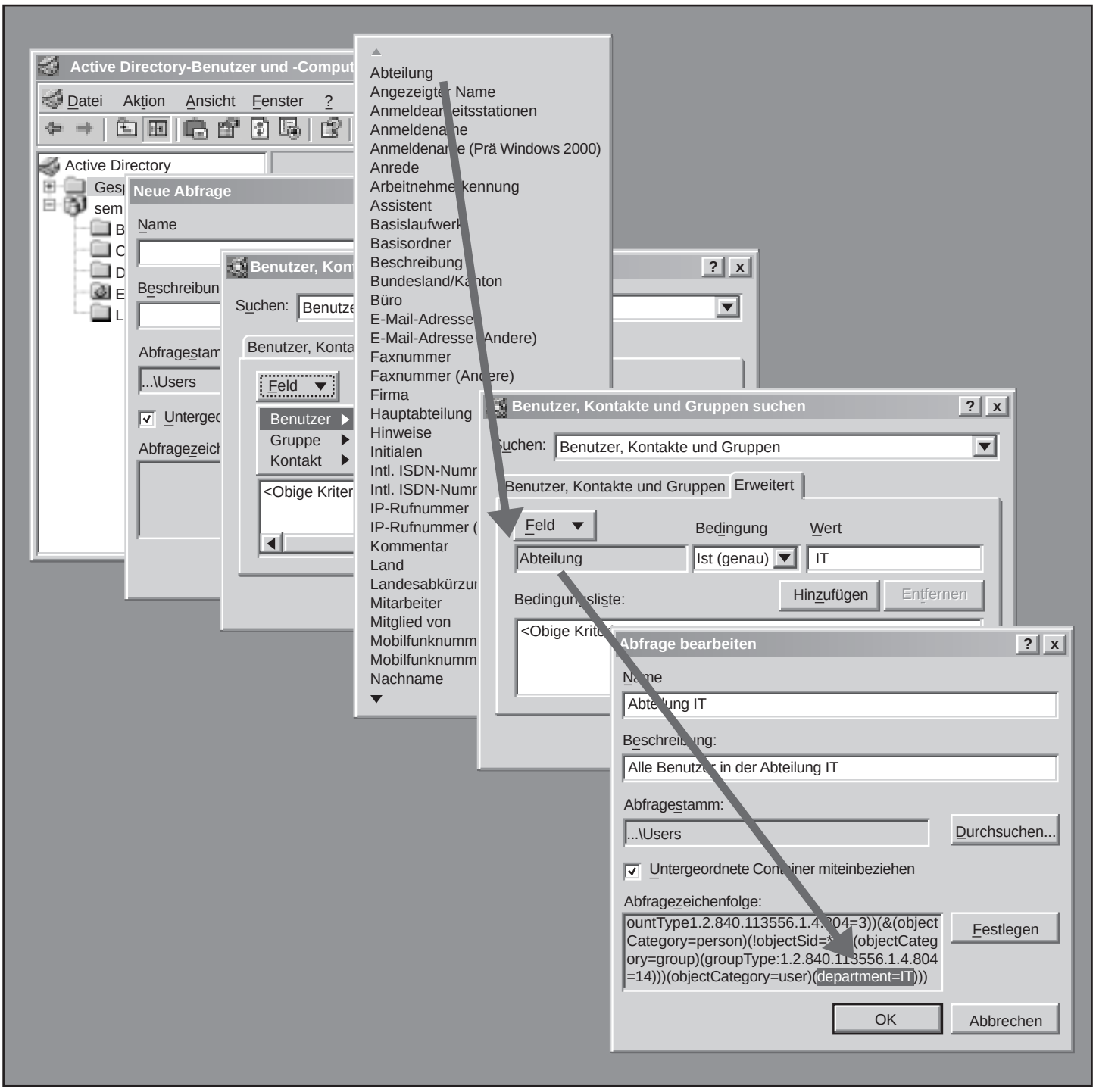
Nach diesem kleinen Exkurs zum Thema Metadirectory wenden wir uns wieder Neuerungen unter Windows Server 2003 Active Directory zu. Bei der Behandlung der Functionality Levels wurden auch Verbesserungen der Benutzer-Interfaces genannt. Stellvertretend sollen an dieser Stelle drei Änderungen angesprochen werden. Lt. Microsoft ist eine Verbesserung der neue "Object Picker" (auch in Windows XP enthalten), der es ermöglicht, gezielt - je nach Situation -Objekte auszuwählen. Prinzipiell wird zwar damit die Möglichkeit geschaffen, Abfragen - z.B. zur Rechtevergabe - zu verfeinern, doch für Administratoren ist diese Implementierung eher gewöhnungsbedürftig, da ein zusätzlicher Schritt erforderlich ist. Kann man unter Windows NT oder auch 2000 direkt aus einer Liste auswählen, so muss ab Windows Server 2003 entweder ein Suchkriterium eingegeben werden (siehe in Bild 16 "Name: Beginnt mit Markus") oder man lässt die Suchkriterien offen und lässt sich wieder alle Einträge anzeigen.

Bild 16 Object Picker



Interessanter in diesem Zusammenhang ist, dass "gespeicherte Abfragen" genutzt werden können, da dadurch Administratoren sich die MMC (Mircosoft Management Console) individuell anpassen können. Die Kriterien können auf verschiedene Objekte (siehe Beispiel Bild 17, wo "Benutzer" ausgewählt wurde) zielen, wobei dann die Auswahl auf Attributsebene verfeinert werden kann (siehe Bild 17: Abteilung). Bei der Verfeinerung können dann noch verschiedene Bedingungen, wie beispielsweise "Ist (genau)" (siehe Bild 17), "Ist nicht", "Vorhanden" u.s.w., angewendet werden. Auch kann der Bereich eingeschränkt werden, auf den sich die Abfrage bezieht. Letztendlich wird eine LDAP-Abfrage generiert, die dann auch angezeigt wird (siehe Bild 17: Abfragezeichenfolge: ... department=IT). Im Gegensatz zum Object Picker ist dies eine sinnvolle Ergänzung, wobei der Einsatz dieser Funktionalität sicher von der Größe der zu betreuenden Landschaft abhängt und natürlich auch, wie das Design auf OU-Ebene implementiert wurde, da man damit auch schon "gewisse Abfragen" überflüssig machen kann.

Bild 17 Gespeicherte Abfrage erstellen

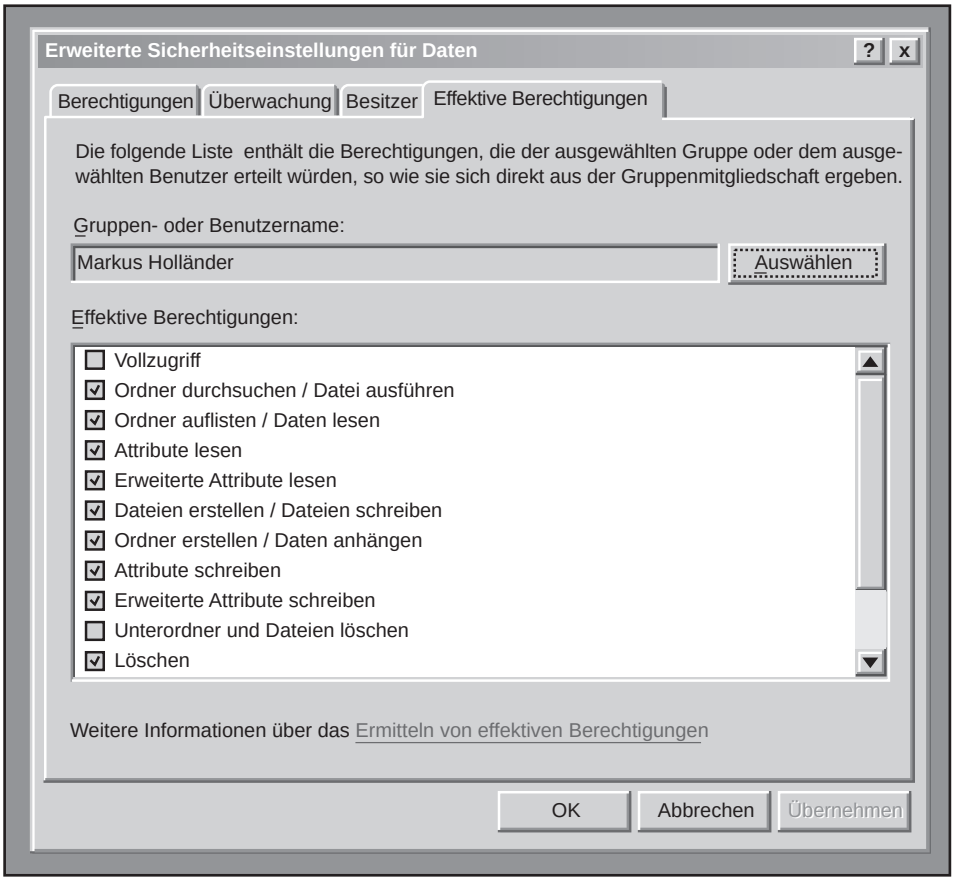


Eine andere Neuerung ist die Anzeige der "effektiven Berechtigungen". Für eine Datei, einen Ordner oder ein Active Directory Objekt lassen sich die Berechtigungen für einen Benutzer oder eine Gruppe anzeigen. Dabei werden z.B. für einen Benutzer auch sämtliche Rechte aus Gruppenmitgliedschaften und vererbte Berechtigungen berücksichtigt (siehe Bild 18). Dies ist sicherlich ein Schritt in die richtige Richtung, doch fehlt eigentlich immer noch das Werkzeug, dass es ermöglicht, sämtliche Rechte - beispielsweise eines Benutzers - anzeigen zu können. Natürlich ist dies "not by design" und von Microsoft nicht so vorgesehen, da dann alle Ressourcen abgefragt werden müssten, wobei dann auch wieder fraglich ist, ob alle Ressourcen zur Verfügung stehen. Dies liegt daran, dass die Berechtigungen in den ACLs (Access Control Lists) der Ressourcen gespeichert werden.Bezüglich der Analyse zu Benutzer- und Gruppenrechten sollte auch noch das Tool "Resultant Set of Policies" (RSoP) erwähnt werden, welches erlaubt festzustellen, welche Gruppenrichtlinien für eine Gruppe oder einen Benutzer gelten. Besonderes interessant ist dabei die Funktion "what if", die es erlaubt Szenarien zu simulieren, bevor eine neue Gruppenrichtlinie zugewiesen wird.

**Gruppenrichtlinienexplosion**

Zum Thema Gruppenrichtlinien: Diese Thematik nimmt in aktuellen Konzipierungen einen immer größeren Block in Anspruch. Betrug die Ausgangsbasis bei NT noch ca. 100 "Policyeinstellungen", werden unter Windows 2000 ca. 500 Gruppenrichtlinien vorgehalten, diese Zahl liegt nach der Einführung von Windows XP und dann mit Windows Server 2003 bei ca. 900! Eines ist dabei besonders zu beachten, teilweise bzw. vereinzelt sind die neuen Gruppenrichtlinien bereits im Windows 2000-Umfeld nutzbar (siehe DNS). Dies macht es unbedingt erforderlich, dass sich Planer und Designer auch mit dieser Thematik bei Konzipierungen im 2000-Umfeld auseinander setzen. Einige Unternehmen hegen zwar die Hoffnung, dass man dieses Thema "klein halten" kann, doch die Realität sieht meist anders aus. In einem aktuellen Fall, wo diese Hoffnung bestand, kamen zum Abschluss doch weit über 100 GPOs (Group Policy Objects) zum Einsatz. Eine nähere Betrachtung würde sicherlich einen eigenen Artikel rechtfertigen, so dass hier nicht weiter darauf eingegangen wird.

Bild 18 Anzeige der effektiven Berechtigungen




**Windows XP – der Druck zur Migration!**

Bei den Neuerungen spielt auch oft das Clientbetriebssystem eine nicht zu unterschätzende Rolle. Im vorhergehenden Abschnitt wurden die Gruppenrichtlinien besprochen, diese finden zum allergrößten Teil nur Ihre Anwendung, wenn das Clientbetriebssystem Windows XP lautet! Sicherlich wird auch eine Vielzahl von Windows 2000 (Professional) genutzt, doch sehr schwierig wird es, wenn Windows NT 4.0 Workstation am anderen Ende steht, denn dann fallen die Gruppenrichtlinien so gut wie weg. Betrachtet man die Thematik andersherum - Windows NT 4.0 auf Serverseite und Windows XP auf Clientseite -, dann fällt die Funktionalität der Gruppenrichtlinien ganz weg. Natürlich können dann die "paar" Policy-Einstellungen aus dem NT-Umfeld genutzt werden, dies geht aber zu Lasten der Clients, da dann die Registry an der "falschen Stelle" verändert wird, so dass bei einem späteren Einsatz von Windows 2000 oder Windows Server 2003 "verunreinigte" Clients vorliegen. Die logische Konsequenz ist dann wiederum ein erneutes Rollout dieser Clients oder zumindest ein nicht zu unterschätzender Aufwand, die nicht gewünschten Konfigurationen wieder rückgängig zu machen. Um dies zu verhindern, sollte also unbedingt auf Serverseite Windows 2000 (Active Directory) oder in ein paar Monaten auch Windows Server 2003 (Active Directory) implementiert sein, bevor auf Clientseite Windows XP (Windows 2000) eingesetzt wird.

Die beschriebene Konstellation hat aber auch noch einen hochbrisanten Effekt! Bei der Einleitung zu diesem Artikel wurde die Einstellung des Supports für Windows NT 4.0 Server zum 31.12.2004 als kritisches Datum genannt, tatsächlich ist aber das entscheidende Datum der 30.06.2003, denn dann endet die "Extended Support"-Phase für Windows NT Workstation, zumindest wenn man sich obiger Argumentationskette anschließt.

Aktuell führt dies in der Kundenwelt zu einigen sehr stark gepushten Projekten, damit die Phase nach dem 30.06. mit Windows NT Clients nicht zu lang wird. Auf der anderen Seite gibt es noch eine Vielzahl von Unternehmen, denen entweder nicht so richtig bewusst ist, dass es eine solche Konstellation gibt, oder die aufgrund des fehlenden Budgets in diesen Umstand geraten. Es stellt sich "nur" wieder die Frage, wie hoch ist der PONI? Bevor jedoch jetzt versucht wird die Ausgangsfrage zu beantworteten, erfolgt noch ein Blick auf das Thema Migration.

**Migration zu Windows Server 2003 Active Directory**

Hinsichtlich der Migration stellen sich zwei unterschiedliche Grundszenarien dar: Migration von Windows NT 4.0 oder Migration von Windows 2000 nach Windows Server 2003. Ein Punkt kann direkt definiert werden, der große Schritt ist immer, wenn die Migrationsbasis Windows NT lautet (auch wenn nach Windows 2000 migriert wird). Bei der Migration von Windows 2000 aus kann man fast von einem (großen) Update sprechen und nicht von einer Migration, auch ist der Planungsaufwand nicht so groß, wie in der anderen Konstellation.

Interessant ist es, wenn Windows NT das Quellsystem ist. Hier stehen dann grundsätzlich die beiden Wege "direkte Migration nach Windows Server 2003 Active Directory" oder "mit Windows 2000 als Zwischenstopp" zur Auswahl.

Ein wichtiges Argument wurde im Verlauf des Artikels bereits genannt: die Gruppengrößenbeschränkung unter Windows 2000. Ein anderes Argument ist einfach die Tatsache, die Migrationsschritte zu minimieren und direkt in das eigentliche Ziel zu migrieren und somit den Aufwand zu reduzieren.

Anhaltspunkte, welche Schritte durchgeführt werden sollten, bieten die einzelnen Functionality Levels, die definieren, welche Funktionen wann zur Verfügung stehen. Natürlich hat auch die Migrationsstrategie Auswirkungen auf den Migrationsweg. Grundsätzlich stehen ein Inplace-Upgrade, eine Parallel-Migration, ein unabhäniger Aufbau und diverse Mischformen dieser Strategien zur Verfügung.

Im Windows 2000-Umfeld als Zielsystem wurde und wird meist eine Parallelmigration angestrebt, wobei die Zieldomäne dann bereits im einheitlichen Modus (native mode) vorliegt, um alle Features aus Windows 2000 nutzen zu können.

Ein Inplace-Upgrade, also das Upgrade bestehender Domänenkontroller, kann meist nicht empfohlen werden, da entweder zum einen die Hardware-Ressourcen nicht ausreichen und / oder "Altlasten" nicht mitmigriert werden sollen, so dass ebenfalls ein "erzwungener" Konsolidierungseffekt eintritt. Welche Strategie letztendlich verwendet wird, kann nicht pauschal beantwortet werden und ist in einem Projekt zu erarbeiten.

Ein weiterer Parameter zur Definition der Strategie sind die Migrationstools. Microsoft liefert mit Windows 2000 das ADMT (Active Directory Migration Tool) in der Version 1 aus. Je nachdem, welche Anforderungen bestehen (z.B. keine Migration der Kennwörter oder nur Umbenennung von Objekten mittels Prä- oder Suffix) und wie groß die zu migrierende Umgebung ist, wird und wurde dieses Tool bei Migrationen genutzt und hat sich bewährt. Bestehen erhöhte Anforderungen, so werden derzeit meist Tools von anderen Herstellern genutzt. Zu den von mir favorisierten Tools zählen dabei Produkte der Hersteller NetIQ*, Aelita** und Quest Software***. Es ist jedoch im Einzelfall zu entscheiden und zu testen, welches Tool die spezifischen Anforderungen erfüllt.

Mit Windows Server 2003 liefert Microsoft jetzt eine weiter entwickelte Version des ADMT aus – die Version 2.0. Mit dieser Version wird die Lücke zu den oben genannten Tools anderer Hersteller verkleinert, aber nicht geschlossen. Es ist jedoch so, dass die Neuerungen die Verwendung des Tools noch ein wenig interessanter machen und dass somit dieses Tool häufiger zum Einsatz kommen wird, nicht zuletzt auch dadurch, dass es im Lieferumfang von Windows Server 2003 enthalten ist und keine zusätzlichen Lizenzkosten verursacht. In folgender Aufstellung werden einige Neuerungen kurz vorgestellt:

- Mit der neuen Version wird ein Kommandozeilentool "admt.exe" zur Verfügung gestellt, welches skriptierbar ist. Es wird somit die Möglichkeit gegeben, eigene Skripte zu generieren und Migrationen automatisiert ablaufen zu lassen. Eine Funktion wie der "undo-Wizard" des ADMT, der es ermöglicht Teilschritte, rückgängig zu machen, wird jedoch nicht in der admt.exe unterstützt. Allerdings ist es so, dass Schritte, die im Wizard rückgängig gemacht werden könnten aber mit der admt.exe durchgeführt wurden, im Wizard dann doch rückgängig gemacht werden können.
- Im ADMT V2 wird auch die Passwortmigration für die "Inter-Forest"-Migration (zwischen Gesamtstrukturen, wobei eine Gesamtstruktur auch eine NT-Domäne als Quelldomäne sein kann) unterstützt. Hierzu ist es allerdings erforderlich, dass in der Quelldomäne ein so genannter "Password Export Server" (PES) installiert wird, was mit zusätzlichem Aufwand verbunden ist. Insbesondere muss auf jedem PES und dem Rechner der den ADMT ausführt, 128-bit Verschlüsselung implementiert sein, also auch auf Seiten von NT.
- Die Protokollierung wurde etwas verbessert. Es gibt nicht mehr nur eine Log-Datei für alle Migrationsschritte (inkl. der Tests), sondern für jeden Migrationsschritt wird jetzt eine eigene Log-Datei generiert. In der Voreinstellung werden bis zu 20 dieser Logs vorgehalten, bevor diese überschrieben werden. Dieser Wert kann aber in der Registry erhöht werden.

Weiterhin gibt es eine Reihe von Neuerungen, die z.B. die erforderlichen Rechte zur Nutzung des ADMT betreffen und den Ausschluss von Attributen (Windows 2000).

Eine sehr interessante Randbemerkung unter den "Known Issues" zum ADMT ist, dass der ADMT nicht in einer Umgebung läuft in der keine NetBIOS-Namensauflösung zur Verfügung gestellt wird:

"Operating ADMT in a NetBIOS less enviroment is not supported. ADMT requires NetBIOS name resolution for all migration operations. ..." (Quelle: "readme.doc" im Installtionsverzeichnis zum ADMT Version 2).

Dies bekräftigt die Aussage des Competence Center Backoffice der ComConsult Beratung und Planung GmbH, dass das Thema NetBIOS(-Namensauflösung) im Microsoft-Umfeld (leider) noch immer aktuell ist, also auch bei Windows Server 2003 (siehe hierzu auch die Ausführungen am Anfang des Artikels).

---

* Migration Suite/Domain Migraton Admininstrator – http://www.netiq.com/products/migrate/default.asp

** Domain Migration Wizard – http://www.aelita.com/solutions/MigrationDeployment.htm

*** Fast Lane Migrator – http://www.quest.com/solutions/ms_admin_and_deployment.asp

# Windows (.NET-)Server 2003 – warten oder starten?

### Warten oder Starten?

### Windows 2000

Die Firmen, die Windows 2000 Server und das Active Directory eingeführt haben, können sicherlich der Einführung von Windows Server 2003 gelassen entgegen sehen. Sie haben den großen Schritt mit der Migration von Windows NT 4.0 nach Windows 2000 hinter sich.

Es wäre sicherlich etwas verwegen, die Einführung von Windows Server 2003 mit einem großen Service-Pack zu vergleichen, doch mit Blickrichtung Active Directory und DNS erfolgen "nur" punktuelle Verbesserungen.

Diesen Firmen obliegt jetzt die Aufgabe zu definieren, ob diese Neuerungen für sie von Bedeutung sind. Auch kann die Migration schonend erfolgen, so dass Schritt für Schritt die Domänenkontroller auf Basis von Windows Server 2003 implementiert werden können. In diesen Szenarien ist es auch durchaus viel eher vorstellbar, dass ein Inplace-Upgrade stattfindet.

Druck kommt in einer solchen Konstellation hauptsächlich, wenn neue Funktionalitäten tatsächlich schnell benötigt werden. Dies kann z.B. dann erfolgen, wenn sich der Konzern auf Unternehmensebene verändert und ggf. Namensänderungen erforderlich sind oder andere Unternehmen mit eigenen Gesamtstrukturen integriert werden müssen.

Wichtig ist, dass, wie bereits erwähnt, die elementaren Entscheidungen im Bereich des Active Directory mit der bereits durchgeführten Migration zu Windows 2000 Server implementiert wurden und nicht so leicht wieder verändert werden können. Tritt der Fall ein, dass dies erforderlich ist, dann wird eine Migration erforderlich, die dann als Ziel sicherlich keine andere Windows 2000-Umgebung hat, sondern eine Windows Server 2003-Landschaft. In diesem Fall kann dann auch nicht mehr von einem kleinen Projekt geredet werden und auch der Sache gelassen entgegen gesehen werden, denn dann gibt's ein Projekt inkl. aller Zutaten: Neues Design (Konzipierung) und Migration dorthin.

Fazit: Ist Windows 2000 (Active Directory) erfolgreich implementiert und bestehen keine besonderen Anforderungen, die durch Windows Server 2003 umzusetzen wären, dann ist die Antwort ganz klar: "warten"!

### Windows NT 4.0

Viele IT-Abteilungen suchen immer nach dem "Killer-Argument", damit eine Migration von Windows NT 4.0 weg, auch im Management entsprechende Unterstützung findet. Hierzu wird dann oft der auslaufende Support verwendet, auch wenn keiner so richtig weiß, was danach geschieht, wenn mal was Elementares passiert.

An dieser Stelle noch eine persönliche Randnotiz: Haben wir genau gewusst, was uns mit dem Wechsel zum Jahr 2000 erwartet, wenn wir nichts im Vorfeld unternehmen?

Auch hat Microsoft kürzlich die "Extended Support"-Phase für Windows NT 4.0 Server noch mal um 1 Jahr verlängert (wie eingangs erwähnt auf den 31.12.2004). Dies spielt aber nur scheinbar den Leuten in die Hände, die die Komplexität des Ganzen unterschätzen. Baut man nämlich auf das Argument des auslaufenden Supports, dann ist in sehr vielen Fällen – das Clientbetriebssystem ist Windows NT 4.0 – ein ganz anderes Datum wichtig, nämlich der 30.06.2003, denn dann endet die "Extended Support"-Phase für Windows NT 4.0 Workstation.

Zugegeben: die Herleitung ist ein wenig schwierig, insbesondere wenn es leicht verständlich wiedergegeben werden muss. Dies ist aber der Fakt und führt in einigen Fällen dazu, dass eine Migration zum Active Directory nur Bestandteil eines Projektes der Migration zu Windows XP ist. In diesen Fällen kommen dann die Argumente pro Windows XP hinzu und diese sind im Zweifel leichter verständlich zu machen, da beispielsweise Entscheider auch Notebooks nutzen. Schade dabei ist nur, dass die wichtigen Veränderungen, die auch dem Unternehmen einen Mehrwert bieten, wie z.B. der Aufbau eines zentralen Verzeichnisdienstes mit allen Vorteilen hinsichtlich Kommunikation etc., in den Hintergrund treten.

Aber zurück zur Ausgangsfrage "warten oder starten?": Ist die Basis Windows NT 4.0, dann stellt sich eine ganz andere Ausgangslage als bei Windows 2000 dar.

Geht man davon aus, dass Windows 2003 Server noch im ersten Halbjahr 2003 veröffentlicht wird, man beabsichtigt direkt auf Windows 2003 Server (Acitve Directory) zu migrieren und man hat bis auf gewisse Vorüberlegungen noch nichts gemacht, dann lautet die Antwort ganz klar starten und zwar mit der Konzipierung!

ach Größe und Struktur der Unternehmung und den anderen Themen, die noch mit ins Projekt gepackt werden (z.B. Migration zu Windows XP) kann der Planungszeitraum zwischen 6 Monaten und weit über einem Jahr liegen.

Würde man heute bzw. im März 2003 starten, so könnte die Durchführung der Migration im Mittel mit Anfang 2004 starten! Dies betrifft aber die Migration zum Active Directory, zu diesem Zeitpunkt ist noch kein Client umgestellt! Also die Phase "ohne" Support beträgt nach dieser Berechnung mindestens 6 Monate, in realen Projekten meist (viel) mehr, insbesondere bis der letzte Client migriert ist.

Anders stellt sich die Ausgangsfrage, wenn ein Projekt mit Migrationsziel Windows 2000 Active Directory ist, die Basis aber weiterhin NT lautet. An dieser Stelle muss dann genau abgewogen werden, was sich ändert, wenn man kurzfristig auf Windows Server 2003 als Migrationsziel wechselt. Insbesondere ist der Aufwand zu prüfen, der mit der Anpassung der Konzeption verbunden ist. Natürlich ist der geplante Migrationszeitpunkt auch von elementarer Bedeutung, denn so ganz sicher kann man sich nicht sein, wann genau Windows Server 2003 veröffentlicht wird. Allerdings spricht eine (persönliche) Hoffnung bzw. Einschätzung dafür, dass es sich lohnen könnte auf Windows Server 2003 zu setzen: Die ersten Service-Packs brauchen (ggf.) nicht abgewartet zu werden, da Microsoft doch sehr viel in die Entwicklung investiert hat. Somit lautet unter diesen Gesichtspunkten die nicht so ganz klare Antwort, starten (mit der Anpassung der Konzeption), wenn es terminlich passt.

---

**Literatur:**

Eine gute Grundlage für diesen Artikel bietet der Artikel "Active Directory und DNS eine Welt?" aus dem Netzwerk Insider vom August 2001, den ich zusammen mit meinem Kollegen Herrn Lars Kuhl erstellt habe.

**Quellen:**

Die dargestellten Neuerungen und Screenshots wurden in erster Linie dem RC 2 zu Windows .NET-Server 2003 entnommen.

Kasten 2 Domain Rename (-Tool)-1

**Domain Rename (-Tool)**

Microsoft stellt ein gesondertes Tool zur Umbennung von Domänen (außer der Active Directory Root Domäne), wie bereits im Artikel beschrieben, zur Verfügung. Mit diesem Tool ist es auch in Teilen möglich, das Design des Active Directory zu verändern. Bevor auf die grundsätzlichen Möglichkeiten, die durch dieses Tool geliefert werden, eingegangen wird, ein Zitat aus einem korrespondierenden White-Paper von Microsoft: "In Windows Server 2003, the goal of the domain rename functionality is to ensure a supported method to rename domains when necessary; it is not intended to make domain rename a routine operation. Thus, although renaming domains is possible in Windows Server 2003, the process is complex and should not be undertaken lightly." (Quelle: "Understanding How Domain Rename Works" von Microsoft).

Wie dieses Statement eindeutig darlegt, ist die gegebene Möglichkeit nur in Ausnahmefällen zu nutzen.
Doch jetzt zu den neuen zusätzlichen Optionen, die durch das Tool ermöglicht werden. Durch das Tool können auch Domänen innerhalb der Gesamtstruktur "verschoben" werden. Die Bilder 19 bis 22 zeigen zwei mögliche Szenarien.

Im ersten Szenario (Bilder 19 und 20) wird eine untergeordnete Domäne (mig.sub.comconsult.com - 3. Ebene) in eine neue "tree root domain" migriert bzw. es wird eine neue Struktur geschaffen (comconsult-akademie.de - 1. Ebene).

Bild 19 Szenario 1 : Vor der Umstrukturierung und Umbenennung

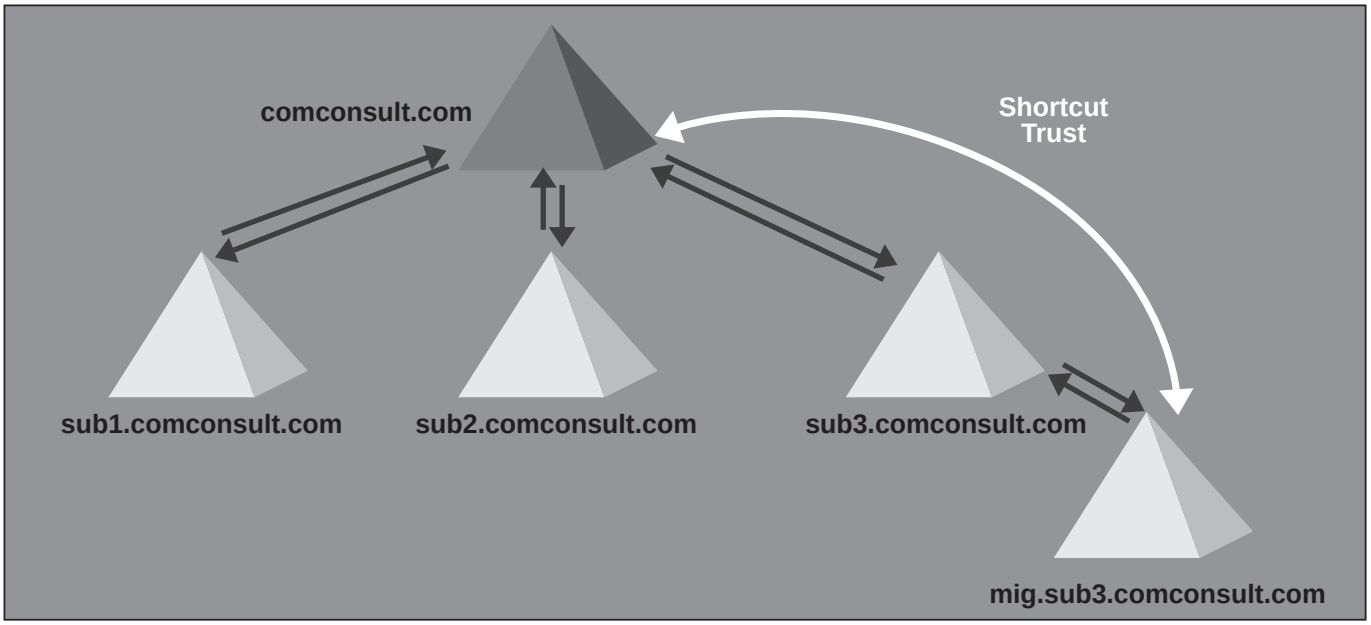
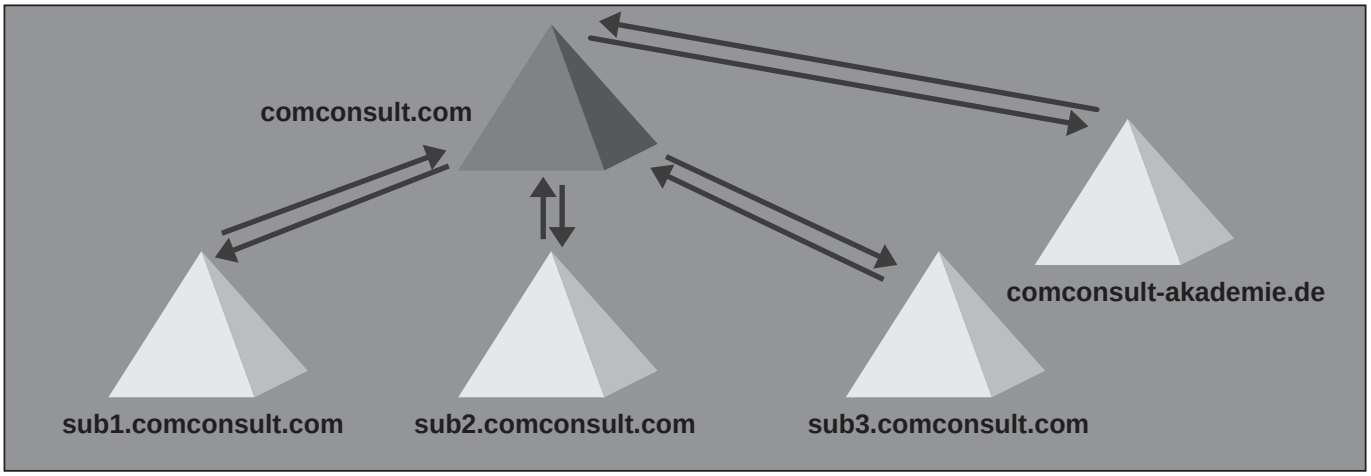



Bild 20 Szenario 1 : Nach der Umstrukturierung und Umbenennung



Kasten 3 Domain Rename (-Tool)-2

Das zweite Szenario (Bilder 21 und 22) skizziert, wie eine untergeordnete Domäne (sub.mig.sub3.comconsult.com - 4. Ebene) im gleichen Namensraum "eine Stufe höher klettert" (new.sub3.comconsult.com) und die "Zwischendomäne" (mig.sub3.comconsult.com - 3. Ebene) in einen anderen Zweig wechselt (mig.sub1.comconsult.com - 3. Ebene).

Bild 21 Szenario 2 : Vor der Umstrukturierung und Umbenennung

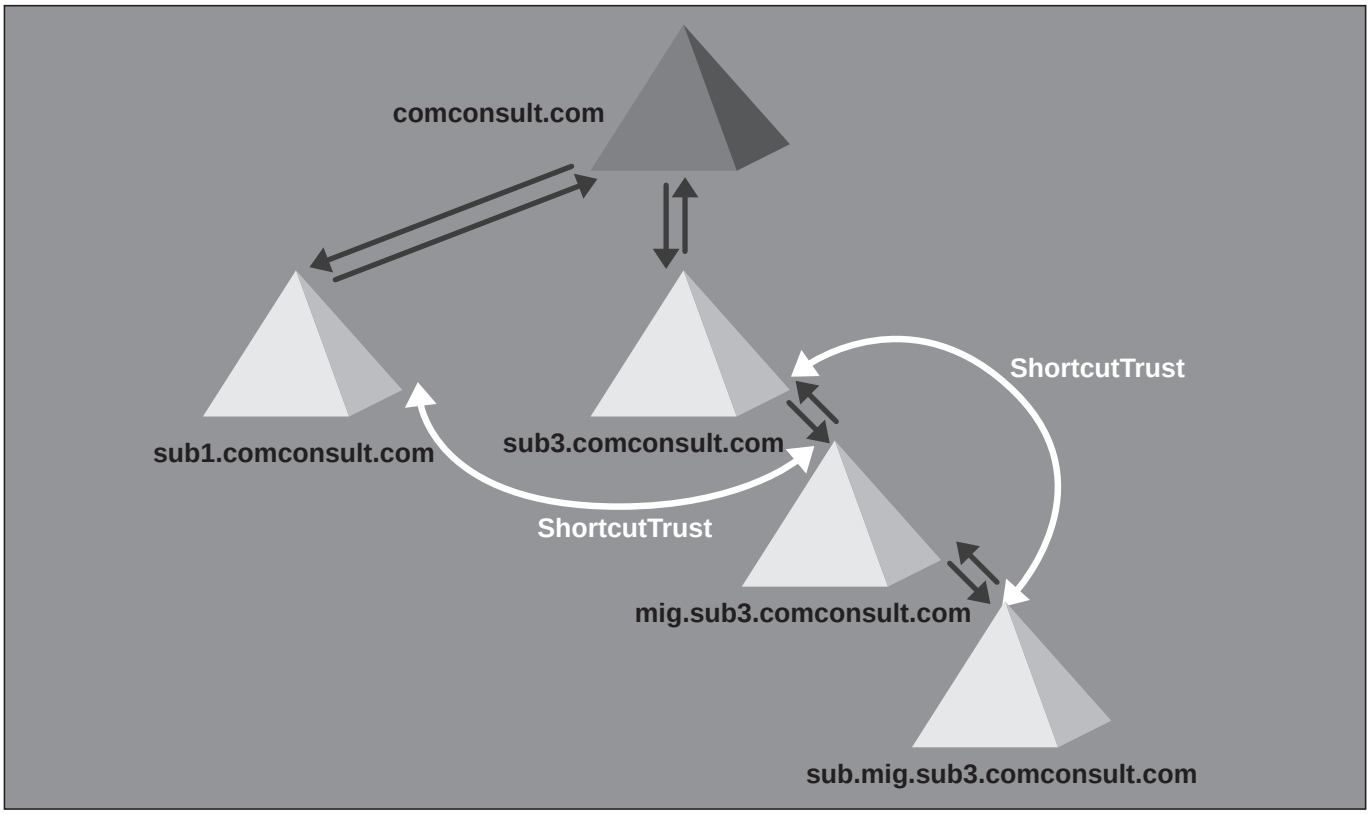
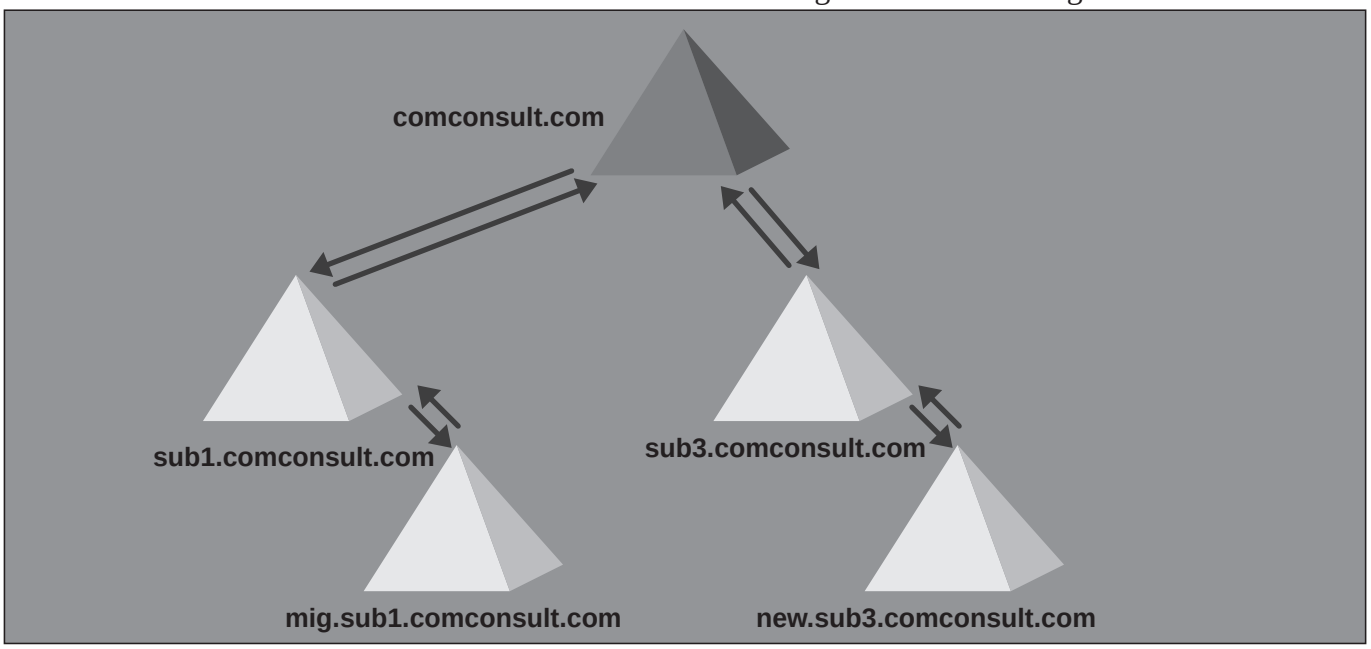



Bild 22 Szenario 2 : Nach der Umstrukturierung und Umbenennung



Kasten 4 Domain Rename (-Tool)-3

Wie aus diesen Beispielen bereits abzuleiten ist, sind fast sämtliche Konstellation vorstellbar

– Ausnahme hierbei bildet die Active Directory Root Domäne.

Doch müssen auch die grundsätzlichen Anforderungen beachtet werden:

- Die Umbennung von Domänen ist nicht in einer Gesamtstruktur möglich, in der Exchange 2000 implementiert ist.
- Der Forest Functionality Level muss Windows .NET sein (alle Domänenkontroller auf Windows Server 2003).
- Die Operationen müssen von Enterprise-Admins durchgeführt werden.
- Die so genannte "Control Station", der Rechner auf dem die Operationen durchgeführt werden, muss Windows Server 2003 (Enterprise, Datacenter) als Betriebssystem haben und darf kein Domänenkontroller sein.
- Alle Server, die eine DFS-Root vorhalten, müssen mindestens Windows 2000 mit Service Pack 3 haben.

Wie ebenfalls aus den Szenarien der Bilder 19 - 22 zu ersehen ist, spielen Shortcut-Trusts eine wichtige Rolle, wobei die Implementierung dieser Vertrauensstellungen nur einen Teil der Aufgaben darstellt.

Folgende Bereiche sind ebenfalls vor, während oder nach dem Umbennungsprozess zu beachten:

- DNS,
- Ordnerumleitung und Roaming-User Profile im domänenbasiertem DFS,
- Konfiguration der (Domänen-) Computer,
- Replikation,
- Management von Zertifikaten und weiteres.

Eine Konkretisierung dieser Themen, sowie die Definition der einzelnen Migrationsschritte sprengt den Rahmen dieses Artikels.

Doch es ist ganz eindeutig anhand der genannten Themen und Anforderungen erkennbar, dass der Einsatz des Domain Rename Tools (fast) ein eigenes Projekt darstellt und die zitierte Aussage von Microsoft unterstreicht.

Insofern behalten die im Artikel gemachten Aussagen hinsichtlich der Wichtigkeit im dcpromo-Prozess und des Einsatzes einer dedizierten Active Directory Root Domäne ihre volle Gültigkeit.

Zum Autor:

Markus Holländer ist Competence Center Leiter Backoffice bei der ComConsult Beratung und Planung GmbH. Neben der Leitung des Competence Centers sind seine Hauptaktivitäten Projektleitungen und Konzipierungen im Bereich der Themen Active Directory, DNS und Windows XP. Insbesondere zu diesen Themenkomplexen verfügt er über jahrelange Projekterfahrung bei namhaften Unternehmen. Zurzeit ist er auf Ebene der Projektleitung bei Migrationen zu Windows XP (inkl. AD-Migration) in mehreren Projekten für mehr als insgesamt 15.000 Clientrechnern tätig. Herr Holländer ist auch für die Entwicklung der .NET-Seminare des Competence Centers in Zusammenarbeit mit der ComConsult Akademie verantwortlich und einer der Hauptreferenten. Zu erreichen ist er unter hollaender@comconsult.com.

Neues Seminar

# Migration zu Microsoft Active Directory – starten oder warten?

**Vom 19. bis 21. Mai 2003 veranstaltet die ComConsult Akademie im Hilton Hotel in Bonn zum ersten Mal ihr neues Seminar "Migration zu Microsoft Active Directory – starten oder warten?"**

Die Motivation zur Einführung der neuen Betriebssystemgeneration von Microsoft beruht auf den hohen Aufwänden im administrativen Umfeld sowie vielen nicht ausgereiften oder fehlenden Leistungsanforderungen. Die Tendenz zur Abkehr reiner Client-Server-Landschaften ist mit dem starken Interesse an Windows Terminal Server Lösungen deutlich zu erkennen. Ist hier eine Koexistenz denkbar – und sinnvoll? Gibt es echte Alternativen zu Microsoft Produkten? Das anstehende Investment zur Migration der bestehenden Client-Server-Infrastruktur in Richtung Windows 2000 / 2003 ist immens – der tatsächliche Benefit für die Unternehmen ist oft nur schwierig zu erkennen. Mit der Einführung eines Active Directory sind neben technischen Belangen insbesondere organisatorische Aspekte gefragt, die bei dem Design der zukünftigen Landschaft berücksichtigt werden müssen. Dazu müssen allen direkt oder indirekt Projektbeteiligten die Grundzüge der Betriebssystemplattform mit Ihren Leistungsmerkmalen sowie die integralen Bestandteile eines Active Directory bekannt sein.

Das 3-tägige Seminar richtet sich an IT-Entscheider und Projektleiter, die diese komplexe Thematik kennen- und einschätzen lernen wollen.

Unter der Leitung von Dipl.-Ing./MCSE Martin Barbian - Geschäftsführer der ITC GmbH werden die unterschiedlichen Leistungsmerkmale, Features und Funktionen vorgestellt. Dabei werden viele Bestandteile live demonstriert. Neben Wirtschaftlichkeitsbetrachtungen werden realitätsbezogene Einsatzszenarien aufgezeigt. Zudem wird ein Argumentationsleitfaden aufgebaut, jedoch auch die Defizite und Grenzbereiche genannt. Darüber hinaus werden konkrete Lösungsansätze erörtert und die konzeptionelle Vorgehensweise aufbereitet.

Der Referent Dipl.-Ing. / MCSE Martin Barbian von der ITC GmbH mit den Standorten Detmold, Düsseldorf, Frankfurt und Hamburg zählt mit seinem Team zu den führenden deutschen SMS-Experten. Darüber hinaus befasst sich das anerkannte Beratungshaus neben dem Desktopmanagement mit anderen aktuellen Themen, die einer betriebswirtschaftlichen Optimierung der IT-Landschaft Rechnung tragen. Dazu zählen das Netz- und Systemmanagement sowie eMail- und Informationssysteme, User Help Desk Lösungen und Multiuser Systeme (Windows Terminal Server) unter Windows NT / 2000. Im Zuge der Weiterentwicklung der Windows Betriebssystemfamilie und der BackOffice Suite gewinnt die 2000er Generation zunehmend Akzeptanz in bundesdeutschen Unternehmen. Die ITC GmbH blickt bereits auf einige Windows 2000 Projekte mit unterschiedlichsten Schwerpunkten zurück, so daß die Praxisnähe eingehend vermittelt werden kann. Als Microsoft Cold Certified Partner ist die ITC GmbH frühzeitig in Beta-Evaluierungsphasen involviert und stets als Teilnehmer auf internationalen Microsoft Strategieveranstaltungen vertreten.

## Zum Thema

Das Microsoft Multitasking Betriebsystem Windows NT 4.0 ist server- wie clientseitig weltweit etabliert und hat größte Teile des Wettbewerbs in vielen Branchen und Anwendungsbereichen verdrängt. Die stetig wachsende BackOffice Suite untermauert diesen fortschreitenden Prozess. Trotzdem weist Windows NT 4.0 auch bei Berücksichtigung des aktuellen Service Packs in vieler Hinsicht Schwächen auf. Das Spektrum reicht von mangelnder Administrierbarkeit, über begrenzte Skalierbarkeit bis hin zu eingeschränkter Verfügbarkeit.

Die neue Generation – Windows 2000 – hat lange auf sich warten lassen – angekündigt waren die Verbesserungen schon frühzeitig, doch die Resultate im endgültigen Final Release blieben zunächst aus.

Seit Frühjahr 2000 ist Windows 2000 in verschiedenen Ausführungen verfügbar - weitere Varianten wie der Data Center Server folgten später. Auch die BackOffice 2000 wurde erst zum Ende 2000 endgültig freigegeben, da wichtige Bestandteile wie SQL Server 2000 und Exchange Server 2000 nicht abschließend released werden konnten.

Kaum sind alle maßgeblichen Komponenten der Windows 2000er Familie vorhanden wird schon die nächste Generation – jetzt mit der aktuellen Bezeichnung "Windows Server 2003" – für Frühjahr 2003 angekündigt.

In der Vergangenheit gab es doch schon einige Umbenennung mit entsprechenden Irritationen:

- Aus NT 5.0 wurde seinerzeit über Nacht Windows 2000.
- Aus Windows .NET Server wurde kürzlich erst Windows .NET Server 2003.
- Mitte Januar 2003 wird aus Windows .NET Server 2003 kurzerhand Windows Server 2003.

Dabei handelt es sich um ein Minor Upgrade – also quasi eine Version NT 5.1, wenn Windows 2000 unter NT 5.0 eingeordnet wird. Es handelt sich im Wesentlichen um Verbesserungen oder Optimierungen in vielen Komponenten, Funktionen und Features der Produktfamilie. Die grundlegende Architektur und Philosophie ist allerdings geblieben. Neben den diversen elementaren, integrierten Diensten ist der Verzeichnisdienst sozusagen das Herz der Windows basierten Client-/ Serverlandschaft.

## Migration zu Microsoft Active Directory - starten oder warten?

Das Seminar beantwortet folgende Fragen:

- Ist Windows 2000 stabil und zuverlässig?
- Bereinigt es wirklich die Defizite im NT 4.0 Umfeld?
- Wird es doch Zeit die Umgebung Novell Netware zu verlassen?
- Was bringen die neuen Features und Funktionen?
- Welche Vorteile ergeben sich durch den Verzeichnisdienst Active Directory?
- Welche Schnittstellen zur Integration und Administration können genutzt werden?
- Welche Anwendungen laufen überhaupt unter Windows 2000?
- Setzen wir auf Windows XP oder auf W2k Prof. Workstations – wo liegen die Vorteile?
- Ist eine unternehmensweite Windows Terminal Server Farm eine Alternative?
- Warten wir auf die 2003er Familie im Server Umfeld – wo liegen die Verbesserungen?
- Welche W2k Dienste und "built in" Funktionen sollen konkret verwendet werden?
- Wie muss ich Exchange und andere BackOffice Komponenten berücksichtigen?
- Wie groß sind die Kosten für Konzeption, Planung und Realisierung?
- Wie strukturiere und organisiere ich ein derartiges Projekt?
- Welche typischen Projektphasen sind zu berücksichtigen?
- Welche Arbeitspakete sind zu definieren?
- Welche konkreten Maßnahmen sind zu ergreifen?
- Welche Abhängigkeiten ergeben sich zu den einzelnen Meilensteinen?
- Welche Randbedingungen sind zu berücksichtigen?
- Welche Risiken sind einzukalkulieren?
- Wie hoch werden die Personalaufwände sein?
- Welche Tools könnten hilfreich sein?
- Wie hoch wird das Investitionsvolumen in Hard- und Software sein?
- Wie betreibe ich die neue Umgebung?
- Welche Rollout-Verfahren und Management-Werkzeuge sind zu berücksichtigen?

**Migration zu Microsoft Active Directory - starten oder warten? – Die Inhalte**

**Einleitung**
Definition Client-/Server-Architektur und Verzeichnisdienste

**Aktuelle Betriebssysteme im Überblick**
- Hersteller und Anbieter • Client- und Servertypen
- Lösungsansätze und Technologien im Kurzvergleich
- Anwendungs- und Datenbankenplattformen

**Windows 2000 / 2003 - die Produktfamilie**
- Komponenten und Varianten
- BackOffice 2000 und andere 2000er / 2003erProdukte
- Dienste und integrierte Applikationen
- Philosophie, Architektur und Verzeichnisdienst AD

**Windows 2000 / 2003 - Konzeption**

**Organisation: Active Directory**
- Active Directory Grundlagen
- Standards von Verzeichnissen & Verzeichnisdienste
- Schema und Namenskonventionen • Forests und Trees
- Domains und Organizational Units • Vertrauensstellungen
- Betriebsmodi • Spezielle Funktionen von Domain Controllern
- Rechte und Berechtigungen • Benutzer und Gruppen
- Group Policies und Profiles

**Infrastruktur**
- Dynamic DNS / static DNS / WINS / DHCP • RAS
- Clustering und DFS • Windows Terminal Server Service
- Server und Network Loadbalancing (SLB / NLB)
- Backup- und Restore • Integration, Migration, Upgrade

**Management und Administration**
- RIS und PXE • IntelliMirror und MSI • MMC und WEBM
- Remote Administration und Monitoring • Administration des AD

**Security**
- SmartCard und PKI • NTFS und Encrypted File System
- VPN • IPSec und Kerberos

**Realisierung**
- Installation und Konfiguration • Rollout
- Einrichtung Environment

**Produktivbetrieb**
- Benutzer- und Gruppen Administration
- Ressourcenverwaltung • Softwareverteilung

**Resümee und Ausblick**
- Vor- und Nachteile im Vergleich zu NT 4.0, LINUX, Netware
- Empfehlungen

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

# Seminar-Anmeldung

☐ Ich melde mich an für das Seminar

**Migration zu Microsoft Active Directory – starten oder warten?**

vom 19.05. - 21.05.03 in Bonn
zum Preis von € 1.590,-- zzgl. MwSt.

☐ Buchen Sie für mich ein Zimmer im Hilton

Buchen Sie über unsere Web Site:
**www.comconsult-akademie.de**

| | |
|---|---|
| Vorname, Nachname | Vorname |
| Firma | PLZ, Ort |
| Straße | eMail |
| Telefon, Fax | Unterschrift |

Anzeige

# Ausbildung zum ComConsult Certified Network Engineer


## Jetzt mit HP 5450 oder Sony Clie NX70V als Bestandteil der Ausbildung

**Komplett-Paket:** Für die komplette Ausbildung mit allen vier Seminaren zum ComConsult Certified Network Engineer zahlen Sie statt € 7.960,-- nur den Paketpreis von € 6.690,-- zzgl. MwSt. und erhalten zusätzlich wahlweise ein HP 5450 oder ein Sony Clie NX70V als Bestandteil des Ausbildungspakets bis zum 30.06.03.

## Das CCNE-Praxis-Seminar:

**LAN-Praxis-Intensiv-Seminar:**
**Praktischer Aufbau von lokalen Netzen und Umsetzung typischer Netzwerk-Konfigurationen**
Einzelpreis: € 2.290,-- zzgl. MwSt.
Zusätzlich zum Komplett-Paket: € 1.890,-- zzgl. MwSt.

- **05.05. - 09.05.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**

## Termine 2003

**Lokale Netze**
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **17.03. - 21.03.03 in Aachen**
- **19.05. - 23.05.03 in Aachen**
- **21.07. - 25.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **10.11. - 14.11.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

**TCP/IP und SNMP**
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **17.03. - 21.03.03 in Berlin**
- **05.05. - 09.05.03 in Bonn**
- **21.07. - 25.07.03 in Berlin**
- **22.09. - 26.09.03 in Berlin**
- **13.10. - 17.10.03 in Berlin**
- **08.12. - 12.12.03 in Berlin**

**Internetworking**
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **05.05. - 09.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

**Neue Ethernet Technologien**
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **17.03. - 21.03.03 in Aachen**
- **12.05. - 16.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**
- **13.10. - 17.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

ComConsult Akademie

ComConsult Veranstaltungskalender

# Aktuelle Veranstaltungen

## Service Level Management in der Praxis, 17. - 19.03.03 in Köln

Das Seminar behandelt die Königsdisziplin des Netzwerk- und System-Managements: Service Level Management, wo die technischen und organisatorischen Fäden einer IT-Organisation zusammenlaufen und die zentrale Schnittstelle zwischen Betreibern und Anwendern innerhalb einer Firma oder zwischen externen Dienstleistern und Anwendern liegt.
Referenten: Heinz Hüsges und Martin Rother (Arxes NCC AG) Preis: € 1.590,-- zzgl. MwSt.

## .NET SQL Server, 17. - 19.03.03 in Köln

Das Seminar mit Praxisteil gibt einen Überblick über die Features, die SQL Server 2000 zur Verfügung stellt. Dabei wird auf die Schnittstellen zu Active Directory und den Office bzw. Backoffice-Produkten ebenso Wert gelegt wie auf die Erklärung der verschiedenen Datenzugriffspfade der Programmierwelt.
Referent: Hans-Willi Kremer (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

## Lokale Netze für Einsteiger, 17. - 21.03.03 in Aachen

Das Intensiv-Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referenten: Dipl.-Ing. Roland Moos und Dr. Jürgen Suppan, ComConsult Akademie Preis: € 1.990,-- zzgl. MwSt.

## TCP/IP und SNMP, 17. - 21.03.03 in Berlin

Das Intensiv-Seminar vermittelt einen praxis-orientierten Einblick in den Aufbau und den Betrieb von heterogenen Netzen, die den Kommunikationsstandard TCP/IP und den Netzmanagement-Standard SNMP benutzen.
Referent: Matthias Hein Preis: € 1.990,--zzgl. MwSt.

## Sicherheitslösungen für vernetzte IT-Umgebungen, 17. - 21.03.03 in Köln

Das Seminar beschäftigt sich mit modernen Sicherheitslösungen für den Internet-Zugang, das Mail-System, die Server, die Clienten und das Netz. Referenten: Das IT-Sicherheits-Team der ComConsult Beratung und Planung Preis: € 1.990,-- zzgl. MwSt.

## Neue Ethernet-Technologien, 17. - 21.03.03 in Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke. Referenten: Dipl.-Inform Oliver Flüs, Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause, Dr. Joachim Wetzlar, ComConsult Beratung und Planung Preis: € 1.990,--zzgl. MwSt.

## IT-Projektmanagement I, 17. - 21.03.03 in Bonn

Das Seminar ist der erste von zwei Teilen der Ausbildung zum "ComConsult Zertifizierter IT-Projektleiter". Hier lernen die Teilnehmer ein Projekt effektiv zu organisieren und überzeugend zu führen, sowie die Prozess-Optimierung der Projektabwicklung.
Referent: Dr. Ralf Hillemacher Einzelpreis: € 2.290,-- zzgl. MwSt.

## Mobile und drahtlose Datenkommunikation..., 19. - 20.03.03 in München

Das Seminar gibt am 1. Tag einen Überblick über mobile und drahtlose Kommunikation, behandelt vertieft die GSM-Datendienste und zeigt die Möglichkeiten für die Unternehmenskommunikation auf und widmet sich am 2. Tag schwerpunktmäßig dem Wireless LAN.
Referenten: Dipl.-Inform. Andreas Meder, Dr. Simon Hoff, Dr. Jochen Wetzlar Preis: € 1.290,-- zzgl. MwSt.

## Sonderveranstaltung: Windows-Security, 31.03 - 01.04 in Köln

Das Seminar beschäftigt sich mit dem Haupt-Sicherheitsrisiko der gesamten IT-Infrastruktur: dem Netzwerk-Clienten – typischerweise ein PC mit Windows-Betriebssystem – im Zusammenhang mit der Planung und Umsetzung von VPN-Lösungen und Wireless Security.
Preis (incl. Report) € 1.980,-- zzgl. MwSt., Paketpreis (mit zusätzlichen Reports VPN und Wireless LAN Sicherheit) € 2.248,-- zzgl. MwSt.

## Windows Server 2003 und PKI – die richtige Kombination? 31.03 - 01.04 in Köln

Das Seminar macht die Teilnehmer neben den theoretischen Grundlagen einer PKI auch mit der grundsätzlichen Installation, Konfiguration, Administration und dem Betrieb einer Windows 2000 / .Net PKI im Rahmen von Live-Präsentationen vertraut.
Referent: Dipl.-Ing. Martin Barbian (ITC GmbH) Preis: € 1.290,-- zzgl. MwSt.

## IT Asset-Management wertschaffend einsetzen, 31.03 - 01.04 in Köln

Das Seminar bietet anhand von Analysten-aussagen und Studien einen Überblick der zukünftigen Herausforderungen an ganzheitliches IT-Asset Management und die hieraus entstehenden Kosteneinsparpotentiale.
Referent: Dr. Roger H. Jakobs (ComConsult Kommunikationstechnik) Preis: € 1.290,-- zzgl. MwSt.

## ITIL-Foundation, 31.03 - 01.04 in Köln

Das Seminar ist der Einstieg in die ITIL-Thematik. Die Teilnehmer haben im Anschluss an das Seminar am zweiten Tag die Möglichkeit das Foundation Exam abzulegen mit dem Zertifikat "Foundation Certificate in IT Service Management".
Referent: Dipl.-Verwaltungswirt Jürgen Dierlamm Preis: € 1.290,-- zzgl. MwSt.

ComConsult Veranstaltungskalender

# Aktuelle Veranstaltungen

## .NET ISA Server, 31.03 - 01.04 in Leverkusen

Das Seminar befasst sich mit der Implementierung vom Microsoft Internet Security & Acceleration (ISA) Server 2000und zeigt die verschiedenen Modi und diversen Einstellungsoptionen des ISA Servers sowie deren sinnvollen Einsatz im Netzwerk.
Referent: Hans-Willi Kremer (ComConsult Beratung und Planung) Preis: € 1.290,-- zzgl. MwSt.

## Verkabelungssysteme für Lokale Netzwerke, 31.03 - 02.04 in Köln

Das Seminar führt methodisch vom aktuellen Stand der Technik bis zu Leistungsmerkmalen zukünftiger Lösungen. Neben einer Betrachtung des aktuellen Normungsstands und Vergleich mit herstellerspezifischen Lösungen wid auf die Planungs- und Installationsmaßnahmen eingegangen, die vor der Verlegung der ersten Kabel zu beachten sind.
Referent:en: Mark Groten, Dipl.-Ing. Hartmut Kell Preis: € 1.290,-- zzgl. MwSt.

## Moderne Datenkommunikation: Durchblick im Netzwerk, 31.03 - 04.04 in Aachen

Das Intensiv-Seminar vermittelt Techniken, Verfahren und Systeme der Datenkommunikation für Ein- und Umsteiger. Der Schwerpunkt liegt auf dem erfolgreichen Einsatz der Internet/Intranet-Technologien.
Referent: Dr. Franz-Joachim Kauffels Preis: € 1.990,-- zzgl. MwSt.

## Trouble Shooting in geswitchen Ethernet-Umgebungen, 31.03 - 04.04 in Bonn

Das Seminar ist der zweite von drei Teilen der Ausbildung zum "ComConsult Certified Trouble Shooter" und beschäftigt sich mit Störungen im Netzwerk-Bereich, di e durch fehlerhafte Konfiguration von Switching-Verfahren oder durch Fehler in der Firmware von Switch-Systemen entstehen, sowie mit "Konfigurations-Fallen", die in Redundanz-Situationen ein Netzwerk ins Leere laufen lassen können.
Referenten: Dipl.-Inform. Oliver Flüs, Dr. Jochen Wetzlar Einzelpreis: € 2.490,-- zzgl. MwSt.

## IP-Wissen für die Praxis, 07. - 09.04 in Köln

Das Seminar bietet Grundlagen, Tipps und neueste Entwicklungen und vermittelt praxisnah die für den Betrieb von IP-Netzen notwendigen Basis-Kenntnisse.
Referenten: Dipl.-Inform. Oliver Flüs und Dipl.-Inform. Andreas Meder (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

## Performance-Qualitätssicherung von C/S- und Web-Applikationen, 07. - 11.04 in Köln

Das Seminar vermittelt eine Einführung in die Performance-Qualitätssicherung mit besonderem Augenmerk auf die Definition und Überprüfung von Service Level Requirements. Durch Fokussierung auf C/S- und Web-Applikationen werden konkrete Praxisbezüge hergestellt und der Teilnehmer in die Lage versetzt, die Güte von Performance-Tests zu bewerten, aufzusetzen, zu steuern und durchzuführen.
Referenten: Dr. Stephan Baumhoff, Dr. Armin Wachter Preis: € 1.990,-- zzgl. MwSt.

## IT-Projektmanagement II, 07. - 11.04 in Köln

Das Seminar ist der zweite von zwei Teilen der Ausbildung zum "ComConsult Zertifizierter IT-Projektleiter". Hier lernen die Teilnehmer Sitzungen zu moderieren, Projekte zu präsentieren, erfolgreich zu verhandeln und Projektteams zu leiten.
Referent: Dr. Ralf Hillemacher Einzelpreis: € 2.290,-- zzgl. MwSt.

## Sicherheits-Praxis-Seminar, 07. - 11.04 in Aachen

Das Seminar vermittelt nach der konzeptionellen theoretischen Einführung die praktische Implementierung an typischen Beispielen: Firewall-Praxis inkl. Proxy-Konfiguration, VPN-Praxis mit Appliances und Windows2000-Servern, Härtung von Windows, Linux und Solaris Betriebssystemen, WLAN-Sicherheit
5 Referenten der ComConsult Beratung und Planung Preis: € 2.290,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

# Anmeldung

Titel des Seminars

Termin

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.de**

Vorname

Firma

Straße

Telefon, Fax

Nachname

PLZ, Ort

eMail

Unterschrift

Handelsplattform für gebrauchte Netzwerkkomponenten

# Gebrauchte Netzwerkkomponenten

## Die Spielregeln

Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffentlichen es unter einer Anzeigen-Nr. im Netzwerk Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her. Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

## Gebote

### Adapter

**3Com** CoreBuilder 9000, Anzahl 1, Preis VS, 1 x 3CB9E16 CoreBuilder 9000 Chassis 2 x 3CB9LG9MC 9 x 1000Base-SX, SC 3 x 3CB9LF36R 36 x 10/100Base-TX, RJ45 2 x 3CB9FG24T Switch Fabric 48Gbps 1 x 3CB9LF10MC,10 x 100Base-FX, SC, 1 x 3CB9LG2MC, 2 x 1000Base-SX, SC, 2 x 3CB9EP8 Power Supply, 1 x 3CB9EMC Redundant Management Engine Controller, 1 x 3CB9EME Management Engine Anzeigen-Nr. B21216

### Erweiterungseinheit

**Erweiterungseinheit** a`20 ICS-Ports (PN: 53F5501), Anzahl 19, Preis VB, Anzeigen-Nr. B30103

### Steuereinheit

**IBM** 5394-01B, BOS e-Twinax (IP) Controller B044656 für 56, Anzahl 1, Preis VB, Geräteadressen mit 8-Port Controller-Adapter B04500, Kaufpreis Euro 11.400 /Okt 2000, Anzeigen-Nr. B30101

### Switch/Brücke

**Madge** Deskstream 24 Port Token Ring Switch, Anzahl >10, Preis 1.200,-- Euro VB, Bemerkung: Demo-Equipment, wie neu, incl. Garantie, incl. Stackingmodul, Ethernet und HSTR Uplinks ebenfalls vorhanden, Anzeigen-Nr. B21217

## Gebote

### Switch/Brücke

**Cabletron**
1 x MMAC-M8FNB à 200,00 Euro, 4 x M8PSM-E à 50,00 Euro, 5 x ESXMIM à 100,00 Euro, 1 x ESXMIM-F2 à 160,00 Euro, 1 x EMM-E6 à 180,00 Euro, Anzeigen-Nr. B21210

**Cabletron**
2 x ATX LANSwitch à 300,00 Euro, 2 x 3CPSM-R-ATX à 100,00 Euro, 6 x 3F00-01 à 120,00 Euro, 1 x 3H02-04 à 120,00 Euro, 1 x 3E08-04 à 80,00 Euro, 1 x 3E02-08 à 80,00 Euro, 1 x 3E02-04 à 40,00 Euro, Anzeigen-Nr. B21213

**Enterasys**
2 x SmartSwitch 9000/14-Slot à 700,00 Euro, 1 x SmartSwitch 9000/6-Slot à 400,00 Euro, 2 x 9C214-1 à 100,00 Euro, 2 x 9C206-1 à 50,00 Euro, 2 x 9F426-03 à 360,00 Euro, 1 x 9H421-12 à 720,00 Euro, 11 x 9H422-12 à 360,00 Euro, 2 x 9H423-28 à 390,00 Euro, 2 x 9E428-12 à 240,00 Euro, 8 x 9E423-36 à 360,00 Euro, Anzeigen-Nr. B21211

**Cabletron** Modell: ESX 1380, Anzahl 1, Preis 300,00 Euro, Bemerkung: Inklusive: 1 x BRIM-E100, 1 x FE100-FX, Anzeigen-Nr. B21214

**Enterasys**
1 x 2E42-27R à 240,00 Euro, 2 x HSIM-F6 à 120,00 Euro, 6 x FE100-TX à 30,00 Euro, 3 x FE100-FX à 60,00 Euro, Anzeigen-Nr. B21215

### Sonstige

**IBM** Modell: 8230-001, Anzahl 8, Preis VB, Anzeigen-Nr. B30102

**NetScout** Modell: TR 7103R/TR, Anzahl 1, Preis VB, Bemerkung: FDDI DAS/Token Ring - Probe, Anzeigen-Nr. B30204

**IBM** Lanstreamer, Anzahl 31, Preis VB, Anzeigen-Nr. B30206

**NetScout** Dolch, Anzahl 1, Preis 20.000 Euro, Bemerkung: Protokoll Analysator für Gigabit Ethernet, PAC 65, Pentium II 400 MHZ Mit NT 4.0 Softwareversion Sniffer Pro Version 4.0.12 ist aufgespielt und funktional. Zusätzlich Sniffer Predictor Release 2.0.1.1203, Anzeigen-Nr. B30201

## Gebote

### Sonstige

**NetScout** Modell: 8211ET/128 mit Zubehör, Anzahl mehrere, Preis verschieden, Bemerkung: 4 x NetScout: 8211ET/128 (7.500,00 Euro/St.), 4 x NetScout: TX-Tap-Copper Tap Kit (820,00 Euro/St.), 8 x NetScout: 60/40 Singlemode Fiber Optic Splitter (1.100,00 Euro/St.), Anzeigen-Nr. B30202

**Fax an ComConsult 02408/955-399**

☐ **Ich suche**

☐ **Ich biete**

☐ **Antwort auf Anzeigen-Nr.** ☐ _____

Produkt/Komponente/Release/Software

_____

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon

_____

Fax

_____

eMail

**Weitere Anzeigen** finden Sie auf dem Web-Server der ComConsult Akademie www.comconsult-akademie.de